

Как ИТ-организация может завоевать доверие своих клиентов: практический подход

А.Н. Бирюков

E-mail: anbiryukov@fa.ru

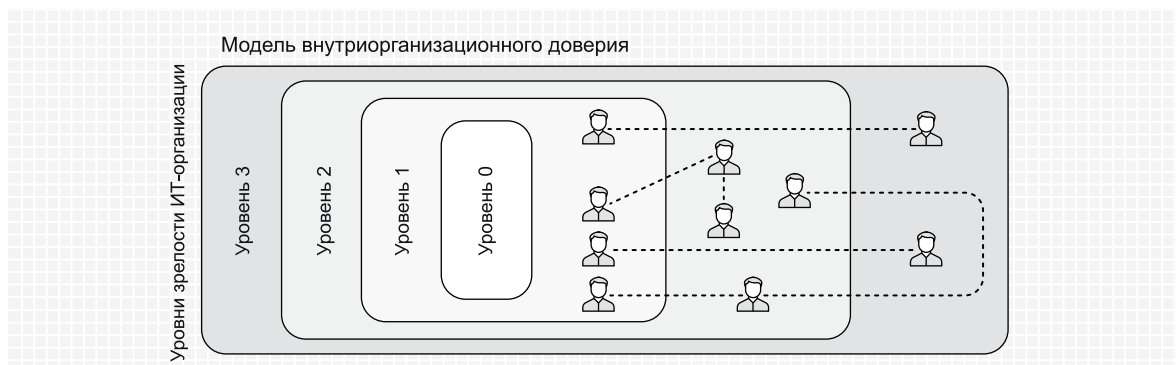
Финансовый университет при Правительстве РФ

Адрес: 125993, г. Москва, Ленинградский пр-т, д. 49

Аннотация

В статье описан подход, которым внутренний провайдер ИТ-услуг может воспользоваться для того, чтобы завоевать доверие своих бизнес-клиентов. В качестве клиентов внутреннего провайдера рассматриваются исключительно внутренние клиенты. Отличительной чертой предлагаемого подхода является его ориентированность на достижение практических целей, т.е. на построение доверия между ИТ-организацией и ее клиентами в конкретной организации. Идея подхода заключается в том, что принимается ряд допущений об объективно измеримых предпосылках возникновения такого доверия, что позволяет конструктивно ставить и решать задачу построения отношений доверия. Предлагается модель внутриорганизационного доверия, которая совершенствуется по мере того, как ИТ-организация развивает свои способности к построению отношений доверия. Эта модель описывает всех потребителей услуг и взаимоотношения между ними, а также учитывает специфику внутреннего рынка ИТ-услуг в организации. Приводится высокоуровневое описание модели доверия, которое может служить отправной точкой при построении модели внутриорганизационного доверия в конкретной организации. Предлагается подход к совершенствованию модели внутриорганизационного доверия, основанный на принципах, близких к тем, которые используются в традиционной модели СММИ. Этот подход позволяет ИТ-провайдеру использовать преимущества методов оценки зрелости для улучшения деятельности по управлению доверием.

Графическая аннотация



Ключевые слова: провайдер ИТ-услуг; внутренний рынок ИТ-услуг; доверие; ИТ-организация; критерии доверия; модель внутриорганизационного доверия; управление доверием; завоевание доверия; зрелость; уровень возможностей.

Цитирование: Бирюков А.Н. Как ИТ-организация может завоевать доверие своих клиентов: практический подход // Бизнес-информатика. 2019. Т. 13. № 3. С. 67–77. DOI: 10.17323/1998-0663.2019.3.67.77

Введение

За последние десятилетия понимание доверия и его роли для организаций существенно выросли. Сегодня доверие рассматривается как чрезвычайно сложный многомерный феномен, существующий во многих формах, таких как доверие между людьми или межличностное доверие [1, 2], доверие между организациями (межорганизационное доверие) [3], доверие в рамках одной организации (внутриорганизационное доверие) [2, 4, 5]. Доверие изучается с разных точек зрения: психологической, экономической, философской, управленческой [2, 4–6]. В современной литературе представлены исследования, посвященные доверию в множестве отраслей, начиная с электронного бизнеса и заканчивая политическими и культурными сферами деятельности. Несмотря на ряд оригинальных и глубоких идей, предложенных исследователями, и значительный объем затраченных усилий, до сих пор не удалось выработать целостный подход к изучению доверия. Не существует даже определения доверия, которое принималось бы всеми исследователями (или значительной их частью) в качестве отправной точки для дальнейшего исследования. Практически каждый исследователь предлагает собственное определение доверия, что только повышает уровень несогласованности и несравнимости получаемых результатов [7].

По нашему мнению, такая ситуация является следствием не только сложной природы доверия, но и того, что большая часть исследователей придерживается описательного, качественного подхода к изучению доверия. Как правило, в основе лежит статистическая обработка результатов всевозможных опросов, выявляющих отношение людей к разным факторам, влияющим на доверие. Обзор методов исследования доверия приведен в работе [5], где рассматриваются онтологические, телеологические и эпистемологические аспекты процесса исследования, включающего проведение опросов и последующий качественный и количественный анализ результатов. Некоторые современные методы исследования доверия, преимущественно бази-

рующиеся на различных формах интервьюирования, представлены также в работе [8].

Несмотря на то, что усредненное определение доверия, получающееся при таком подходе, неизбежно имеет субъективный характер, создается впечатление, что построение универсального или хотя бы широко признанного определения неявно признается необходимой предпосылкой для разработки методов практического управления доверием. При отсутствии прогресса в разработке такого определения практические методы управления доверием исследователями практически не рассматриваются.

В настоящей статье применен противоположный подход. Мы считаем, что практическое управление доверием необходимо и возможно, даже если нет полного понимания природы доверия. Речь дальше пойдет только о внутриорганизационном доверии. Этот вид доверия относительно хорошо изучен [9–14], разработано множество разнообразных метрик для измерения доверия в организациях [7], предложено понятие гражданского организационного поведения (*organizational citizenship behavior*), исследованы поведенческие паттерны, влияющие на внутриорганизационное доверие. В то же время попытки сформулировать универсальное определение внутриорганизационного доверия пока не увенчались успехом, более того, разнообразие определений только растёт [7].

В литературе есть лишь несколько публикаций, посвященных доверию в сфере ИТ (например, [15]). Как правило, они ограничиваются межорганизационными взаимодействиями, в частности, ИТ-аутсорсингом. Как будет показано ниже, этот опыт, к сожалению, неприменим для внутренних провайдеров ИТ-услуг в силу принципиальных различий между внешним и внутренним рынками ИТ-услуг.

Наконец, важно отметить, что внутриорганизационным доверием заинтересовались коммерческие организации, предлагающие практические услуги по построению, поддержанию и измерению доверия в организациях [16, 17]. Это говорит о растущем значении внутриорганизационного доверия для развития организаций.

1. Цель работы и постановка задачи

Статья преследует двоякую цель. Во-первых, мы предлагаем практический метод управления доверием для конкретной ситуации взаимодействия внутреннего ИТ-провайдера и его бизнес-клиентов. Во-вторых, мы описываем количественный (но не эмпирический) подход к описанию доверия в этом частном случае. В основе данного подхода лежит представление о том, что каждая организация должна разработать и применять собственное индивидуальное определение доверия, которое в наибольшей степени удовлетворяет ее требованиям.

Это определение далее называется моделью внутриорганизационного доверия. Мы считаем, что общее определение доверия может возникнуть только вследствие обобщения опыта, накопленного многими организациями. Что же касается модели внутриорганизационного доверия, то это индивидуальный инструмент, имеющий вид структуры данных, которая помогает сотрудникам ИТ-организации выстраивать отношения доверия с клиентами и количественно оценивать результат.

Важно подчеркнуть, что внутриорганизационное доверие не может рассматриваться как результат выполнения формально определенных бизнес-процессов, поскольку как само доверие, так и деятельность по его построению в большой (если не в решающей) степени зависят от личных качеств сотрудников организации.

Сформулируем общие предположения и ограничения, на которых базируется предлагаемый подход.

1. Задача построения доверия решается только применительно к организационным ролям, поведение которых определяется общими организационными политиками, корпоративными правилами и организационной культурой (в отличие от поведения свободных индивидуумов).

2. Необходимость в доверии возникает тогда, когда взаимодействующие роли не могут объективно оценить деятельность друг друга.

3. У каждой роли есть собственное представление о том, как достигать взаимного доверия с взаимодействующей с ней ролью. Эти представления у разных ролей, в общем случае, различны.

Выбор в качестве объекта изучения практики построения доверия между ИТ-организацией и ее клиентами представляется актуальным, по меньшей мере, по двум причинам. Во-первых, в отсутствие методики объективного и строгого обоснования ИТ-инвестиций нужен общий консенсус для приня-

тия управленческих инвестиционных решений. Достаточно высокий средний уровень внутриорганизационного доверия к ИТ-организации со стороны ее клиентов, включая руководство организации, может послужить основой такого консенсуса.

Во-вторых, специфика деятельности внутренней ИТ-организации такова, что неспециалист в области ИТ часто не может оценить качество и смысл ее работы. Рассматривая внутреннюю ИТ-организацию как провайдера ИТ-услуг, мы исходим из того, что ее клиенты далеко не всегда могут контролировать качество ИТ-услуг, даже располагая информацией о процессах их создания и предоставления. Доверие к ИТ-организации со стороны конкретного клиента может в определенной мере компенсировать недостаток у него необходимой ИТ-квалификации.

Конечно, можно считать, что другие структурные подразделения также оказывают услуги своим клиентам (хотя это не очень распространенный взгляд на организацию). Рассмотрим, например, бухгалтерию или отдел кадров. Их услуги, как правило, понятны пользователям-неспециалистам, а процессы оказания этих услуг в основном законодательно регламентированы. Поэтому для недоверия к услугам этих подразделений формальных оснований нет. Если же рассмотреть подразделения, оказывающие сложные индивидуальные услуги (например, техническую дирекцию на производстве), то их пользователи и клиенты (производственные и смежные с ними структуры) обычно располагают специалистами, хорошо разбирающимися в деятельности технической дирекции и способными объективно оценить качество ее услуг.

ИТ-услуги отличаются тем, что они, с одной стороны, затрагивают практически всех сотрудников организации и, с другой стороны, слишком сложны для того, чтобы бизнес-клиенты и пользователи, не являющиеся специалистами в ИТ, могли объективно оценить, насколько добросовестно работает ИТ-организация.

Стратегическая важность доверия для ИТ-организации была рассмотрена в статье [8]. В настоящей статье описывается операционная деятельность, обеспечивающая постоянную поддержку приемлемого уровня доверия между провайдером ИТ-услуг и его клиентами. Далее предполагается, что внутренний провайдер в своей деятельности придерживается принципов ITSM, в частности, заключает с клиентами соглашения об уровне обслуживания.

Далее будут использоваться следующие термины:

◆ **ИТ-организация** – внутренняя ИТ-функция организации, независимо от организационной формы (например, ИТ-департамент, группа ИТ-департаментов или даже отдельное юридическое лицо);

◆ **внутренний провайдер ИТ-услуг** – синоним ИТ-организации;

◆ **построение доверия** – деятельность ИТ-организации, направленная на достижение доверия со стороны конкретного клиента.

2. ИТ-организация и внутренний рынок ИТ-услуг

Следуя [19], будем различать заказчиков услуг и пользователей услуг ИТ-организации. Можно выделить, как минимум, четыре группы клиентов и пользователей, которые получают ИТ-услуги:

◆ **участники бизнес-процессов, использующие ИТ в ходе своей повседневной деятельности.** Это пользователи ИТ-услуг. Заказчиком таких услуг обычно является один из менеджеров, отвечающий за взаимодействие с ИТ-организацией от имени некоторого структурного подразделения или бизнес-организации в целом;

◆ **владельцы и менеджеры бизнес-процессов, заинтересованные в улучшении своих бизнес-процессов с помощью ИТ.** Типичная услуга для этой категории клиентов – автоматизация бизнес-процессов;

◆ **топ-менеджеры и руководители.** ИТ-услуги для этих клиентов включают, например, реализацию систем масштаба организации, таких как ERP-системы или системы управления мастер-данными, а также оптимизацию ИТ-бюджета, повышение эффективности ИТ-организации или обеспечение надлежащего уровня информационной безопасности;

◆ **акционеры и инвесторы.** ИТ-услуги для этой категории клиентов могут быть направлены на повышение отдачи от инвестиций в ИТ (использование лучших практик и проверенных решений, привлечение надежных и квалифицированных внешних подрядчиков и т.д.).

Некоторые владельцы бизнес-процессов в организационной иерархии могут занимать должности функциональных руководителей. Например, владелец бизнес-процесса закупок обычно является руководителем департамента закупок, владелец бизнес-процесса бюджетирования – руководителем бюджетного или финансового департамента и так далее.

Что касается внутреннего рынка в целом, следует отметить следующие его принципиальные отличия от свободного рынка:

◆ внутренняя ИТ-организация фактически является монополистом на внутреннем рынке, обладая исчерпывающей информацией о потребностях и ожиданиях бизнес-клиентов. Она определяет требования к внешним провайдерам ИТ-услуг. С другой стороны, ИТ-организация не может игнорировать запросы на ИТ-услуги, сформированные бизнес-клиентами;

◆ клиенты на свободных рынках могут привлекать разных провайдеров ИТ-услуг, каждый из которых предлагает услуги наивысшего качества в своей области. Клиенты на внутреннем рынке, напротив, вынуждены полагаться на единственного провайдера ИТ-услуг, который не может быть одинаково успешен во всех областях, не говоря уже о тех ИТ-услугах, которые возникнут в будущем;

◆ клиенты на свободном рынке могут использовать коммерческий договор в качестве инструмента управления взаимоотношениями с провайдером. На внутреннем рынке соглашение об уровне обслуживания таким инструментом служить не может, оно лишь фиксирует договоренности и взаимные обязательства.

Специфические условия внутреннего рынка порождают специфические отношения между ИТ-организацией и ее клиентами. Взаимное доверие может принести обоим сторонам ряд выгод, к числу которых, например, относятся:

◆ минимизация затрат на взаимный контроль;

◆ снижение внешних рисков за счет того, что проблемы решаются локально, без вмешательства со стороны вышестоящих руководителей;

◆ возможность использования долгосрочных форм взаимодействия, использующих, например, гибкие технологии или методы непредикативного управления.

Поскольку клиенты ИТ-организации – это сотрудники компании, а ИТ-организацию для них представляет ее руководитель, можно считать, что доверие между ИТ-организацией и ее клиентами – это разновидность межличностного доверия.

3. Измерение доверия и построение доверия

В фундаментальной обзорной статье [7] сформулированы важнейшие принципы измерения внутриорганизационного доверия. Прежде всего,

отмечается, что подавляющее большинство исследователей рассматривает внутриорганизационное доверие как многомерное понятие. Измерение доверия состоит в проведении опросов с помощью специально разработанных для разных ситуаций вопросников, включающих метрики доверия. Метрики – это утверждения, уточняющие свойства доверия или его измерения. Они распадаются на независимые группы, соответствующие разным измерениям доверия. Например, метрика может выглядеть так: «Мои коллеги, которые также взаимодействуют с моим контрагентом, считают его заслуживающим доверия». Восприятие метрик всегда субъективно, в результате чего требуется усреднение, позволяющее точно определить, что именно группа опрошенных понимает под конкретным измерением доверия. По существу, то, что называется измерением доверия, представляет собой процесс построения его согласованного определения. Работ, посвященных измерению в традиционном смысле (т.е. количественной оценке внутриорганизационного доверия) авторами работы [7] выявлено не было (хотя такие работы существуют в области межорганизационного доверия, например, [16]). Наконец, в статье констатируется огромное разнообразие метрик в литературе, причем практика повторного применения метрик другими исследователями (отличными от их авторов) практически отсутствует.

В работе [7] выявлено пять категорий доверия, метрики для которых наиболее точно определены и приняты рядом исследователей. Эти разновидности соответствуют пяти разным постановкам задачи изучения доверия. Две из них описывают межличностное доверие [20, 21], одна – доверие между структурными подразделениями и другими рабочими группами [22], еще одна – доверие между подчиненным и руководителем. Последняя категория рассматривает доверие как психологическое состояние, подразумевающее стремление добровольно принять уязвимое положение по отношению к субъекту, в отношении которого имеются позитивные ожидания. Для наших целей наиболее интересны две первые категории. Между ними есть существенная разница.

Первая категория [20] рассматривает доверие как двумерный объект, включающий так называемое когнитивное доверие (cognition-based trust) и эмоциональное доверие (affect-based trust). Соответствующие группы метрик описывают восприятие доверяющим способности того, кому доверяют, достигать ожидаемого результата, а также уверенность в эмоциональ-

ной поддержке, сочувствии и готовности помочь.

Вторая категория [21] включает четыре измерения. Это взаимная информационная открытость, взаимное стремление к неформальным отношениям, взаимный контроль (surveillance) и взаимная координация взаимосвязанных работ.

Применительно к доверию между ИТ-организацией и ее клиентами можно объединить обе категории в одну, включающую все перечисленные измерения, кроме эмоционального доверия.

Все сказанное выше создает предпосылки для перехода к главной задаче настоящего исследования – разработке подхода к практическому построению доверия между ИТ-организацией и ее клиентами. Поскольку ИТ-организация не может влиять на поведение клиентов, задача сводится к определению того, что ИТ-организации может сделать со своей стороны, чтобы достичь доверия со стороны клиентов. Поэтому дальше мы будем говорить об информационной открытости, стремлении к неформальным отношениям, контролю и координации работ только со стороны ИТ-организации. Кроме того, ИТ-организация должна управлять когнитивным доверием клиентов. Мы исходим из того, что ИТ-организация может придерживаться единых методов построения доверия для всех своих клиентов.

На основании метрик, приведенных в работе [7], для взаимодействия ИТ-организации и ее клиентов мы определили количественные метрики, представленные в *таблице 1*. Этот набор количественных метрик не претендует на полноту, а только иллюстрирует саму возможность их построения.

Наша главная идея состоит в том, что доверие клиента всегда складывается из двух компонентов: 1) его собственного доверия, вызванного текущим и предыдущим опытом и/или персональной склонностью к доверию, и 2) влияния его окружения. Метрики, выражающие влияние окружения, приведены в *таблице 1* курсивом. Мы не анализируем индивидуальное поведение клиентов, лишь предполагая, что приведенные метрики помогают клиенту сформировать свое восприятие ИТ-организации и, в конечном счете, повысить уровень доверия к ней. Влияние окружения важно, потому что причины низких значений некоторых метрик (например, качества услуг ИТ-организации или величин рисков) не могут быть объективно оценены неспециалистами в ИТ. В таком случае мы предполагаем, что клиенты ориентируются на мнение об ИТ-организации, существующее в их окружении.

Таблица 1.

Количественные метрики для построения доверия между ИТ-организацией и ее клиентами

Измерение доверия	Метрика	Способ измерения
Когнитивное доверие	Качество ИТ-услуг	Количество нарушений SLA
	Удовлетворенность предшествующим опытом	Процент продленных SLA
	<i>Процент клиентов, удовлетворенных опытом и качеством ИТ-услуг</i>	<i>Оценка доли удовлетворенных клиентов</i>
Информационная открытость	Готовность делиться информацией	Количество нарушений договоренностей о предоставлении информации
Неформальные отношения	Понимание клиентом уровня строгости системных требований в SLA	Процент выявленных и согласованных с клиентом рисков
	Понимание клиентом требований к срокам и трудоемкости работ	Процент других клиентов, с которыми согласован план работ ИТ-организации
	<i>Процент клиентов, стремящихся к неформальным отношениям с ИТ-организацией</i>	<i>Оценка доли таких клиентов</i>
Контроль	Клиентские затраты на контроль сроков и объема выполненных работ	Анализ информации, полученной от клиента
	Клиентские затраты на контроль качества	Профиль отклонений по затратам для работ в плане качества
	<i>Процент клиентов, стремящихся снизить затраты на контроль</i>	<i>Оценка доли таких клиентов</i>
Координация взаимосвязанных работ	Процент обоснованно отклоненных внеплановых изменений со стороны клиента	Процент отклоненных изменений, согласованных с другими клиентами, присутствующими в плане работ ИТ-организации
	Количество внеплановых изменений со стороны ИТ-организации, не связанных с другими клиентами	Анализ внутренней документации ИТ-организации
	<i>Процент клиентов, удовлетворенных координацией работ с ИТ-организацией</i>	<i>Оценка доли таких клиентов</i>

Как именно клиент воспринимает информацию, полученную от окружения, зависит от его индивидуальных характеристик, например, склонности доверять коллегам, уровня ИТ-квалификации, желания/нежелания тратить ресурсы на контроль и т.п. Во всяком случае, ИТ-организация должна учитывать фактор окружения и, по возможности, управлять им. Иными словами, это означает, что ИТ-организация должна знать структуру коммуникаций в организации и, по возможности, учитывать ее в своей деятельности.

Все сказанное выше наводит на мысль о том, что природа внутриорганизационного доверия в каждой организации глубоко индивидуальна и зависит, в частности, от уникальной структуры межличностного доверия между клиентами внутреннего ИТ-провайдера (и другими сотрудниками организации). Более того, структура межличностного доверия изменяется во времени, как и поведение каждого клиента. Это ставит под сомнение возможность и целесообразность построения усредненного определения доверия в организации.

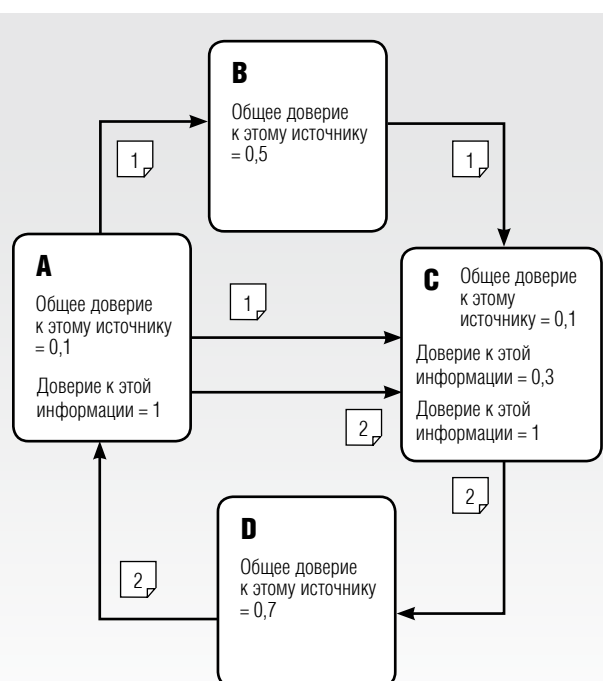


Рис. 1. Пример структуры межличностного доверия в организации

Сказанное иллюстрируется примером структуры межличностного доверия, представленной на *рисунке 1*.

На *рисунке 1* прямоугольниками представлены четыре субъекта окружения (А–D), стрелками показаны направления передачи информации. В частности, от А к С передается информация двух видов, например, об удовлетворенности качеством ИТ-услуг (1) и о стремлении к неформальным отношениям с ИТ-организацией (2). Внутри прямоугольников указаны уровни доверия как к передаваемой информации, так и к источнику в целом. Структура описывает не конкретную ситуацию обмена информацией, а все потенциальные направления такого обмена в общем случае, т.е. исторически сложившиеся информационные потоки между клиентами.

В каждый момент времени уровень доверия каждого клиента может зависеть от следующих факторов:

- ◆ личного восприятия каждым клиентом его текущих взаимоотношений с ИТ-организацией;
- ◆ метода оценки информации, поступающей от окружения;
- ◆ состояния окружения на данный момент.

В качестве примера рассмотрим ситуацию, когда клиент С запрашивает мнения о качестве ИТ-услуг у клиентов А и В, которым он доверяет. Вообще говоря, неизвестно, обращался ли уже клиент В с аналогичной просьбой к клиенту А. Если это так, то клиент С получит от В информацию, на которую уже повлиял А, а если нет, то мнение В будет независимым (никаких указаний на этот счет структура, представленная на *рисунке 1*, не дает). Затем С каким-то образом корректирует свое восприятие ИТ-организации с учетом полученной информации. Например, он может повысить собственную оценку ИТ-организации, если взвешенная сумма полученных мнений сравнима с его личной оценкой, либо пренебречь мнениями окружающих, если эта взвешенная сумма мала. Каким именно способом действует клиент в каждый момент времени, точно утверждать невозможно.

Несмотря на то, что результат оперативного взаимодействия клиентов остается во многом неопределенным, рассмотренная структура позволяет ИТ-организации понять, кто из клиентов способен оказать наибольшее влияние на остальных, каковы риски снижения качества ИТ-услуг для конкретного клиента, какие группы доверяющих друг другу клиентов существуют в организации и т.п.

Эта информация может оказаться полезной для внутреннего ИТ-провайдера даже если структура в

целом настолько сложна, что не позволяет проанализировать поведение каждого клиента в отдельности. С другой стороны, наблюдая за закономерностями или повторяющимися паттернами поведения клиентов, можно попытаться учесть их в описании структуры внутриорганизационного межличностного доверия.

Назовем эту структуру моделью внутриорганизационного доверия. Эта модель не является универсальной, она адекватна только для случая построения доверия между ИТ-организацией и ее клиентами.

4. Управление построением доверия и совершенствование модели доверия

Приведенные выше соображения, конечно же, нуждаются в валидации, основанной на практическом опыте. Опыт накапливается в результате выполнения ИТ-организацией активностей, направленных на завоевание доверия клиента. Отметим, что эти активности не могут быть смоделированы обычными бизнес-процессами, по крайней мере, по двум причинам. Во-первых, для достижения доверия может оказаться важным участие конкретных людей, что не позволяет моделировать соответствующую деятельность традиционным бизнес-процессом. Во-вторых, неясно, повлияет ли эта деятельность на доверие клиента, т.е., будет ли получен реальный выход.

Также маловероятно, что существуют лучшие практики достижения доверия. Об этом косвенно говорит отсутствие универсального определения доверия. Все это, тем не менее, не означает, что ИТ-организация не может продуктивно добиваться доверия со стороны клиентов.

Деятельность по валидации и совершенствованию описанной выше модели доверия можно организовать по аналогии с тем, как деятельность по совершенствованию производственного процесса организуется в модели СММИ [23–25]. Для этого достаточно заменить в СММИ for Services [24] совокупность процессных областей моделью доверия. Аналогично процессным областям, эта структура уточняется и стандартизируется по мере продвижения ИТ-организации по уровням зрелости. Подобно тому, как набор процессных моделей на каждом уровне описывает степень институционализации бизнес-процессов организации, наша модель будет описывать текущее представление о доверии клиентов. Иными словами, точность, полнота и степень использования ИТ-специалистами и ИТ-менеджерами модели доверия будет характеристикой уровня зрелости ИТ-

организации. Заметим, что стремление к повышению традиционной зрелости, основанной на возможностях процессных областей, не соответствует ситуации, в которой находится ИТ-организация. При отсутствии возможности раз и навсегда сфокусироваться на определенных услугах ИТ-организации просто нет смысла совершенствовать какие-то определенные группы процессов. Совершенствование модели доверия, напротив, позволяет ИТ-провайдеру более точно соответствовать ситуации в организации, независимо от конкретного набора клиентов и ИТ-услуг.

Краткое описание соответствующих уровней зрелости ИТ-организации приведено ниже. Важно подчеркнуть, что модель зрелости, в отличие от модели процессных областей CMMI for Services, не является предопределенной заранее и для каждой организации должна разрабатываться индивидуально.

Уровни зрелости, описанные ниже, предназначены только для того, чтобы дать специалистам-практикам общее представление о том, как можно использовать подход, основанный на оценке зрелости, для улучшения деятельности по построению доверия со стороны ИТ-организации. Можно выделить следующие уровни зрелости:

◆ **незавершенный:** необходимость построения доверия не осознается ИТ-организацией. Активности, направленные на достижение доверия, выполняются нерегулярно и могут быть незаконченными;

◆ **начальный:** в ИТ-организации есть общее понимание необходимости достижения доверия клиента. Разные специалисты-практики достигают доверия клиентов по-разному. Факт повышения или понижения доверия объективно устанавливается по формальным признакам. Никакого согласия о том, как нужно достигать доверия, не существует, т.е. общая модель доверия отсутствует;

◆ **управляемый:** ИТ-организация располагает несколькими апробированными практиками достижения доверия со стороны части клиентов. Установлены межличностные доверительные отношения между этими клиентами и конкретными ИТ-специалистами. Существуют внутренние правила и политики, касающиеся построения доверия, которых придерживаются все менеджеры по клиентам в ИТ-организации. Для достижения доверия со стороны отдельных клиентов используются элементы модели доверия;

◆ **определенный:** в ИТ-организации имеется единый взгляд на то, как нужно достигать доверия со стороны всех клиентов, т.е. стандартная общая модель

доверия. Определены правила, позволяющие адаптировать модель для конкретного клиента или группы клиентов.

Как уже было отмечено, для использования модели доверия необходимо оценивать индивидуальное доверие каждого клиента в каждый момент времени. Естественно, техника опроса для этого применяться не может. Тем не менее, существуют косвенные признаки повышения или понижения доверия, которые можно объективно наблюдать и использовать. К ним относятся, например, следующие события:

◆ изменение соглашения об уровне обслуживания в сторону смягчения или ужесточения контроля со стороны клиента;

◆ снижение или рост количества эскалаций проблем во взаимоотношениях между клиентом и ИТ-организацией вверх по управленческой иерархии;

◆ снижение или рост объема затрат на взаимный контроль;

◆ рост или снижение количества изменений со стороны клиента без перезаключения SLA;

◆ отказ клиента от сотрудничества с определенными ИТ-специалистами.

Разумеется, важнейшим неформальным способом выяснения уровня доверия со стороны клиента является использование межличностного доверия между менеджером по клиенту и самим клиентом.

На управляемом уровне ИТ-организация учитывает доверительные отношения между некоторыми конкретными клиентами, и методы взаимодействия с этими клиентами обязательно учитывают эти отношения. В то же время доверие между клиентом и соответствующим менеджером со стороны ИТ-организации по-прежнему играет существенную роль для выяснения уровня доверия клиента.

На определенном уровне ИТ-организация ориентируется не на построение доверия со стороны конкретного клиента, а на достижение доверия со стороны всех существующих и отчасти потенциальных клиентов. Для этого она использует общую модель внутриорганизационного доверия, где учитываются все взаимосвязи между ее клиентами.

Пытаться описывать более высокие уровни зрелости в настоящее время не имеет смысла. Необходимо накопить достаточный опыт работы с моделями доверия, чтобы можно было говорить о методах их измерения или улучшения.

В условиях отсутствия формальных бизнес-процессов модель доверия позволяет фиксировать, форма-

лизываться и анализировать результаты сложных и, зачастую, неформальных активностей, направленных на достижение доверия.

Конкретная реализация модели доверия может варьироваться от простейшей совокупности файлов до комплексной модели данных, контролируемой и сопровождаемой с использованием формальных бизнес-процессов.

Заключение

Подход, представленный в настоящей статье, представляет собой лишь первый шаг к практическому управлению доверием в ИТ-организации. Основным его результатом является демонстрация возможности практического построения доверия между ИТ-организацией и ее клиентами даже в отсутствие об-

щего определения внутриорганизационного доверия.

Дальнейшие шаги могут сделать только ИТ-специалисты, ответственные за управление доверием в ИТ-организациях. Поэтому представляется очень важной задачей получить обратную связь от менеджеров по клиентам, пресейл-менеджеров и других специалистов, вовлеченных во взаимодействие с клиентами. Для этого нужно проделать значительную работу по разработке простых и эффективных инструментов для валидации описанного подхода.

Еще одна важная задача — экономическое обоснование управления доверием. Хотя выгоды от достижения доверия представляются очевидными, обеспечение баланса между этими выгодами и затратами на повседневную деятельность по достижению доверия, представляет собой сложную задачу. ■

Литература

1. Paliszkiwicz J. Trust management: Literature review // *Management*. 2011. Vol. 6. No 4. P. 315–331.
2. Feltman C. *The thin book of trust: An essential primer for building trust at work*. Bend: Thin Book, 2008.
3. Paliszkiwicz J. Inter-organizational trust: Conceptualization and measurement // *International Journal of Performance Measurement*. 2011. Vol. 1. P. 15–28.
4. Kramer R., Tyler T. *Trust in organizations: Frontiers of theory and research*. Sage Publications, 1996.
5. Muhl J.K. *Organizational trust: Measurement, impact and the role of management accountants*. Springer, 2014.
6. Shaw R.B. *Trust in the balance: Building successful organizations on results, integrity, and concern*. San Francisco: Jossey-Bass, 1997.
7. McEvily B., Tortoriello M. Measuring trust in organisational research: Review and recommendations // *Journal of Trust Research*. 2011. Vol. 1. No 1. P. 23–63.
8. Lyon F., Mollering G., Saunders M. (eds.) *Handbook of research methods on trust*. Edward Elgar, 2015.
9. Zaheer A., McEvily B., Perrone V. Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance // *Organization Science*. 1998. Vol. 9. No 2. P. 141–159.
10. Vangen S., Huxham C. Nurturing collaborative relations // *Journal of Applied Behavioral Science*. 2003. Vol. 39. No 1. P. 5–31.
11. Fulmer A., Dirks K. Multilevel trust: A theoretical and practical imperative // *Journal of Trust Research*. 2018. Vol. 8. No 2. P. 137–141.
12. Dar O.L. Trust in co-workers and employee behaviours at work // *International Review of Business Research Papers*. 2010. Vol. 6. No 1. P. 194–204.
13. Paille P., Bourdeau L., Galois I. Support, trust, satisfaction, intent to leave and citizenship at organizational level. A social exchange approach // *International Journal of Organizational Analysis*. 2010. Vol. 18. No 1. P. 41–58.
14. Fulmer A., Gelfand M.J. At what level (and in whom) we trust: Trust across multiple organizational levels // *Journal of Management*. 2012. Vol. 38. No 4. P. 1167–1230.
15. Ali Babar M., Verner J.M., Nguyen P.T. Establishing and maintaining trust in software outsourcing relationships: An empirical investigation // *Journal of Systems and Software*. 2007. No 80. P. 1438–1449.
16. Paine K.D. *Guidelines for measuring trust in organizations*. Gainesville, FL: Institute for Public Relations, University of Florida, 2013.
17. *Building trust. The critical link to a high-involvement, high-energy workplace begins with a common language*. The Ken Blanchard Companies, 2017. [Электронный ресурс]: <https://www.connexpartners.com/hubfs/assets/Building%20Trust.pdf> (дата обращения 15.02.2019).
18. Biryukov A.N. Strategic management in the IT department // *Business Informatics*. 2017. No 2. P. 17–24.
19. *ITIL Service Strategy*, 2011 edition. London, UK: The Stationery Office, 2011.
20. McAlister D.J. Affect and cognition-based trust as foundation for interpersonal cooperation in organizations // *Academy of Management Journal*. 1995. Vol. 38. No 1. P. 24–59.
21. Cural S.C., Judge T.A. Measuring trust between organizational boundary role persons // *Organizational Behavior and Human Decision Processes*. 1995. Vol. 64. No 2. P. 151–170.
22. Cummings L.L., Bromiley P. The organizational trust inventory (OTI): Development and validation // *Trust in organizations: Frontiers of theory and research* / R.M. Kramer, T.R. Tyler (eds.). Thousand Oaks, CA: Sage Publications, 1996. P. 302–330.
23. CMMI for Development, Version 1.3. CMMI Product Team. *Improving processes for developing better products and services*. Technical Report. CMU/SEI-2010-TR-033. ESC-TR-2010-033. Pittsburgh, PA: Carnegie Mellon University, 2010.

24. CMMI for Services, Version 1.3. CMMI Product Team. Improving processes for developing better products and services. Technical Report. CMU/SEI-2010-TR-034. ESC-TR-2010-034. Pittsburgh, PA: Carnegie Mellon University, 2010.
25. CMMI for Acquisitions, Version 1.3. CMMI Product Team. Improving processes for developing better products and services. Technical Report. CMU/SEI-2010-TR-032. ESC-TR-2010-032. Pittsburgh, PA: Carnegie Mellon University, 2010.

Об авторе

Бирюков Александр Николаевич

кандидат физико-математических наук;

доцент кафедры бизнес-информатики, Финансовый университет при Правительстве РФ,

125993, г. Москва, Ленинградский пр-т, д. 49;

E-mail: anbiryukov@fa.ru

How can an IT organization earn its customers' trust: A practical approach

Alexander N. Biryukov

E-mail: anbiryukov@fa.ru

Financial University under the Government of the Russian Federation
Address: 49, Leningradskiy Prospect, Moscow 125993, Russia

Abstract

The paper describes a practical approach which can be used by internal IT organizations to gain their business customers' trust. The variety of customers of the internal IT service provider is limited to internal customers only. The distinguishing feature of the proposed approach is that it is completely practice-oriented, i.e. primarily aimed at building trust among IT service providers and their customers in a particular organization. The approach is based on the idea that there are measurable prerequisites for the emergence of a customer's trust which allow you to partially formalize the IT organization's intention to earn its customers' trust. A model of intra-organizational trust is proposed; it is progressively improved as the IT organization develops its trust-building capabilities. The model comprises all IT service customers in an organization along with their communications and accounts for internal organizational IT service market specifics. A high-level blueprint of the trust model is described which can serve as a starting point when developing a full-scale trust model in a particular IT organization. We present an approach to the trust model improvement which builds upon principles adopted from widely recognized CMMI model. With this approach, an internal IT service provider can benefit from maturity assessment methods to improve its trust building capabilities.

Key words: IT service provider; internal IT service market; trust; IT organization; trust criteria; intra-organizational trust model; trust management; earning trust; maturity; capability level.

Citation: Biryukov A.N. (2019) How can an IT organization earn its customers' trust: A practical approach. *Business Informatics*, vol. 13, no 3, pp. 67–77. DOI: 10.17323/1998-0663.2019.3.67.77

References

1. Paliszkiwicz J. (2011) Trust management: Literature review. *Management*, vol. 6, no 4, pp. 315–331.
2. Feltman C. (2008) *The thin book of trust: An essential primer for building trust at work*. Bend: Thin Book.
3. Paliszkiwicz J. (2011) Inter-organizational trust: Conceptualization and measurement. *International Journal of Performance Measurement*, vol. 1, pp. 15–28.

4. Kramer R., Tyler T. (1996) *Trust in organizations: Frontiers of theory and research*. Sage Publications.
5. Muhl J.K. (2014) *Organizational trust: Measurement, impact and the role of management accountants*. Springer.
6. Shaw R.B. (1997) *Trust in the balance: Building successful organizations on results, integrity, and concern*. San Francisco: Jossey-Bass.
7. McEvily B., Tortoriello M. (2011) Measuring trust in organisational research: Review and recommendations. *Journal of Trust Research*, vol. 1, no 1, pp. 23–63.
8. Lyon F., Mollering G., Saunders M. (eds.) (2015) *Handbook of research methods on trust*. Edward Elgar.
9. Zaheer A., McEvily B., Perrone V. (1998) Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science*, vol. 9, no 2, pp. 141–159.
10. Vangen S., Huxham C. (2003) Nurturing collaborative relations. *Journal of Applied Behavioral Science*, vol. 39, no 1, pp. 5–31.
11. Fulmer A., Dirks K. (2018) Multilevel trust: A theoretical and practical imperative. *Journal of Trust Research*, vol. 8, no 2, pp. 137–141.
12. Dar O.L. (2010) Trust in co-workers and employee behaviours at work. *International Review of Business Research Papers*, vol. 6, no 1, pp. 194–204.
13. Paille P., Bourdeau L., Galois I. (2010) Support, trust, satisfaction, intent to leave and citizenship at organizational level. A social exchange approach. *International Journal of Organizational Analysis*, vol. 18, no 1, pp. 41–58.
14. Fulmer A., Gelfand M.J. (2012) At what level (and in whom) we trust: Trust across multiple organizational levels. *Journal of Management*, vol. 38, no 4, pp. 1167–1230.
15. Ali Babar M., Verner J.M., Nguyen P.T. (2007) Establishing and maintaining trust in software outsourcing relationships: An empirical investigation. *Journal of Systems and Software*, no 80, pp. 1438–1449.
16. Paine K.D. (2013) *Guidelines for measuring trust in organizations*. Gainesville, FL: Institute for Public Relations, University of Florida.
17. The Ken Blanchard Companies (2017) *Building trust. The critical link to a high-involvement, high-energy workplace begins with a common language*. Available at: <https://www.connexpartners.com/hubfs/assets/Building%20Trust.pdf> (accessed 15 February 2019).
18. Biryukov A.N. (2017) Strategic management in the IT department. *Business Informatics*, no 2, pp. 17–24.
19. The Stationery Office (2011) *ITIL Service Strategy, 2011 edition*. London, UK: The Stationery Office.
20. McAlister D.J. (1995) Affect and cognition-based trust as foundation for interpersonal cooperation in organizations. *Academy of Management Journal*, vol. 38, no 1, pp. 24–59.
21. Cural S.C., Judge T.A. (1995) Measuring trust between organizational boundary role persons. *Organizational Behavior and Human Decision Processes*, vol. 64, no 2, pp. 151–170.
22. Cummings L.L., Bromiley P. (1996) The organizational trust inventory (OTI): Development and validation. *Trust in organizations: Frontiers of theory and research*. Thousand Oaks, CA: Sage Publications, pp. 302–330.
23. Carnegie Mellon University (2010) *CMMI for Development, Version 1.3. CMMI Product Team. Improving processes for developing better products and services. Technical Report. CMU/SEI-2010-TR-033. ESC-TR-2010-033*. Pittsburgh, PA: Carnegie Mellon University.
24. Carnegie Mellon University (2010) *CMMI for Services, Version 1.3. CMMI Product Team. Improving processes for developing better products and services. Technical Report. CMU/SEI-2010-TR-034. ESC-TR-2010-034*. Pittsburgh, PA: Carnegie Mellon University.
25. Carnegie Mellon University (2010) *CMMI for Acquisitions, Version 1.3. CMMI Product Team. Improving processes for developing better products and services. Technical Report. CMU/SEI-2010-TR-032. ESC-TR-2010-032*. Pittsburgh, PA: Carnegie Mellon University.

About the author

Alexander N. Biryukov

Cand. Sci. (Phys.-Math.);

Associate Professor, Department of Business Informatics, Financial University under the Government of the Russian Federation, 49, Leningradskiy Prospect, Moscow 125993, Russia;

E-mail: anbiryukov@fa.ru