

Архитектура информационной системы, оценка рисков и совокупная стоимость владения

Николай Михайловский

В последнее время все больше директоров информационных служб понимают, что архитектура информационной системы должна выбираться с учетом нужд бизнеса, а не личных пристрастий разработчиков. Данная статья предлагает методику выбора архитектуры информационной системы исходя из минимизации совокупной стоимости владения и анализа рисков.

Некоторое время назад нам довелось выполнять консалтинговый проект по разработке архитектуры достаточно крупной и нетривиальной информационной системы. И если вопрос построения архитектур-кандидатов казался более или менее очевидным (в конце концов, существует несколько содержательных и весьма различных методик построения архитектур, некоторые из них будут названы далее), то вопрос выбора архитектуры из кандидатов, как оказалось, не столь проработан. В данной статье излагается метод выбора архитектуры информационной системы (ИС¹), к которому мы пришли в результате реализации двух аналогичных проектов и основные идеи которого могут быть сформулированы в двух тезисах.

1. В проектах построения информационных систем, для которых важен экономический эффект, должна выбираться архитектура системы с минимальной совокупной стоимостью владения.

2. Совокупная стоимость владения информационной системой состоит из плановых затрат и стоимости рисков. Стоимость рисков определяется стоимостью бизнес-рисков, вероятностями технических рисков и матрицей соответствия между ними. Матрица соответствия определяется архитектурой информационной системы.

Если первый тезис может быть для кого-то открытием, вероятно, только в силу значительной «паранормальности» многих российских проектов ИС, то второй впервые сформулирован, по-видимому, здесь. С другой стороны, подобные предлагаемой в данной статье, хотя и менее детальные методики, уже некоторое время известны. Так, например, в [6] совокупная стоимость владения серверными кластерами определяется как сумма затрат на их приобретение, стоимости серверов, эксплуатационных затрат и стоимости потерь от простоев. Последняя как раз и соответствует стоимости рисков в нашем понимании.

Что такое архитектура ИС и инфраструктура ИС

Архитектура — это то, за что увольняют системного архитектора и руководителя проекта. (Кто-то может сказать, что проекты на самом деле проваливаются из-за неправильной организации процесса разработки. Не отрицая этого, отмечу, что знаю гораздо больше успешных систем, построенных в кривом процессе разработки, чем успешных систем с кривой архитектурой.)

Между тем, слова «архитектура информационной системы» обычно довольно согласованно понимаются специалистами на уровне подсознания, и столь же несогласованно определяются². Два основных класса определений архитектур — определения «конструктивные» и «идеологические».

Основные идеологические определения архитектуры ИС таковы:

¹ Вероятно, перед этим следовало бы определить, что такое ИС... Будем надеяться, что читатель это интуитивно понимает. Намекнем лишь, что встроенное ПО роутеров, операционные системы, прикладные пакеты программ не являются ИС.

² На сайте SEI имеется специальный раздел, посвященный определениям архитектуры. Там их собрано более ста.

1. «Архитектура ИС — это набор решений, наиболее существенным образом влияющих на совокупную стоимость владения системой».
2. «Архитектура ИС — это набор ключевых решений, неизменных при изменении бизнес-технологии в рамках бизнес-видения».

Оба эти определения согласованы в том смысле, что если ключевое решение приходится изменять при изменении бизнес-технологии в рамках бизнес-видения, то резко возрастает стоимость владения системой. Следствием этих определений является понимание важности принятия архитектуры системы как стандарта предприятия, ввиду значимости архитектурных решений и их устойчивости по отношению к изменениям бизнес-технологии. Еще одно важное следствие первого определения — архитектура системы на самом деле должна строиться еще на стадии технико-экономического обоснования системы.

Конструктивно архитектура обычно определяется как набор ответов на следующие вопросы:

- что делает система;
- на какие части она разделяется;
- как эти части взаимодействуют;
- где эти части размещены³.

Таким образом, архитектура ИС является логическим построением, или моделью, и влияет на совокупную стоимость владения через набор связанных с ней решений по выбору средств реализации, СУБД, операционной платформы, телекоммуникационных средств и т. п. — то есть через то, что мы называем инфраструктурой ИС. Еще раз подчеркну, что инфраструктура включает решения не только по программному обеспечению, но и по аппаратному комплексу и организационному обеспечению. Это вполне соответствует пониманию системы в наиболее современных стандартах типа ISO/IEC 15288 [1].

Требования к методике выбора архитектуры ИС

По всей видимости, число проектов, в которых архитектура системы выбирается сознательно, относительно невелико (в отличие от архитектуры программного обеспечения, которая, в соответствии с нашими определениями, является только частью архитектуры системы). Естественно, архитектура будет наличествовать в любом случае, другое дело, что она может не конструироваться и не выбираться сознательно.

(А то, что выбор делать надо, указывается, например, в RUP [2], но, к сожалению, там не объясняется, как это делать!)

Более того, несмотря на то, что большинство методик разработки подчеркивают важность архитектуры (исключением является, пожалуй, XP), ни одна не дает внятной методики ее выбора. Причины такого положения кроются, как нам представляется, во-первых, в том, что фирменные методики навязывают с разной степенью настойчивости, фирменную же архитектуру и инфраструктуру (таковы, в частности, Oracle CDM и MSF), а XP фактически отрицает существование архитектуры, что может быть оправданно для некрупных проектов, выполняемых небольшой командой (1-3 пары программистов). А во-вторых, традиционные методики:

- а. не позволяют оценить качество разработанной архитектуры;
- б. ориентированы на архитектуру программной системы и не учитывают того факта, что система состоит не только из программных, но также и из технических средств и людей;

³ Этот список примерно соответствует архитектурным срезам (architectural views) RUP [2].

- в. разделяют процессы технико-экономического обоснования системы, разработки бизнес-процессов и разработки архитектуры системы;
- г. не учитывают бизнес-цели и цели использования системы.
- д. в результате осмысления имеющихся методик нами были сформулированы следующие требования к методике выбора архитектуры.

Методика должна:

- отражать связь архитектуры и совокупной стоимости владения;
- связывать разработку архитектуры, бизнес-анализ и технико-экономическое обоснование в едином процессе;
- отражать итерационную природу разработки ИС;
- иметь своей целью выбор архитектуры системы в целом, а не только ее программной составляющей.

Совокупная стоимость владения системой и риски

Как мы уже говорили, основным критерием выбора архитектуры и инфраструктуры ИС является минимизация совокупной стоимости владения системой. По крайней мере, такой критерий кажется естественным для коммерческих организаций, эффективность деятельности которых определяется по затратам и доходам.

К сожалению, интегральные затраты на систему могут быть полностью известны только после завершения проекта. До завершения проекта интегральные затраты могут быть только оценены (см. формульную оценку во врезке).

Отметим, что в предложенном методе оценки затрат использована величина Pt^{oc} — оценка потерь, связанных с бизнес-рисками в периоде t .

Конечно, мы будем использовать характеристики и чисто технических ИТ-рисков. Для того чтобы знать и правильно организовать описание всего набора возможных рисков полезно опираться на некую общую модель архитектуры как предприятия, так и его ИС. В качестве таких моделей могут применяться модели Захмана [3] или Зиндера [4].

По всей видимости, с каждой из ячеек этих моделей связаны свои специфические риски. А связи этих ячеек, предусмотренные неявно в [3] или явно в [4], позволяют, например, хорошо определять связи между техническими, операционными и бизнес-рисками, которые будут разбираться далее. Кроме того, наличие временной оси в модели [4] позволяет работать не со статической «фотографией» проекта или жизни системы, но учитывать их существование во времени (имеется в виду то самое время, которое «работает» в формульных оценках затрат, приведенных на врезке). Кроме того, наличие этой оси времени позволяет вычленять бизнес-риски типа «неопределенность» (см. ниже) при рассмотрении проекта в бизнес-времени и проектные риски при рассмотрении проекта в проектном времени.

Вопросы соответствия различных типов рисков ячейкам архитектурной модели [4] и их связям требуют дополнительной теоретической проработки. Однако и без нее тем, кто знаком с вышеуказанными моделями, нетрудно будет соотнести определенные ячейки архитектуры (architectural framework) с различными рисками и таким образом составить, назвать и описать актуальные для проекта/системы группы рисков. Мы же в рамках данной статьи выделим несколько наиболее значимых и принципиально различных типов рисков:

- проектные риски при создании системы;
- технические риски, состоящие в простоях, отказах, потере или искажении данных и т. п.;
- риски бизнес-потерь, связанные с эксплуатацией системы (возникающие, в конечном счете, из-за технических рисков). Такие риски бизнес-потерь назовем бизнес-рисками. Каждый бизнес-риск принадлежит, по крайней мере, одному

из вариантов бизнес-использования (business use case) системы. Например, для интернет-магазина бизнес-риски «Покупатель не может сделать заказ и уходит» и «Покупатель делает заказ, но уходит рассерженный функционированием системы» принадлежат вариантам бизнес-использования «Сделать заказ».

- риски бизнес-потерь, связанные с вариативностью бизнес-процессов. При этом потери происходят оттого, что:
 - а. бизнес-процессы надо изменять, а информационная система не готова к этому, и потери связаны с неоптимальным функционированием бизнеса;
 - б. приходится платить за модификацию системы.

Такие риски бизнес-потерь назовем неопределенностями (RUP упоминает аналогичные по смыслу «варианты изменения», change cases).

Затраты на создание и эксплуатацию системы с некоторой точностью оцениваются достаточно стандартно. Динамические же бизнес-риски количественно учесть невозможно, и их следует оценивать исключительно качественно (на уровне понимания, насколько бизнес-процессы в организации являются определенными/застывшими/неустоявшимися). Наиболее интересная часть совокупной стоимости владения системой - статические бизнес-риски и риски разработки.

Каждый вариант бизнес-использования реализуется с помощью набора операций соответствующих бизнес-процессов, а бизнес-риск возникает по причине неисполнения одной или нескольких операций. Такие риски мы называем операционными. Таким образом операционные риски являются источниками бизнес-рисков.

Например, источниками риска «Покупатель не может сделать заказ и уходит» могут быть операционный риск «Информация о заказе не может быть передана для обработки в систему».

В свою очередь операционные риски для автоматизированных операций могут возникать по причине технических рисков. Например, операционный риск «Информация о заказе не может быть передана для обработки в систему» может возникнуть по причине реализации технического риска «Обрыв канала связи».

С другой стороны, бизнес-риск может быть парирован соответствующей организацией процесса и/или архитектурным решением.

На основе вышесказанного получаем следующую методику выбора архитектуры ИС.

1. Проводится описание бизнес-процессов в организации с ограниченным уровнем детальности (как правило, не пооперационно). Описание бизнес-процесса должно включать его целевые нефункциональные характеристики (частоту возникновения, продолжительность и т. п.)⁴. Результатом данного этапа может стать набор вариантов использования (Use case view) описания архитектуры системы в смысле RUP.

2. На основе описания бизнес-процессов описываются бизнес-риски. Каждый бизнес-риск оценивается в терминах бизнес-потерь. Это описание является параметрическим — бизнес-потери могут зависеть от продолжительности действия риска, частоты его возникновения и т. п. (см. пример оценки бизнес-риска во врезке). Критерии качества описания статических бизнес-рисков:

- *уникальность оценок* — если два риска оцениваются по одной и той же формуле (возможно, с точностью до константы), то это два названия одного бизнес-риска;
- *одночленность* — если оценка бизнес-риска определяется как сумма многих слагаемых без общих членов, то на самом деле это несколько бизнес-рисков.

⁴ Такие характеристики обычно включаются в шаблоны типа business use cases [5]. Альтернативным вариантом является построение EDFD-диаграммы потоков данных, на которой указаны нефункциональные характеристики каждого потока данных.

Наш опыт показывает, что для достаточно крупных систем выявляется порядка 20-30 бизнес-рисков, из которых действительно архитектурно значимыми можно считать 7-10. Для каждого такого риска следует построить маленькую экономическую модель, позволяющую оценить величину риска в зависимости от параметров.

3. Определяются возможные вариации бизнес-процессов. На их основе описываются неопределенности (см., например, шаблон ?change cases? RUP).

4. На основе описания бизнес-процессов описываются архитектурно-значимые функциональные модули системы. Разделение функциональности системы по модулям осуществляется исходя из инвариантности относительно деталей реализации и физического размещения отдельных модулей. Описание каждого модуля включает функции и данные, объединяемые в данный модуль. Результатом данного этапа может стать разбиение (Logical view) описания архитектуры системы в смысле RUP.

5. Строятся архитектуры-кандидаты с учетом нефункциональных требований к системе и неопределенностей. Различные архитектуры-кандидаты реализуют один и тот же набор функций и функциональных модулей и отличаются только способами физического размещения и реализации этих модулей. Для каждой архитектуры-кандидата описываются:

- цели;
 - основные характеристики;
 - логическая структура (диаграмма развертывания);
 - физическая структура (схема сети);
 - взаимодействие модулей системы:
- компоненты и подсистемы ИС и их физическое расположение,
 - синхронность/асинхронность общения между компонентами системы,
 - выбор и определение характеристик каналов связи и т. п.,
 - выбор протоколов и программных интерфейсов,
 - выбор типа ПО промежуточного слоя (middleware),
 - выбор форматов документов, передаваемых в системе.

Например, в проектах достаточно крупных и территориально распределенных систем мы рассматриваем, по крайней мере, три архитектуры-кандидата:

- полностью централизованная система (например, основанная на web-технологиях); система, максимально адаптированная к офлайновой работе (основанная на сообщениях);
- система, максимально парирующая риски разработки (двухуровневая клиент-серверная).

6. Выбираются необходимые для реализации архитектуры элементы инфраструктуры — аппаратные средства, операционная система, СУБД, инструментальные средства, прикладные комплексы. Для каждого элемента инфраструктуры рассматриваются варианты его реализации. Оцениваются стоимость владения каждым элементом инфраструктуры архитектуры-кандидата в течение планового периода жизни системы и вероятности возникновения технических рисков в виде отказов элементов инфраструктуры архитектуры-кандидата.

Например, характерными элементами архитектуры являются:

- центральный сервер;
- центральная БД;
- коммуникационный канал между центром и филиалом;
- сервер филиала;
- БД филиала;
- рабочие станции;
- ПО Message Oriented Middleware.

Технические риски в данной архитектуре относятся к одному из классов, приведенных в таблице 1.

Вероятности реализации каждого из технических рисков можно получить из соответствующей литературы, например, коэффициенты надежности серверов можно получить из исследований надежности соответствующих серверных платформ. Экспертные оценки тоже можно рассматривать в качестве эффективного подхода к определению коэффициентов надежности. На самом деле, экспертные оценки, которые мы использовали сначала, оказались весьма точны для одиночных серверов, но надежность кластерных решений при первоначальной экспертной оценке была завышена на несколько порядков.

7. Строится матрица соответствия элементов архитектуры-кандидата и операций. На основе этой матрицы и матрицы соответствия статических бизнес-рисков и операционных рисков строится матрица соответствия технических рисков и бизнес-рисков. Значения элементов этой матрицы получаются как количество реализаций бизнес-риска на одну реализацию технического риска.

8. Если целью является именно построение архитектуры, то нужно вывести из рассмотрения те бизнес-риски, которые во всех архитектурах-кандидатах реализуются совершенно одинаково, и далее установить соответствие между оставшимися рисками и вариантами бизнес-использования. Построение указанных выше модулей на основе агрегирования вариантов бизнес-использования в пакеты позволило установить соответствие бизнес-рисков и модулей. Логическая структура системы, связывающая модули и элементы инфраструктуры, устанавливает соответствие между бизнес-рисками и элементами инфраструктуры. Технические же риски привязаны непосредственно к элементам инфраструктуры.

9. Наконец, количественные значения элементов матрицы соответствия бизнес-рисков и технических рисков получаются на основе тех же экономических моделей, которые разрабатывались для описания самих бизнес-рисков.

10. На основе матрицы соответствия технических рисков и бизнес-рисков для каждой архитектуры-кандидата и каждого варианта инфраструктуры оценивается часть общей стоимости владения системой, ассоциированная с бизнес-рисками. Выбираются оптимальные для каждой архитектуры-кандидата элементы инфраструктуры.

11. В качестве архитектуры системы выбирается архитектура-кандидат с минимальной оценкой совокупной стоимости владения.

Наш опыт показывает, что приведенная выше методика является эффективным средством при выборе архитектуры информационной системы, а также может стать важным этапом технико-экономического обоснования системы.

Автор выражает искреннюю благодарность А. Агапову, Е. Зиндеру, А. Малькову, Ю. Мартыненко, А. Столянкову, Г. Циперману, общение с которыми помогло в написании этой статьи.

Литература

1. Оценка и аттестация зрелости процессов создания и сопровождения программных средств и информационных систем (ISO/IEC TR 15504), М., Книга и бизнес, 2001.
2. Rational Unified Process 2002a, Rational Software, 2002.
3. J. F. Sowa, J. A. Zachman. Extending and Formalizing the Framework for Information System Architecture. IBM System Journal, vol. 31, №3, 1992.
4. Е. З. Зиндер. «3D-предприятие» — модель трансформирующейся системы.//CWR Директору информационной службы, №4, 2000.

5. Comparing Sun Solaris 8 and Microsoft Windows 2000 Server Technologies. White paper. Microsoft Corporation/ One Microsoft Way/ Redmond, WA 98052-6399, USA, №9, 2000.
 6. Total Cost of Ownership for Low-End and Mid-Range Server Clusters. A Detailed Analysis of the Total Cost of Ownership of Various RISC and Intel-Based Server Cluster Solutions. TechWise Research, 2001.
 7. OpenVMS: When Continuous Availability Really Matters. Harvard Research Group, 2001.
 8. Real-World System Availability Measurements for Compaq NonStop(tm) Integrity Systems. Compaq Inform, №28, 1999.
-

Пример оценки бизнес-риска

Пример является условным, поскольку привести данные из реально осуществленных проектов невозможно в силу вполне понятных причин (слишком рискованно!). Однако он полностью отражает схему описания и оценки бизнес-риска, и автор надеется, что для читателей не составит труда применить ее при работе над своими реальными проектами.

1. Сущность риска

В результате утечки информации в газете «Московский перец» может быть помещена заметка о том, что водка «Перечный стандарт» содержит метиловый спирт. Распространение этой информации сокращает продажи и снижает прибыль.

2. Принятые допущения

- В случае утечки информации заметка будет опубликована с вероятностью 80% (p_0).
- Газету «Московский перец» читает приблизительно 1 000 000 человек (N).
- 25% (p_1) читателей полностью доверяют содержанию публикаций такого рода и откажутся от приобретения этого товара.
- 10% (p_2) читателей газеты употребляют водку «Перечный стандарт».
- В месяц каждый потребитель приобретает в среднем пять единиц указанной продукции (k).
- Прибыль составляет 27,5% от стоимости единицы продукции (prf).
- Отпускная стоимость единицы товара составляет 100 руб. (pr).
- Через месяц потребители забывают о заметке.

3. Стоимость риска

Потери составят:

$$Loss = p_0 * N * p_1 * p_2 * k * add * prf * pr = (\text{в данном случае}) = 2\,750\,000 \text{ руб.}$$

Таблица 1

ОЦЕНКА ИНТЕГРАЛЬНЫХ ЗАТРАТ НА СИСТЕМУ

В любой момент T реализации проекта дисконтированные (приведенные к одному моменту времени — началу проекта) интегральные затраты на систему могут быть оценены как

$$Z_{инт}^{ог} |_{\tau} = Z_{факт}^{ог} |_{\tau} + \sum_{t=\tau}^T (1+E)^{-t} Z_t^{ог}, \quad (1)$$

где $Z_{инт}^{ог} |_{\tau}$ — оценка дисконтированных интегральных затрат проекта в момент T ;

E — норма дисконтирования, отражает разную стоимость затрат, произведенных в разное время;

$Z_{факт}^{ог} |_{\tau}$ — дисконтированная сумма фактических интегральных затрат проекта, произведенных к моменту T ;

T — период жизненного цикла системы;

$Z_t^{ог}$ — оценка интегральных затрат на проект в периоде t .

В свою очередь, оценку интегральных затрат на проект в периоде t можно представить как

$$Z_t^{ог} = Z_t^{пл} + P_t^{ог}, \quad (2)$$

где $Z_t^{пл}$ — плановые затраты на проект в периоде t ;

$P_t^{ог}$ — оценка потерь, связанных с бизнес-рисками в периоде t .

Далее, плановые затраты на проект определяются следующим образом:

$$Z_t^{пл} = Z_t^{ко} + Z_t^{оф} + Z_t^{смф} + Z_t^{вн} + Z_t^{эк} + Z_t^{см}, \quad (3)$$

где $Z_t^{ко}$ — затраты на приобретение готового программного обеспечения и технических средств в периоде t ;

$Z_t^{оф}$ — затраты на проектирование системы в периоде t ;

$Z_t^{смф}$ — затраты на строительные-монтажные работы в периоде t ;

$Z_t^{вн}$ — затраты на внедрение системы в периоде t ;

$Z_t^{эк}$ — эксплуатационные затраты в периоде t ;

$Z_t^{см}$ — затраты на сопровождение в периоде t .