

ние  $\psi = F(\Delta)$ . Для вероятности этой четырехцикло-вой характеристики можно записать выражение

$$p_T^{(4)} = (p_1 p_2 p_3)^2 \cdot p_T, \quad (2)$$

В то же время для четырех циклов, составленных из двух цикловых обнуляющих характеристик, имеем

$$p_T^{(4)} = (p_T)^2. \quad (3)$$

Из сопоставления выражений (2) и (3) следует, что

$$(p_1 p_2 p_3)^2 p_T (p_T)^2 > (p_1 p_2 p_3)^2 \cdot p_T,$$

так как всегда  $p_T > (p_1 p_2 p_3)^2$  и, в частности,

$$\frac{1}{341} > \left(\frac{12}{64}\right)^6.$$

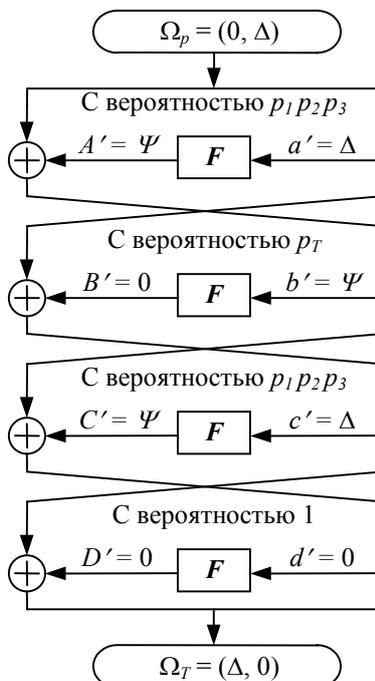
Представляется также очевидным, что реализация характеристик с меньшим числом тривиальных переходов тем более не приведет к большей угрозе дифференциальной атаки, чем рассмотренные выше.

К сожалению, и в новой редакции требование 4.1 оказывается недостаточным для обеспечения защиты от атак дифференциального криптоанализа. Обеспечив при отборе случайных таблиц должный уровень защиты от известных атак, использующих трехблочные характеристики, мы оставили без должного внимания возможность реализации характеристик, которые применяют меньшее число активных S блоков. В стандарте, как показывает анализ, эти характеристики исключены, в то время как для рассматриваемой случайной таблицы может быть построена характеристика с двумя активными S блоками и максимальным значением нуль-преобразования для одного S блока, равным  $P_D = \frac{6}{64}$ . В этом случае имеем

$$\left(\frac{6}{64}\right)^{2 \times 6} = 2^{-40,98},$$

что существенно хуже стойкости стандарта. Таким образом, предлагаемые критерии отбора случайных таблиц подстановок все еще не позволяют решить задачу формирования S блоков, полностью защищенных от атак дифференциального криптоанализа.

**Литература:** 1. Лисицкая И.В., Головашич С.А., Олешко О.И., Олейников Р.В., Коряк А.С. Построение таблиц подстановок для стандарта шифрования данных // Проблемы бионики. 1999. Вып. 50. С.185-194. 2. Горбенко И.Д., Лисицкая И.В. Критерии отбора случайных таблиц под-



Четырехцикловая характеристика

становок для алгоритма шифрования по ГОСТ 28147-89 // Радиотехника. 1997. Вып. 103. С. 121-130. 3. ANSI X9.F.1. TDEA modes of operation. Draft 5.5, X9.52, March 29, 1996. 4. NIST. AES announcement. Draft, June 15, 1997. 5. Lars R. Knudsen DEAL - A 128-bit Block Cipher. 1998. P.1-9. 6. E. Biham, A. Shamir Differential Crypto-analysis of the full 16-round DES. Technical Report-Computer Science Department, Technion, Israel, 1993. 11p. 7. Schneier B. Applied Cryptography. Second Edition: protocols, algorithms, and source code in C. Published by John Wiley & Sons, Inc, New York, 1996. 758p.

Поступила в редколлегия 02.03.99

Рецензент: д-р техн. наук Стасев Ю. В.

**Лисицкая Ирина Викторовна**, канд. техн. наук, доцент ХТУРЭ. Научные интересы: вероятностно-статистические методы и методы теории чисел в задачах криптографических преобразований и защиты информации. Адрес: Украина, 310180, Харьков, пер. Шекспира, 7, кв. 84, тел. 32-44-60.

**Олейников Роман Васильевич**, аспирант кафедры ЭВМ ХТУРЭ. Научные интересы: криптография, информационные технологии. Адрес: Украина, 310058, Харьков, ул. Маяковского, 14, кв. 249, тел. 30-24-52.

**Головашич Сергей Александрович**, аспирант кафедры ЭВМ ХТУРЭ. Научные интересы: криптография. Адрес: Украина, 310174, Харьков, пр. Победы, 61, кв. 311, тел. 30-24-52.

**Коряк Алексей Сергеевич**, аспирант кафедры ПО ЭВМ ХТУРЭ. Научные интересы: криптография. Адрес: Украина, 310140, Харьков, пр. Гагарина, 48, кв. 24, тел. 30-24-52.

**Олешко Олег Иванович**, аспирант кафедры ПОЭВМ ХТУРЭ. Научные интересы: криптография. Адрес: Украина, 310202, Харьков, пр. Победы, 51<sup>Б</sup>, тел. 30-24-52.

УДК 519.711

## ЗНАНИЕ - ОРИЕНТИРОВАННЫЙ ПОДХОД К РЕИНЖИНИРИНГУ БИЗНЕС-ПРОЦЕССОВ

ЧАЛЫЙ С.Ф., КАУК В.И.

Рассматриваются вопросы влияния реинжиниринга бизнес-процессов на систему знаний, накопленных в организации. Приводится структура бизнес-процессов и подход к их перепроектированию. Формулируются основные аспекты влияния реинжиниринга бизнес-процессов на систему знаний организации. Предлагаются направления реорганизации знаний при реинжинирин-

ге бизнес-процессов на основе использования информационных технологий.

### 1. Реинжиниринг бизнес-процессов

Реинжиниринг бизнес-процессов - это интенсивно развивающееся направление в менеджменте, направленное на радикальное повышение эффективности функционирования организации как единого целого. Реинжиниринг предполагает "фундаментальное переосмысление и радикальное перепроектирование" бизнес-процессов для достижения существенных улучшений в таких ключевых для современного бизнеса показателях результативности, как затраты, качество, уровень обслуживания и оперативность [1].

Бизнес-процесс представляет собой поток работы, переходящий от одного исполнителя к другому. Под исполнителем здесь подразумевается как один человек, так и целое подразделение организации. Бизнес-процессы можно описать на разных уровнях, но они всегда имеют четко очерченные границы [2]. Для любого отдельно взятого процесса эти границы установлены первичными входами и выходами. Входы связаны с первичными поставщиками. На выходе выдаются результаты первичным клиентам процессом, как показано на рисунке. Например, первичным входом в процессе сбыта может быть получение документов с подтверждением заказа. Первичным выходом процесса может быть получение определенной информации, услуги, документа.

После начала процесса у него могут появиться вторичные входы – например, управленческая информация. Точно так же у процесса могут существовать и вторичные выходы, которые получаются как его побочные продукты.

Необходимым условием выделения бизнес-процессов является формирование главной цели организации и критических факторов успеха, необходимых для достижения этой цели. Критические факторы успеха представляют собой цели более низкого уровня, отражающие ключевые составляющие фирмы и ее связи с другими организациями. Обычно критические факторы связаны с поставщиками, покупателями, персоналом, факторами окружающей среды и оборудованием [2]. Признаком критичности каждого фактора является невозможность без него достичь главной цели организации. Достижение всех подцелей позволяет достичь общей цели организации.

Реинжиниринг бизнес-процессов предполагает в идеале формирование процессов производства продукции "с чистого листа". Однако при реальном проектировании таких процессов необходимо учитывать существующие организационные структуры, накопленный ими опыт и знания. Все организационные бизнес-процессы определяются суммой знаний, накопленных в организации т.е. ее системой знаний.

В то же время выделение и классификация знаний организации обеспечивает возможность для автоматизации самих процессов реинжиниринга.

## 2. Виды знаний в организации

Можно выделить следующие ключевые элементы системы знаний организации [3]:

1. *Стратегическое знание.* Оно представляет собой знание высшего руководства организации. К нему относятся мысленные установки, цели, подходы к решению задач, устоявшиеся положения, которые определяют стратегию организации – т.е. все факторы, которые влияют на принятие стратегических решений по управлению.

Основная цель фирмы связана именно с этим видом знания.

2. *Структурное знание.* Это знание о структуре организации. Оно включает в себя типовые решения и рекомендации по координации различных видов деятельности организации. Хотя

обычно считается, что жестко фиксированная организационная структура ограничивает приобретение нового опыта и адаптацию организации, она в то же время может рассматриваться как хранилище накопленного и закодированного опыта. Так, структурное знание, вложенное в бюрократические правила и процедуры, используется при функционировании организации как единого целого, например, сотрудники должны быть обучены определенным (и единым для организации) правилам ведения документооборота.

Структурное знание отражает как собственный эволюционный опыт организации, так и опыт других фирм. В связи с этим считается, что организации имеют тенденцию изоморфизма, т.е. принимать аналогичную организационную структуру.

Структурное знание наряду со стратегическим определяет рассмотренные выше критические факторы успеха реинжиниринга бизнес-процессов организации.

3. *Системное знание.* Это знание закодировано в основных подсистемах организации и включает в себя, например, знания о конструкции информационных систем организации, систем управления, о человеческих ресурсах. Такое знание близко связано со структурным.

Оно может быть передано как между организациями, так и внутри одной организации, что создает предпосылки для стандартизации и автоматизации процессов реинжиниринга. Особенно важна такая возможность при интеграции подсистем разных организаций, например, при разработке совместных проектов.

Системное знание наряду со структурным и стратегическим оказывает влияние на формулирование критических факторов успеха и, соответственно, подцелей организации.

4. *Знание культуры.* Оно определяется как совокупность ценностей и норм, которые являются фундаментом поведения индивидуума. Такое знание описывается в форме символов, рассказов, а не через объективные факты и данные. При этом потребление изменения культуры производства часто рассматривается как важная мера для успешного реинжиниринга.

Согласно зарубежным источникам, ключевая цель изменения производственной культуры состоит в том, чтобы "переключить внимание от проблем и полумок к наиболее полному удовлетворению проблем покупателя" [4].

5. *Практическое знание.* Значительная часть знания, которое используется при работе организации, это так называемое "знание по умолчанию". Оно развивается из обучения на собственном опыте, из практической деятельности. Такое знание воплощено в установившейся практике и реализуется "по умолчанию"

индивидуальными служащими. При решении производственных задач часто возникают группы служащих, объединенных практическим опытом решения данной задачи. Персонал объединяется в такие группы не в соответствии с формальной структурой организации, а в целях реализации ка-



кой-либо задачи (например, обслуживания клиента, завершения проекта и т. п.).

Рассмотренные элементы организационной системы знаний, как правило, иерархически взаимосвязаны сверху вниз, начиная от стратегического знания и заканчивая практическим. Так, изменения стратегического мышления могут приводить к освоению новых рынков для продукции организации, что, в свою очередь, вызывает изменение структуры организации. Аналогично, структурные изменения могут приводить к пересмотру конструкции систем организации с целью достижения большей гибкости или стандартизации [3].

Вместе с тем взаимосвязь различных уровней знаний не всегда является иерархической. Так, стратегическое знание близко связано со структурным. Масштаб и уровень стратегического мышления отражает знание того, как координировать различные подразделения бизнеса. Например, существует стиль стратегического менеджмента, называемый "финансовое управление". В соответствии с этим стилем стратегические решения возлагаются на подразделения организации, но вместе с тем существуют системы финансового контроля, цель которых – извлечение прибыли.

С течением времени по мере развития организации и под влиянием конкуренции возникает эффект взаимного укрепления знаний, что может блокировать частичные изменения в организационной системе знаний. Изменения в информационных системах, например, могут быть заблокированы устаревшим структурным знанием или культурными антипатиями. Как следствие, подлинные изменения происходят только тогда, когда организация испытывает кризис во взаимоотношениях с внешним окружением. Кризисы имеют важный ударный эффект, который простирается прямо вниз, через структуру к практическим знаниям организации.

### 3. Влияние бизнес-процессов на систему знаний организации

Основной эффект реинжиниринга бизнес-процессов в организации заключается в перераспределении знаний и умений между различными группами людей, независимо от вида знаний. При этом логика сквозных бизнес-процессов предполагает устранение специализированных отделов, с традиционными бюрократическими формами знаний. Задачи, которые ранее были прерогативой отдельных специалистов, решаются различными группами в рамках единого бизнес-процесса. Это поднимает вопрос об использовании компьютерных баз знаний и экспертных систем при реинжиниринге бизнес-процессов и, соответственно, разработке бизнес-процессов приобретения знаний и наполнения таких экспертных систем.

Реинжиниринг бизнес-процессов оказывает следующее влияние на систему знаний организации:

- стратегическое знание – изменяется парадигма управления, т.е. иерархическое управление сменяется управлением бизнес-процессами;
- структурное знание – изменяются подразделения организации и взаимосвязи между ними, меняется и система документооборота;
- системное знание радикально изменяется вследствие использования современных информационных технологий и ориентации информационных подсистем на бизнес-процессы;
- изменение культурного знания предполагает пересмотр взглядов исполнителей на решаемые ими задачи и ориентацию их на требования конкретного потребителя, самоконтроль исполнителей;
- практическое знание – при решении большинства задач универсалы заменяют узких специалистов;

квалифицированные эксперты решают незначительный процент задач, требующий очень высокого уровня компетентности;

Среди наиболее важных факторов, влияющих на реинжиниринг бизнес-процессов в целом и системы знаний организации в частности, следует отметить информационные технологии. Использование таких технологий предполагает:

- создание единой базы данных и базы знаний организации;
- создание систем электронного обмена данными;
- распараллеливание процессов разработки продукции с использованием систем автоматизированного проектирования;
- автоматизацию документооборота организации на основе единой базы данных;
- создание экспертных систем, обеспечивающих поддержку принятия решений непосредственными исполнителями;
- разработку бизнес-процессов приобретения знаний и наполнения компьютерных баз знаний и экспертных систем.

Следует отметить, что сами по себе информационные технологии не обеспечивают успешного реинжиниринга и радикального повышения эффективности функционирования организации. Важно изменение всего комплекса знаний, а информационные технологии предоставляют удобный инструмент для решения этой задачи (анализ, распараллеливание операций, удаление избыточных этапов процесса). Реинжиниринг радикально отличается от автоматизации существующих процессов. Автоматизация некоторого этапа процесса означает, что данный этап больше не будет выполняться вручную, хотя сам по себе остается. Реинжиниринг предполагает творческое изменение процессов на основе новых технологий. В этом смысле технология играет роль движущей силы преобразования бизнес-процессов, предлагая новые методы работы и новые возможности. Однако это предполагает знание новых технологий специалистами, выполняющими реинжиниринг. Следовательно, система знаний организации должна включать новый вид знания – технологическое.

Таким образом, реинжиниринг бизнес-процессов вызывает существенные изменения в системе знаний организации. Наиболее серьезные трудности возникают при изменении стратегических, культурных и структурных знаний. В то же время использование информационных технологий позволяет решить многие из проблем, связанных с реорганизацией знаний.

**Литература:** 1. Хаммер М., Чампи Дж. Реинжиниринг корпорации: Манифест революции в бизнесе: Пер. с англ. СПб.: Изд-во С.-Петербургского ун-та. 1997. 332 с. 2. Робсон М., Уллах Ф. Практическое руководство по реинжинирингу бизнес-процессов: Пер. с англ. / Под ред. Н. Д. Эриашвили. М.: Аудит, ЮНИТИ, 1997. 224 с. 3. Dr. Harry Scarbrough. Business Process Re-design: The knowledge dimension. University of Warwick, 1996. 4. Jones C. 'Rover Group Ltd. Case Study'. Proceedings of Forum 4 (Coventry: ESRC Business Processes Resource Centre, University of Warwick), 1996. 12 с.

Поступила в редколлегия 30.01.99

**Рецензент:** д-р техн. наук Петров Э.Г.

**Чалый Сергей Федорович**, канд. техн. наук, доцент кафедры технической кибернетики ХТУРЭ. Научные интересы: автоматизация бизнес-процессов, информационно-аналитические системы. Адрес: Украина, 310166, Харьков. пр. Ленина, 14, тел. 40-93-35.

**Каук Виктор Иванович**, канд. техн. наук, доцент кафедры программного обеспечения ЭВМ ХТУРЭ. Научные интересы: автоматизация бизнес-процессов, информационно-аналитические системы. Адрес: Украина, 310166, Харьков. пр. Ленина, 14, тел. 40-95-15.