С. М. Авдошин, Е. Ю. Песоцкая

ИНФОРМАТИЗАЦИЯ БИЗНЕСА. УПРАВЛЕНИЕ РИСКАМИ

Допущено УМО по образованию
в области экономики, менежмента, логистики и бизнес-информатики
в качестве учебника для студентов высших учебных заведений,
обучающихся по направлению «Бизнес-информатика» (080700)

ДМК ПРЕСС
издательство

УДК 004:005.334(075.8)
ББК 65.386.8-09я73-1
А18

Рецензенты:
Козырев О. Р. — директор Нижегородского филиала Национального исследовательского университета Высшей школы экономики, заместитель директора Института информационных технологий НИУ ВШЭ, профессор кафедры прикладной математики и информатики НИУ ВШЭ;
Костогрызов А. И. — заслуженный деятель науки РФ, доктор технических наук, профессор, член-корреспондент Российской академии ракетных и артиллерийских наук и Российской академии естественных наук, действительный член Академии информатизации образования, лауреат премии Ленинского комсомола в области науки и техники.

Авдошин С. М., Песоцкая Е. Ю.
А18 Информатизация бизнеса. Управление рисками. — М.: ДМК Пресс, 2011. — 176 с., ил.

ISBN 978-5-94074-109-1

Проблема управления рисками при информатизации бизнеса является одной из наиболее актуальных и значимых в ИТ-индустрии. В предлагаемом учебно-практическом пособии, затронуты как теоретические, так и практические вопросы управления рисками, раскрывается специфика механизма управления рисками при реализации проектов в области информационных технологий.

В основу учебного пособия положен многолетний опыт преподавания авторами дисциплины «Управление рисками» на отделении программной инженерии Высшей школы экономики.

Книга предназначена для студентов магистратуры, обучающихся по направлениям 080500.68 «Бизнес-информатика» и 231000.68 «Программная инженерия», а также для ИТ-специалистов, разработчиков и заказчиков программных продуктов, менеджеров ИТ-проектов.

УДК 004:005.334(075.8)
ББК 65.386.8-09я73-1

ISBN 978-5-94074-109-1

© Авдошин С. М., Песоцкая Е. Ю., 2011
© Оформление, ДМК Пресс, 2011

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 5

ПРЕДИСЛОВИЕ 7

ГЛАВА 1. РИСКИ И НЕОПРЕДЕЛЕННОСТИ ПРИ ИНФОРМАТИЗАЦИИ БИЗНЕСА 12

1.1. Информатизация бизнеса и специфика ИТ-отрасли 12
1.2. Риски в ИТ: термины и определения 18
1.3. Классификация рисков в ИТ-проектах 23

ГЛАВА 2. ОБЗОР СУЩЕСТВУЮЩИХ СТАНДАРТОВ И МЕТОДОЛОГИЙ УПРАВЛЕНИЯ РИСКАМИ 30

2.1. Зачем нужны стандарты и методологии управления рисками 30
2.2. Обзор методологий: достоинства и недостатки 32
2.3. Риски при использовании методологий разработки ПО 38
2.4. Риски в жизненном цикле программного обеспечения 41

ГЛАВА 3. УЛУЧШЕНИЕ КАЧЕСТВА ПО И СНИЖЕНИЕ РИСКОВ ... 44

3.1. Понятие качества и его многомерность 44
3.2. Основные проблемы и ключевые факторы успеха ИТ-проектов 47
3.3. Влияние изменений на риски ИТ 52
3.4. ИТ-аудит как средство управления рисками 55

ГЛАВА 4. ЭТАПЫ УПРАВЛЕНИЯ РИСКОМ ИТ 58

4.1. Планирование и идентификация рисков 58
4.2. Качественная и количественная оценка рисков 68
4.3. Разработка реагирования на риски 86
4.4. Мониторинг, отчетность и контроль управления рисками 94

ГЛАВА 5. РИСКИ В ИТ-АУТСОРСИНГЕ 97
5.1. Необходимость ИТ-аутсорсинга 97
5.2. Риски и выгоды от использования аутсорсинга 101
5.3. Методы управления рисками аутсорсинга 106

ГЛАВА 6. РИСКИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 109
6.1. Понятие информационной безопасности 109
6.2. Основные риски в обеспечении информационной безопасности 112
6.3. Методы управления рисками информационной безопасности ... 117

ГЛАВА 7. ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ РАЗРАБОТКИ ПО И ВНЕДРЕНИЯ ИТ-СИСТЕМ 123
7.1. Организация управления рисками в команде проекта 123
7.2. Как подобрать компетентную команду ИТ-проекта 126
7.3. Характеристики риск-менеджера 131

ГЛАВА 8. ОБЗОР ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ РИСКАМИ 135
8.1. Требования к информационной системе управления рисками ... 135
8.2. Сравнение коробочного и собственного ПО управления рисками 140
8.3. Обзор ПО: преимущества и недостатки 143

ЗАКЛЮЧЕНИЕ 165

ПРИЛОЖЕНИЕ. ТЕМЫ СЕМИНАРСКИХ ЗАНЯТИЙ ПО КУРСУ «ИНФОРМАТИЗАЦИЯ БИЗНЕСА. УПРАВЛЕНИЕ РИСКАМИ» 167

СПИСОК ЛИТЕРАТУРЫ 174

ВВЕДЕНИЕ

Практически в любой современной организации мы можем наблюдать тесное переплетение информационных технологий и бизнес-процессов основной деятельности. Информация для бизнеса является критически важным ресурсом, от качества информации, от скорости ее передачи, надежности хранения зависит успех бизнеса. Работа с информацией, особенно в последнее время, стала подразумевать использование компьютерных технологий. Появился термин «информатизация бизнеса», который предполагает запуск и функционирование некоторой информационной технологии для использования, обработки, хранения и передачи данных для поддержки определенной бизнес-деятельности. Как правило, при информатизации бизнеса одновременно выполняются несколько проектов в области информационных технологий (ИТ), причем все за ограниченное время и с использованием выделенных ресурсов.

Учебник целесообразно использовать при обучении студентов магистратуры по направлениям 080500.68 «Бизнес-информатика» и 231000.68 «Программная инженерия». Он также будет полезен аспирантам, руководителям ИТ-проектов, лидерам команд разработчиков, заказчиков ПО со стороны клиента, сотрудникам ИТ-служб.

Основная цель курса лекций — представить студентам, аспирантам и менеджерам проектов современный комплекс задач, методов и стандартов управления рисками ИТ-проектов при информатизации бизнеса — создания и развития сложных, тиражируемых программных средств (ПС), баз данных (БД), информационных систем (ИС), приложений инфраструктуры, сервисов и средств поддержки информационных технологий. Внимание акцентировано на комплексе методов и процессов, которые способны непосредственно обеспечить управление рисками сложных высококачественных программных продуктов, анализировать, планировать и контролировать проектные риски, эффективно работать в команде, создавать адекватную мотивацию продуктивной работы, использовать современные программные средства.

В учебнике отражены методологические основы современного управления рисками при информатизации бизнеса, раскрыта специфика ИТ-индустрии и разработки программного обеспечения. Представлены обзоры международных стандартов управления программными проектами, опыт разработки систем и комплексов программ при информатизации бизнеса, модели и процессы управления рисками в ИТ-проектах. Значительное внимание уделено областям, непосредственно влияющим на аспекты управления рисками, таким как управ-

ление качеством разработки, управление требованиями, управление командой внедрения, управление поставщиком и подрядчиком. Ряд лекций посвящен разработке требований, планированию информационной безопасности. Рассмотрены основные процессы управления рисками программных проектов: идентификация, качественная и количественная оценка, выбор методов реагирования, контроль управления рисками. Детально изложены подходы к классификации рисков и рискообразующих факторов, методы и процессы идентификации рисков, методы оценки, включая имитационное моделирование, а также даны обзор возможных методов реагирования на риски, примеры отчетности по рискам, рекомендации к ведению и хранению накопленного опыта по управлению рисками. Завершает курс лекций обзор специализированного программного обеспечения. Приведено сравнение коробочной и заказной разработки, сформулированы требования к программному продукту по управлению рисками.

Значительное внимание в курсе уделено практическому применению методологической базы по управлению рисками. Рассматриваются конкретные проекты в специфических предметных областях, проекты, осуществляемые с применением узконаправленных технологий, а также проекты со специфическим конечным продуктом. Рассматриваются конкретные примеры рисков, типичные для ИТ-области, такие как задержки в графике работ проекта, превышение бюджета, несоответствие требуемым стандартам качества или ожиданиям заказчика и прочее. Кроме того, в числе рисков можно отметить непонимание акционерами роли и места информационных технологий, сомнения в окупаемости ИТ-проектов, низкую степень готовности персонала к использованию новых технологий вообще и информационных технологий в частности, слабую материально-техническую базу многих предприятий, которая препятствует созданию фундамента для развития ИТ.

Хочется надеяться, что материал будет полезен не только ИТ-специалистам при проектировании, разработке и внедрении ПО, но и послужит практическим примером для бизнес-заказчиков, менеджеров крупных ИТ-проектов, для аналитиков и ведущих специалистов, обеспечивающих все этапы жизненного цикла крупных программных средств и систем. Практические примеры наглядно покажут, как учиться не на своих ошибках и ошибках своей проектной команды, а на типичных рисках, описанных в этом пособии.

Авторы выражают глубокую благодарность А. И. Костогрызову за предоставленные иллюстративные материалы и помощь в подготовке содержательной части, в значительной мере обеспечившую качество данного учебного пособия. А. Костогрызов внес значительный вклад в развитие отечественных программно-инструментальных комплексов в области управления рисками, которые подробно рассмотрены в отдельной главе настоящего учебника. Написанные им работы породили массу новых исследований в области программной инженерии. Оценка, которую он дал нашей рукописи, и его вклад в эту книгу просто неоценимы.

ПРЕДИСЛОВИЕ

Настоящая монография предоставляет базовые понятия по управлению рисками при информатизации бизнеса, раскрывает специфику индустрии информационных технологий и разработки программного обеспечения. Поскольку по своему замыслу монография ориентирована на студентов магистратуры и начинающих руководителей ИТ-проектов, ее изложение построено как учебник. Но учебник не совсем обычный. Дело в том, что охватываются накопленные знания и опыт из области системной и программной инженерии, то есть того научно-практического направления, которое продолжает находиться в стадии формирования. В отличие от классиков (в России в первую очередь имеются в виду работы профессора Липаева В. В., см. также технический отчет «Руководство в области программной инженерии совокупности знаний — SWEBOK», включающий материалы исследований ученых, опубликованных в англоязычной технической литературе на протяжении последних 30 лет), учебник растолковывает азы и лишь обозначает вершины, к которым должны стремиться профессионалы.

Чтобы понять своевременность появления учебника, необходимо осознать суть основных системных изменений нашего времени. А суть эта по-крупному заключается в:

- проникновении системной и программной инженерии в различные сферы человеческой жизнедеятельности;
- развитии и широком применении «процессного подхода» на уровне международных стандартов;
- достижении системных эффектов, определяемых возможностями применяемых ИТ и возникновением новых рисков, связанных с уязвимостями самих ИТ;
- объективных потребностях адекватного прогнозирования качества и рисков на всех стадиях жизненного цикла систем для различных условий и возможных угроз.

Сегодня эффективные решения и, как следствие, высокий уровень качества (в том числе безопасности) систем[1] во многом связаны с рациональным при-

[1] Под системой понимается комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей (ISO/IEC 15288).

менением стандартов. Действующие на практике стандарты лишь отражают суть научно-технических достижений, фиксируя де-юре те требования и рекомендации, выполнение которых может способствовать относительному совершенству. Конец прошлого века можно признать плодотворным для развития системной[1] и программной инженерии[2]. В целях адекватной реакции на новшества и развитие ИТ подкомитет SC7 «Программная инженерия» объединенного комитета JTC1 «Информационные технологии» преобразован в подкомитет «Системная и программная инженерия» (SC7 JTC1 ISO/IEC), что отражает стремление к целостному решению проблем стандартизации в направлении всеобъемлющего качества именно систем в их жизненном цикле, а не составных компонентов или процессов. К настоящему времени в мире уже не один год действуют стандарты для систем любой области приложения — это набравший популярность ISO 9001 «Системы менеджмента качества. Требования», ISO/IEC 15288 «ИТ. Системная инженерия — процессы жизненного цикла систем», существенно повлиявший на последующее развитие стандартизации — см. рис. 1, 2, а также стандарты серий ISO 14000 (менеджмент экологической безопасности), OHSAS 18000 (менеджмент охраны труда), ISO/IEC 20000 (сервис-менеджмент), ISO/IEC 27000 (менеджмент информационной безопасности), 31000 (менеджмент риска), развиваются стандарты серии ISO/IEC 33000 (оценка процессов) и др. Таким образом, столь естественное наличие типовых процессов и их идентичное развертывание во времени характеризуют логическую похожесть различного рода систем. Именно анализу системных процессов, регламентируемых этими стандартами, в монографии уделено особое внимание.

Чтобы понять важность рассматриваемой тематики, вспомним некоторые факты.

Обратимся к абсолютно приземленным казусам современного интеллектуального рынка. Вспомним 1997 год, когда разразился мировой финансовый кризис. Все началось с обвала акций высокотехнологичных компаний. Ослабление валют стран Юго-Восточной Азии привело к реализованной на

---

[1] Системная инженерия — это избирательное приложение научно-технических усилий по:
- преобразованию функциональных потребностей в описание системной конфигурации, которая наилучшим образом удовлетворяет этим потребностям по показателям эффективности;
- объединению связанных технических параметров и обеспечению совместимости всех физических, функциональных и программно-технических интерфейсов способом, оптимизирующим в целом определение и проектирование всей системы;
- объединению возможностей всех инженерных дисциплин и специальностей в единое системотехническое достижение (SEI).

[2] Программная инженерия — применение систематического упорядоченного количественного подхода к разработке, эксплуатации и сопровождению программного обеспечения (IEEE 610.12).



Рис. 1. Процессы предприятия с ориентацией на потребителя по ГОСТ Р ИСО 9001



Рис. 2. Процессы жизненного цикла систем по ГОСТ Р ИСО/МЭК 15288

программном уровне реакции биржевых роботов (программных систем автоматической биржевой торговли, анализирующих ситуацию на рынках, сравнивающих ее с хранимыми в памяти ситуациями и автоматически принимающих решения). Последние в автоматическом режиме выставили на продажу громадные объемы валют, с учетом чего национальные валюты в этих странах упали в 30—100 раз! А затем дефолт 1998 года в России... Через 10 лет в августе 2007 года те же биржевые роботы среагировали столь же «адекватно», как и были запрограммированы на подобное развитие биржевой ситуации, — в результате выполнения автоматических приказов одновременно был сгенерирован вал заявок на продажу американских ипотечных облигаций. Физика процессов достаточно проста: брокер-человек справляется лишь с 3—4 портфелями одновременно и в день способен заключить до 10—15 сделок, в то время как биржевые роботы управляют 100 портфелями и могут заключать до 500 сделок в день. В погоне за прибылью не было сделано системных ограничений на вал автоматических заявок. В итоге $260 млрд. убытка — это лишь частный побочный эффект от подобной оптимизации на бирже. Подчеркнем, ущерб сопоставим с совокупным годовым бюджетом нескольких государств Восточной Европы! И если в 1997 году в инициировании кризиса объявили нескольких английских брокеров, спекулировавших в Сингапуре, то в 2007 году обвинять некого — не вредоносные, а сугубо мирные компьютерные программы инициировали глобальный финансовый кризис!

Другими словами, если 50 лет назад последствия от применения ядерного оружия оценивались как возможность многократного уничтожения жизни на земле, то сегодня проявления «мирных» угроз со стороны компьютеризированных систем оказываются соизмеримыми с применением того же самого ядерного оружия. То есть в XXI веке военные угрозы дополнились еще более разрушительными «мирными» угрозами, связанными с широким внедрением ИТ!

На практике у каждого из заказчиков, разработчиков, производителей и пользователей современных систем неизбежно возникают принципиальные системные вопросы. Например: «Как достичь уровня международных стандартов?»; «Выполнимы ли задаваемые требования?»; «Каковы возможные ущербы?»; «Какой сделать выбор с учетом возможных рисков, затрат и ожидаемого результата?»; «Какие меры более эффективны?». Предполагаемая монография позволяет взглянуть на решение этих вопросов именно в контексте требований современных стандартов. Причем основные положения необходимо рассматривать не только для ИТ-проектов и систем, но и для любого рода систем, создаваемых или функционирующих с использованием средств автоматизации.

Значительное внимание уделено областям, непосредственно влияющим на аспекты управления рисками, таким как управление качеством разработки, требованиями, командой. Рассмотрены основные процессы управления рисками программных проектов: идентификация, качественная и количественная