Московский экономический журнал. № 1. 2024
Moscow economic journal. № 1. 2024
Научная статья
Original article
УДК 33
doi: 10.55186/2413046X_2023_9_1_10

ПОДХОДЫ К УПРАВЛЕНИЮ РИСКАМИ В ПРОЦЕССЕ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

APPROACHES TO RISK MANAGEMENT IN THE SOFTWARE DEVELOPMENT PROCESS

Иванов Никита Сергеевич, аспирант, Московский финансово-промышленный университет «Синергия», Москва, Россия, E-mail: nikitrit@yandex.ru
Ivanov Nikita Sergeevich, Graduate student, Moscow Financial and Industrial University "Synergy", Moscow, Russia, E-mail: nikitrit@yandex.ru

Аннотация. В данной статье рассматриваются подходы к управления рисками которые возникают во время разработки программного обеспечения. Целью данной статьи является обзор существующих подходов к управлению рисками, возникающими в процессе разработки программного обеспечения. В качестве методов получения научной информации были использованы теоретические методы исследования. В результате был приведен краткий обзор таких методик как: CMMI-DEV, EBIOS Risk Manager, ProRisk Framework, RiskIt и PRINCE2. Для каждого подхода выделены основные этапы и принципы работы с рисками.
Abstract. This article discusses approaches to risk management that arise during software development. The purpose of this article is to review existing approaches to managing risks arising in the software development process. Theoretical research methods were used as methods of obtaining scientific information. As a result, a brief overview of such techniques as: CMMI-DEV, BIOS Risk Manager, Process

Framework, Reskit and PRINCE2 was provided. The main stages and principles of risk management are highlighted for each approach.
Ключевые слова: риск; риск менеджмент; управление рисками; разработка программного обеспечения; процесс разработки; управление проектами

Keywords: risk; risk management; risk management; software development; development process; project management

Введение

Разработка программного обеспечения представляет из себя сложный и многоэтапный процесс, требующий высокой квалификации специалистов, а также характеризующийся изменчивостью требований. В процессе разработки программного обеспечения существует множество факторов, которые необходимо учитывать: ограничение времени, требования заказчика, технологические ограничения и т.д. По данным отчета Chaos Report за 2020 год [1], который публикует международная консалтинговая группа *The Standish Group* только 31% проектов по разработке программного обеспечения оказались успешными. Проекты, в которых возникли проблемы, приведшие к изменению изначальных сроков, пересмотру выделенного бюджета и отклонению от заранее намеченных целей составили 50%. Остальные 19% составили провалившиеся проекты, которые были остановлены, так и не достигнув изначально намеченных целей. Приведенные данные свидетельствуют об актуальности проблемы управления рисками в процессе разработки программного обеспечения. В связи с этим целью данной статьи является обзор существующих методик управления рисками, применяемых для разработки программного обеспечения.

Результаты и дискуссия

CMMI-DEV (Capability Maturity Model Integration for Development) — это модель зрелости для управления проектами разработки программного обеспечения, которая включает в себя методику управления рисками. Управление рисками по методике CMMI-DEV RKSM фокусируется на выявлении рисков на ранних этапах проекта, привлечении заинтересованных

сторон, использовании отраслевых стандартов [2]. Управление рисками в данной методике можно разделить на 3 части:

1. Определение стратегии управления рисками
2. Выявление и анализ рисков
3. Отслеживание рисков и реализация планов по снижению рисков

В первой части идентифицируются источники риска, которые могут быть как внутренними, так и внешними по отношению к проекту. Происходит определение параметров необходимых для классификации и приоритизации:

1. Вероятность риска
2. Последствия риска
3. Критерии запуска действий по управлению рисками

Затем на основе полученных данных строится стратегия управления рисками, включающая в себя следующие элементы:

- Объем усилий готовых затрачиваться на управление рисками
- Методы и инструменты, которые будут использоваться для идентификации, анализа, снижения и мониторинга рисков
- Выделение источников риска характерных для проекта
- Способ организации и классификации рисков
- Параметры для принятия мер в отношении рисков
- Методы снижения рисков
- Временные интервалы для определения и мониторинга рисков

Часть выявление и анализ рисков включает в себя идентификацию рисков из определенных ранее источников, выявление установленных параметров, категоризацию и приоритизацию рисков. Риски, связанные между собой, могут быть сгруппированы для более эффективного мониторинга и выполнения действий управления рисками.

В заключительной части для рисков, представляющих высокую угрозу, строятся планы снижения рисков и планы действий в чрезвычайных ситуациях. Другие риски принимаются и отслеживаются. Планы по снижению рисков

внедряются и осуществляется регулярный мониторинг. Также в соответствии с установленном в плане по управлению рисками интервале происходит пересмотр статуса существующих рисков, данная деятельность может привести к выявлению новых рисков или новых вариантов управления рисками.

Центральная служба безопасности информационных систем (SCSSI) создала методику EBIOS Risk Manager в 1995 году во Франции, и с тех пор она периодически обновляется. На данный момент поддерживается Французским национальным агентством по безопасности информационных систем (ANSSI) [3]. Данная методика соответствует следующим стандартам ISO: ISO 27000, ISO 27005 и ISO 31000. Она состоит из 5 последовательных этапов:

1. Сфера и базовые показатели безопасности
2. Источники риска
3. Стратегические сценарии
4. Операционные сценарии
5. Обработка рисков

Основными задачами первого этапа являются: определение границ исследуемой области, определение базовых показателей безопасности и событий, вызывающих опасения.

Целями второго этапа является идентификация источников риска и их целевых задач. В ходе выполнения данного этапа выявляется список пар (источник риска/последствия риска), затем выбираются только наиболее релевантные именно они и будут использоваться в последующих этапах.

Этап стратегических сценариев необходим чтобы получить представление о цифровой экосистеме и выявить её наиболее уязвимы стороны. На основе полученной информации строятся стратегические сценарии, которые представляют из себя путь, который проделает источник риска для достижения последствий риска. Стратегические сценарии являются основой для построения операционных сценариев.

В ходе выполнения четвертого этапа происходит построение операционных сценариев, представляющих из себя возможные и

детализированные способы достижения последствий рисков. Затем на основе полученных сценариев оценивается вероятность реализации риска.

Цель завершающего этапа заключается в составлении краткого описания всех изученных рисков, определение стратегии снижении рисков, построение системы мониторинга.

Методика ProRisk Framework была представлена в 2004 году Джеффри Роем в статье «A Risk Management Framework for Software Engineering Practice» [4]. Она фокусирует внимание на двух основных областях проекта, в ходе которого разрабатывается программное обеспечение, а именно: бизнес-область и операционная сфера.

В бизнес-область определяется знания и опыт организации, а также уровень уверенности в том, что проект может быть успешно завершен. Также в данной сфере определяется внешняя среда, в которой осуществляется проект, подверженность внешним факторам риска, восприимчивость к результатам работы.

В операционной области выполняются формальные процессы управления рисками:

- Оценка рисков используя опыт и политики организации
- Выявление ключевых факторов риска
- Построение плана действий направленный на снижение ключевых факторов риска
- Реализация плана и повторное выявление ключевых факторов риска
- Объединение вышеописанных шагов в непрерывный цикл, который повторяется до конца жизненного цикла проекта

Методика Risk It была опубликована Ассоциацией аудита и контроля информационных систем в 2009 году [5]. Данная методика является коллегиальным продуктом экспертов и ученых из таких компаний как: IBM, Swiss Life и др. В её основе лежат следующие 6 принципов:

1. Нужно держать в балансе затраты и выгоды от управления рисками

2. Процесс управления рисками является непрерывным процессом и составляющей повседневной деятельности

3. Необходимо способствовать честным и открытым докладам о рисках

4. В процессе управления рисками необходимо ориентироваться на цели бизнеса

5. Установите правильный тон управления, обеспечивая личную ответственность за выполняемую работу, в рамках определенных уровней допуска

6. Приведите управления рисками разработки ПО к общей системе управления рисками

В методике Risk It процессы сгруппированы по трем областям:

- Управление рисками
- Оценка рисков
- Реагирование на риски

В области управления рисками, необходимо убедится, что на предприятии, позволяющую обеспечить максимальную доходность с учетом рисков. Эта область состоит из следующих процессов:

- Создание и поддержание общего представления о рисках
- Интеграция с общей системой управления рисками
- Принятие бизнес-решений с учетом рисков

Область оценки риски ставит целью убедится, что связанные с разработкой ПО риски были определены, проанализированы и представлены в понятных бизнесу формулировках. Данная область содержит в себе следующие процессы:

- Сбор данных
- Анализ рисков
- Поддержка профиля риска

В области реагирования на риски, необходимо убедится, что реакция на риски выполняется экономически эффективным образом и соотносится с целями бизнеса. Данная область состоит из следующих процессов:

- Формулирование риска
- Управление рисками
- Реакция на события

Методология PRINCE2 берет свое начало в середине 1970-х появилась в виде методологии PROMPT, которая была создана в частной компании Simpact Systems Limited. В 1980 данная методология лицензируется центральным компьютерным и телекоммуникационным агентством Великобритании. Далее в 1989 году улучшив PROMPT агентство переименовывает методологию в PRINCE, а уже в 1996 выходит новая версия методологии под названием PRINCE2. В 2009 году выпускается последняя версия PRINCE2. А в 2013 году был передан компании AXELOS Ltd и на данный момент является зарегистрированной торговой маркой данной компании. В данной методологии присутствует 6 целевых показателей за которыми осуществляется контроль: сроки, затраты, качество, объем, преимущества, риск.

Целью подхода по управлению рисками в данной методологии является: выявление, оценка и контроль неопределенности в ходе проекта, и как следствие повышение способности проекта к успеху [6]. В рамках данной методологии риск определяется как, неопределенное событие, которое, если оно произойдет, окажет либо положительное, либо отрицательное влияние на цели проекта. Согласно методологии, управление рисками проходит в 5 этапов: идентификация, оценка, планирование, реализация, общение.

Этап идентификации рисков проекта включает определение контекста, заполнение документа “Подход к управлению рисками” и определение рисков, используя различные методы. В процессе определения контекста необходимо ответить на вопросы о проекте: что это за проект, сколько людей будет использовать продукт, во что обойдется компании если продукт не сработает,

насколько сложен проект и подход организации к рискам. При заполнении документа “Подход к управлению рисками”, необходимо предоставить информацию о процедуре управлении рисками, структуре реестра рисков, категориях рисков, ролях и обязанностях участников, а также о масштабе вероятности, степени воздействия и близости рисков. Для определения рисков можно использовать такие методы, как анализ уроков и журналов рисков из прошлых проектов, использование контрольных списков и проведение мозгового штурма с привлечением специалистов. Описанные риски необходимо характеризовать в терминах причина, событие и следствие.

На этапе оценке для каждого риска выявляются: вероятность риска, воздействие риска, возможное время возникновения и как меняется влияние риска на протяжении проекта. Также во время данного этапа выполняется обобщение рисков с целью получить общую оценку риска для всего проекта.

Этап планирования мер заключается в планировании конкретных ответных мер на угрозы и возможности. Целью планирования ответных мер на риск является уменьшение угроз и максимальное использование возможностей. Для этого PRINCE2 предлагает 6 возможных реакций на угрозы:

1. Избегание. Принятие таких мер чтобы угроза больше не могла произойти или не могла оказать никакого влияния.
2. Снижение. Снижение вероятности возникновения, а также влияния, которое может оказать угроза.
3. Запасной вариант. Снижение воздействия угрозы, за счет применения запасного варианта.
4. Передача. Передача угрозы другой стороне для минимизации влияния.
5. Принятие. Никакие меры в случае реализации риска не принимаются, но угроза по-прежнему отслеживается.
6. Разделение. Снижения убытков от угрозы, за счет разделения.

Кроме реакций на угрозы, PRINCE2 также предлагает 4 реакции на отрывшиеся возможности:

1. Эксплуатация. В случае возникновения возможности она будет использована.

2. Усиление. Повышается вероятности или благоприятного воздействия возможности.

3. Разделение. Разделение прибыли, в случае реализации возможности.

4. Отклонение. В случае наступления возможности не будут предприниматься никакие действия.

Во время этапа реализации распределяются роли владельца риска и исполнитель риска. Владелец риска осуществляет мониторинг и управление риском, а исполнитель риска принимает меры по борьбе с рисками и поддерживает владельца риска.

Этап общения выполняется на протяжении всей процедуры управления рисками и необходим для того, чтобы вся информация, которая относится к угрозам и возможностям была доведена до заинтересованных сторон.

Заключение

В статье были рассмотрены различные подходы к управлению рисками возникающие во время разработки программного обеспечения. Все обозреваемые подходы к управлению рисками представляют из себя многоэтапный процесс, в контексте которого риск рассматривается не только как негативное событие, но и как положительное событие позволяющее извлечь выгоду в случае реализации риска.

Список источников

1. Project Managers Fail to Help Software Projects (Standish Group Chaos 2020). / [Электронный ресурс] // Vitality Chicago: [сайт]. — URL: https://vitalitychicago.com/blog/project-managers-fail-to-help-software-projects-standish-group-chaos-2020 (дата обращения: 5.12.2023).

2. Risk Management (RSKM) (CMMI-DEV) / [Электронный ресурс] // Wibas : [сайт]. — URL: https://www.wibas.com/cmmi/risk-management-rskm-cmmi-dev (дата обращения: 5.12.2023).

3. EBIOS Risk Manager – The method / [Электронный ресурс] // Agence nationale de la sécurité des systèmes d'information : [сайт]. — URL: https://cyber.gouv.fr/en/publications/ebios-risk-manager-method (дата обращения: 7.12.2023).

4. Roy, Geoffrey. (2004). A Risk Management Framework for Software Engineering Practice. 2004. 60-69. 10.1109/ASWEC.2004.1290458.

5. Isaca The Risk IT Framework [Текст] / Isaca — ISACA, 2009 — 107 с.

6. Risk / [Электронный ресурс] // PRINCE2® wiki : [сайт]. — URL: https://prince2.wiki/theme/risk/ (дата обращения: 9.12.2023).

References

1. Project Managers Fail to Help Software Projects (Standish Group Chaos 2020). / [Electronic resource] // Vitality Chicago: [website]. — URL: https://vitalitychicago.com/blog/project-managers-fail-to-help-software-projects-standish-group-chaos-2020 (date of access: 5.12.2023).

2. Risk Management (RSKM) (CMMI-DEV) / [Electronic resource] // Wibas : [website]. — URL: https://www.wibas.com/cmmi/risk-management-rskm-cmmi-dev (date of application: 5.12.2023).

3. EBIOS Risk Manager – The method / [Electronic resource] // Agence nationale de la sécurité des systèmes d'information : [website]. — URL: https://cyber.gouv.fr/en/publications/ebios-risk-manager-method (accessed date: 7.12.2023).

4. Roy, Geoffrey. (2004). A Risk Management Framework for Software Engineering Practice. 2004. 60-69. 10.1109/ASWEC.2004.1290458.

5. Isaca The Risk IT Framework [Text] / Isaca — ISACA, 2009 — 107 p.

6. Risk / [Electronic resource] // PRINCE2® wiki : [website]. — URL: https://prince2.wiki/theme/risk / (date of access: 12/19/2023).

Для цитирования: Иванов Н.С. Подходы к управлению рисками в процессе разработки программного обеспечения // Московский экономический журнал. 2024. № 1. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-1-2024-10/

Московский экономический журнал. № 1. 2024
Moscow economic journal. № 1. 2024
© Иванов Н.С., 2024. Московский экономический журнал, 2024, № 1.