Практическое занятие 11-12: Управление рисками

ДИСЦИПЛИНА	Технологии управления командами разработчиков программного обеспечения
ИНСТИТУТ	Институт перспективных технологий и индустриального программирования
КАФЕДРА	Кафедра индустриального программирования
ВИД УЧЕБНОГО МАТЕРИАЛА	Практические занятия
ПРЕПОДАВАТЕЛЬ	Зарипова Виктория Мадияровна
СЕМЕСТР	3 семестр, 2025-2026 гг.

Тема: Управление рисками в проекте

Цель занятия: Изучить виды рисков ИТ-проектов и их признаки; научиться идентифицировать риски, выделять наиболее вероятные риски для ИТ-проекта, выполнять анализ рисков и составлять стратегии для их решения.

План занятий

- Прочитать теоретическую часть (см. ниже)
- Скачать приложенный файл с примером расчета матрицы рисков в формате Excel
- Посмотреть Пример 1 и Пример 2
- Заполнить
    - СРС - 1 рисками по своему проекту: колонки “Risk event or condition (тригер)” и “Consequence (риск)”
    - СРС-2 оценив начальное влияние рисков
    - СРС-1 заполнить “Risk Modification Plan (план по выходу из зоны риска)”. Учитывайте приоритет рисков при разработке планов.
        - План работы с высокоприоритетными рисками должен быть рассчитан на мониторинг предпосылок возникновения риска и предупреждение риска. Также должны быть указаны мероприятия которые необходимо осуществить если риск все же наступил с зоной ответственности - заказчик должен знать если мероприятия несут для него повышенные финансовые или рабочие издержки
        - План работы со средними рисками должен включать периодический чекап и коррекцию хода проекта. Мероприятия не должны быть долгосрочными или дорогостоящими.

        - План работы с низкоприоритетными рисками должен использовать стратегию игнорирования или замещения. Заказчик должен знать с какими последствиями он может столкнуться в случае наступления риска, в случае необходимости чем заместить пострадавшие части проекта.
    - СРС-2 оценив влияние рисков после плановых мероприятий
    - Заполнить отчет по задаче на странице СРС-1

Итоги работы

При успешном выполнении работы студент должен получить следующие результаты:

- Заполненный на основании перечня и методических указаний шаблон Таблицы рисков (XLS) с указанием
    - Перечень возможных рисков (8-10 шт) для своего проекта
    - Их оценки
    - Предложений по корректировке рисков и их оценки
- Документ с сформированной на основе заполненного шаблона матрицей рисков и выводами по ней
- Ответы на контрольные вопросы

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1. Введение

Управление рисками ИТ-проекта - искусство и наука идентификации, анализа и реагирования на риск в течение жизненного цикла проекта с целью достижения его целей [1][i].

Управление рисками проекта в сфере информационных технологий целесообразно рассматривать как комплекс мер по минимизации влияния потенциальных угроз и усиления влияния возможностей с целью достижения целей ИТ-проекта.[1]

Известно несколько определений понятия «риск»:

Риск - это влияние неопределенности на цели []ii.

Риск – это неопределенное событие или условие, которое, если осуществится, может иметь как негативное, так и позитивное влияние на итоги проекта []iii.

Риск — следствие влияния неопределённости на достижение поставленных целей []iv.

Виды рисков:

- **Известные риски** идентифицируются и подлежат управлению — создаются планы реагирования на риски и резервы на возможные потери.
- **Неизвестные риски** нельзя определить, и, следовательно, невозможно спланировать действия по реагированию на такой риск.

Задача управления рисками ИТ-проектов - это своевременное выявление факторов, связанных с внедрением системы информатизации или автоматизации, что может негативно сказаться на проекте внедрения, а также оптимальное планирование действий по минимизации этих факторов

Цель процесса управления рисками ИТ-проекта - формирование стратегии компании по управлению рисками, основных правил, позволяющих снизить вероятности и воздействия на цели проекта неблагоприятных событий и повысить вероятности и воздействия на цели проекта благоприятных событий.

План управления рисками — документ, разрабатываемый в начале проекта, содержит структуру управления рисками проекта и порядок

---

[1] В мире существует большое число организаций, которые исследуют управление проектами, в т.ч. и управление рисками

- Институт Управления Проектами PMI (США) http://www.pmi.org
- Международная Ассоциация Управления Проектами IPMA (Швейцария) http://www.ipma.ch
- Институт программной инженерии (США) http://www.sei.cmu.edu

выполнения мероприятий в рамках проекта. Этот документ включается в состав плана управления ИТ-проектом.

1.2. 6 этапов процесса управления рисками ИТ-проекта.

1. **Планирование** - определяется стратегия организации процесса, определяются правила взаимодействия.
2. **Идентификация риска** – определение рисков, способных повлиять на проект, и документирование их характеристик. Идентификация эффективнее происходит при наличии подробной *классификации актуальных рисков*.
3. **Оценка рисков** – комплексное мероприятие, цель которого *количественно* (% вероятность возникновения рисков и их последствий) или *качественно* (с привлечением экспертов и вынесением обоснованного оценочного суждения) оценить уровень рисков.
4. **Планирование способов реагирования** – определение действий, способных ослабить отрицательные последствия от рисковых событий. Используется одна из 4 стратегий (уклонение, страхование, минимизация, принятие).
5. **Мониторинг и управление** – это процесс мониторинга выполнения согласованных планов реагирования на риски, отслеживания идентифицированных рисков, выявления и анализа новых рисков и оценки результативности процесса управления рисками на протяжении всего проекта.

Для графического описания процесса управления рисками можно использовать BPMN и IDEF0 модели (Приложение 2., рис.1,2).

Этап 1 Планирование

Базовые планы по проведению операций управления рисками – формируются на совещаниях, разрабатываются элементы стоимости рисков и плановые операции, которые включаются соответственно в бюджет проекта и расписание.

Планирование управления рисками — это процесс принятия решений по определению подходов и планированию операций по управлению рисками проекта.

Цель процесса планирования рисков - обеспечение пропорциональности соотношения между рисками проекта и важностью проекта для организации и других заинтересованных сторон, формирование стратегии компании по управлению рисками, формулировка основных правил, позволяющих управлять рисками проекта.

План управления рисками — документ, разрабатываемый в начале проекта и содержащий описания структуры управления рисками проекта и порядок его выполнения в рамках проекта; включается в состав плана управления проектом

Исходная информация для планирования рисков: факторы внешней среды предприятия, активы организационного процесса (организация может иметь заранее разработанные подходы к управлению рисками).

Процесс планирования начинается сразу после появления замысла проекта и завершается на ранних стадиях проекта. Используются следующие методы: методы экспертной оценки, анализ данных, совещания, анализ заинтересованных сторон. Все методы реализуются в команде проекта.

Этап 2. Идентификация рисков

Идентификация рисков – определение рисков, способных повлиять на проект, и документирование их характеристик (Приложение 2.рис.1.).

Методы идентификации рисков:

Ретроспективный анализ - анализ документов, договоров и реестров рисков ранее завершенных ИТ-проектов, позволяет оперативно выявить уже наступившие риски, которые материализовались и оказали влияние на достижение запланированных целей. Пример: 170 ранее наступивших рисков представлены в *реестре универсальных рисков*. Эти риски являются универсальными, т. е. они актуальны для любого проекта, независимо от его масштаба, сложности, длительности, типа, способов управления и численности участников команды. Вероятные события, которые актуальны исключительно для частного проекта, называются специальными рисками. Для выявления специальных рисков ретроспективный анализ документов не подходит, т. к. требуется использовать творческий подход.

Метод «мозгового штурма», разработанный А. Осборном в 30-х годах XX века, является коллективным методом и может быть использован для идентификации рисков в ИТ-проектах. Основными преимуществами данного метода являются легкость его применения, а также позитивная коллаборация участников. Среди недостатков можно отметить низкий показатель выявления уникальных рисков

Дельфийский метод, создан в 60-е годы XX века сотрудниками RAND Corporation. Изначально разрабатывался, как метод прогнозирования трендов развития технологий, а также возможных сценариев ведения войны. Однако универсальность алгоритма метода позволила использовать его для выявления вероятных проблем. Достоинством дельфийского метода является возможность идентификации уникальных рисков.

SWOT-анализ разработан в 1963 г. Использовался, как метод стратегического планирования деятельности организации. Позднее, с развитием проектной деятельности, сильные стороны стали представляться, как свойства проекта и коллектива, дающие преимущества, слабые стороны – свойства, которые ослабляют проект, возможности – внешние и внутренние факторы, дающие дополнительные преимущества по достижению целей проекта, угрозы – внешние и внутренние факторы, которые способны осложнить процесс достижения проектных целей.

STEEP-анализ дает возможность исследовать социальные, технологические, экономические, экологические и политические риски.

Hazard and Operability Study (HAZOP), автор Т. Клетз, способ идентификации рисков с помощью слов «НЕТ», «БОЛЬШЕ», «МЕНЬШЕ», «ЧАСТЬ» и др. Позднее был доработан

Computer Hazard and Operability Analysis, сокращенно CHAZOP – достоинство: благодаря управляющим словам (НЕТ, БОЛЬШЕ, МЕНЬШЕ и др.) коллективам предоставляется возможность взглянуть на проекты с разных точек зрения.

Structured What-If Technique (SWIFT) – упрощенная версия CHAZOP. Набор фраз, например, таких как «что, если… ?» «к чему это приведет… ?», «что случится, если… ?», «может ли кто-либо… ?», «может ли что-либо… ?» помогает коллективу идентифицировать возможные рисковые события и прогнозировать сценарии того, как будет вести себя проект в случаях их наступления. Достоинства: простота использования (метод не требует предварительной подготовки) и графическое исполнение.

Preliminary Hazard Analysis (PHA) - метод «предварительного анализа опасностей для систем». Направлен на выявление возможных угроз, которые могут причинить вред используемому оборудованию или разрабатываемой системе. Рисковые события группируются на 3 класса. Первый класс – безопасный, т. е. событие не может оказать негативное влияние на проектные цели. Второй класс – пограничный (не вызывает поломки оборудования, отставание от запланированных сроков и др.). Третий класс – критический, например, уход ключевого сотрудника из проекта, отсутствие финансирования и др.

Fault Tree Analysis (FTA) - метод «анализ дерева неисправностей». Это графический метод, который устанавливает взаимосвязь и взаимозависимость между многочисленными рисками с помощью логических схем.

Event Tree Analysis (ETA) - метод «анализ дерева событий». Графический метод, направлен на исследование факторов и источников рисков.

Важно паспортизировать все идентифицированные риски в организации, накапливая базу данных от проекта к проекту. Когда риски и все действия по ним документируются, легко проанализировать, были ли проведенные мероприятия эффективными. Кроме того, сохраняются полученные ценные знания, которые и в будущем можно будет применять.

Паспорт идентифицированного риска представлен в таблице 1.

Таблица 1.

Код риска	**002**
Риск	**Дефецит специалистов**
Ответственный	**Петров И.И.**

Последствия риска	**Превышение сроков реализации проекта**
Приоритет (высокий, средний, низкий)	**Высокий**
Вероятность	**Средняя (3)**
Влияние	**Высокая (4)**
Категория	**Организационный**
Сроки актуальности риска	**Начало проекта – Конец проекта**
Стратегия	**Снижение риска**

Реестр часто встречающихся негативных рисков в ИТ-проектах представлен в Приложении 1. []v

Этап 3. Качественная оценка рисков

Качественные методы – это методы, которые используют экспертные мнения для оценивания характеристик вероятностей и влияний рисков. Как правило, качественные методы применяются, когда наблюдается большая неопределенность, отсутствует необходимая информация и/или нет накопленных статистических данных о ранее наступивших рисках.

Согласно **ГОСТ Р 31010-2011** оцениваются две основные характеристики риска – **вероятность материализации риска** и **возможное влияние в случае его наступления**. Измерение степени вероятности и влияния риска осуществляется с помощью специальных количественных и качественных методов.

Качественные методы применяются для оценивания рисков в следующих случаях:

- в ИТ-проектах наблюдается большая неопределенность,
- имеется вакуум информации,
- в ИТ-организации нет накопленных статистических данных о материализовавшихся ранее рисках,
- время отводимое для планирования на подготовительных этапах ограниченно

При работе с качественными методами оценивая рисков часто используют весовые коэффициенты, базирующиеся на вербально-числовой шкале Харрингтона (табл.2)

Таблица 2.

Степень вероятности наступления риска в проекте	**Коэффициент Харрингтона (согласно PMBoK)**	**Коэффициент Харрингтона**	**Вероятность**

Очень высокая	8-10	5	Риск неизбежен. Гарантированное наступление риска
Высокая	6,4-8	4	Риск вероятен
Средняя	3,7-6,4	3	Нет гарантий, что риск наступит, но все же существует такая возможность
Низкая	2-3,7	2	Есть возможность наступления риска
Очень низкая	0-2	1	Есть потенциальная возможность наступления риска
Нет вероятности	0	0	Риск невозможен

Коэффициенты Харрингтона используются для расчета величины «подверженность риску» - это характеристика риска, которая показывает предрасположенность проекта к наступлению рискового события.

$$RE = P_r \times I_m,$$

Где P_r - вероятность наступления рискового события, I_m - влияние рискового события.

Матрица вероятности и воздействия — это инструмент, используемый в качественном анализе рисков для определения приоритетности рисков и разработки стратегий по их смягчению или управлению. Используется 2 числовых шкалы:

- оценка *вероятности* возникновения рискового события,
- потенциальное *воздействие (влияние),* которое окажет рисковое событие.

Вероятность риска оценивается по шкале от 1 до 5. Вероятность считается очень низкой, если она имеет значение менее 10% - присваивается значение (1); низкой, если ее значение от 10 до 25 % (2); средней при значениях от 25 до 50% (3); высокой, если значение колеблется от 50 до 75% (4); очень высокой при значениях более 75% (5).

Потенциальное влияние, которое окажет рисковое событие можно оценить по совокупности следующих параметров: **Sc**ope (объем), **Q**uality (качество), **C**ost (расходы), **E**ffort (усилие), **D**uration (продолжительность), **R**eputation (репутация), **So**cial Responsibility (социальная ответственность). Каждый из этих параметров можно оценить по целочисленной шкале от 1 до 5, пользуясь таблицей 3.

Результирующее **потенциальное влияние** определяется как среднее значение совокупности всех параметров, округленное до десятичных значений:

$$I_m = \text{ср. знач.} \left(\frac{\sum Sc+Q+C+E+D+R+So}{6} \right), \qquad (2)$$

Таблица 3.

	Scope **(объем)**	***Quality*** **(качество)**	***Cost*** **(расходы)**	***Effort*** **(усилие)**	***Duration*** **(продолжи-тельность)**	***Reputation*** **(репутация)**	***Social Responsibility*** **(социальная ответственность**
Low Impact **(низкое влияние)**	*Minor areas of scope are affected* (Затронуты незначительные области применения)	*Minor quality problems* (Небольшие проблемы с качеством)	*Less than 1 % cost impact* (Влияние на стоимость менее 1 %)	*Less than 2% extra days effort* (Менее 2 % дополнительных дней работы)	*Delay of up to 3%* (Задержка до 3%)	*Very minor impact to enterprise's reputation* (Очень незначительное влияние на репутацию предприятия)	Minor impediment (Незначительная мера социальной ответственности)
Medium Impact **(среднее влияние)**	*Major areas of scope are affected, but workarounds are feasible* (Затронуты основные области применения, но возможны обходные пути)	*Significant quality issues, but the product is still usable* (Серьезные проблемы с качеством, но продукт еще можно использовать)	*More than 1 % but less than 3% impact* (Влияние более 1 %, но менее 3 %)	*2%-10% extra days effort* (2%-10% дополнительных дней работы)	*Delay of 3%-10%* (Задержка от 3% до 10%)	*Moderate impact to enterprise's reputation* (Умеренное влияние на репутацию предприятия)	Major impediment (Средняя мера социальной ответственности)
High Impact **(высокое влияние)**	*The product does not meet the business need* (Продукт не соответствует потребностям бизнеса)	*The product is not usable* (Продукт непригоден к использованию)	*More than 3% impact* (Влияние более 3%)	*More than 10% extra days effort* (Более 10% дополнительных дней работы)	*Delay of more than 10%* (Задержка более 10%)	*Severe impact to enterprise's reputation* (Серьезный удар по репутации предприятия)	Severe impediment (Очень значительная мера социальной ответственности)

Практическое задание

Задание 1. Построить таблицу-перечень возможных рисков (8-10 шт) в соответствии разрабатываемом вами проектом. Оценить вероятность каждого риска по 5-ти бальной шкале (вероятность может принимать дробные значения с точностью до 0,1). Риски выбрать из таблицы Приложения 1 или сгенерировать самостоятельно. Согласовать таблицу с преподавателем. Разработайте стратегию управления рисками, т.е. разработайте план по выходу из зоны риска, предусмотрев для каждого риска 2-5 мероприятий.

Таблица-перечень возможных рисков проекта «*Название проекта***»**

№	Рисковое событие или состояние	Последствия	План по выходу из зоны риска
1	Кол-во негативных обращений на портал после внедрения выросло на 30%	Уровень доверия клиентов к продукту уменьшится, что приведет к утрате пользователей минимум на 10% от уровня до внедрения системы	1. перед началом разработки провести доп. анализ сущности обращений 2. определить топ-3 проблемы, с которыми чаще всего сталкивается клиент 3. внести в план разработки доп.аспекты для минимизации нагрузки по определенным критичным зонам
2			
3			
4			

Задание 2. Загрузите шаблон электронной таблицы Excel для оценки начальных рисков вашего проекта и разработки плана по выходу из зоны риска. Таблица включает 4 листа:

1. Пример 1 – Риски
2. Пример 2 – Влияние
3. СРС 1 – Риски (лист для самостоятельной работы)
4. СРС 2 – Влияние (лист для самостоятельной работы)

На листах 1 и 2 показан пример заполнения таблиц. Листы 3 и 4 предназначены для самостоятельной работы по оценке рисков вашего проекта.

Задание 3. Заполните на листе 3 перечень рисков вашего проекта, ожидаемые последствия проявления рискового события и план мероприятий по выходу из зоны риска. На листе 4 автоматически должен отобразиться перечень рисков в двух таблицах:

1. Начальные значения параметров для оценки влияния
2. Оценка влияния после введения мероприятий по снижению риска

Задание 4. На листе 4 «СРС 2 – Влияние» в таблице «Начальные значения параметров для оценки влияния» проведите анализ потенциального влияния рисков, используя таблицу 3 методички и рассчитайте I_m по формуле (2). Сравните с значениями влияния в столбце I таблицы. Расчет должны совпасть. Обратите внимание на расцветку ячеек столбца I. Сделайте выводы о том какие из рисков оказывают наибольшее влияние на ваш проект.
Задание 5. Расчетные значения I_m должны автоматически отразиться в таблице на листе 3 «СРС 1 – Риски», столбец E «(Влияние)».
Задание 6. Оцените вероятность каждого риска с точность до 0,1 по пятибальной шкале. Используйте собственные экспертные оценки. Заполните столбец D в таблице «СРС 1 – Риски».
Задание 7. Рассчитайте величину «**подверженность риску**» по формуле (1) и сравните с расчетами в таблице «СРС 1 – Риски», столбец F «Подверженность риску». Сделайте вывод какие риски наиболее опасны для вашего проекта.
Задание 8. Оцените вероятность риска и его потенциальное влияние после применения плана корректировки рисков. Для этого заполните данные в таблице «Оценка влияния после введения мероприятий по снижению риска» на листе «СРС 2 – Влияние». Экспертно оцените снижение вероятности возникновения каждого риска в результате принятых мероприятий (заполните столбец H «Вероятность риска после применения плана» в таблице «СРС 1 – Риски». Сделайте выводы как повлияют проведенные мероприятия на снижение рисков вашего проекта.
Задание 9. Результаты выполнения практического задания запишите в отчет. В отчете укажите какие риски наиболее опасны для вашего проекта, а какими можно пренебречь? Обоснуйте свои выводы.

Контрольные вопросы

1. Дайте характеристику процессов управления рисками проекта.
2. Типичные риски ИТ-проектов. Основные признаки риска.
3. Методы реагирования на негативные риски (уклонение, передача, снижение, принятие).
4. Реестр рисков ИТ-проекта. Идентификация рисков.
5. Охарактеризуйте процесс идентификации рисков проекта.
6. Основные задачи качественного анализа рисков ИТ-проекта.
7. В чем отличие качественного и количественного анализа рисков.
8. Опишите процесс планирования реагирования на риски.

Приложение 1

Реестр негативных рисков ИТ-проектов

№	НАЗВАНИЕ РИСКА	Вер-ть	Влияние
1	Риск изменения требований в процессе реализации ИТ-проекта	4,2	4,4
2	Риск того, что по факту ИТ-проект будет значительно сложнее, чем предполагалось изначально	2,8	2,9
3	Риск длительного изучения бизнес-процессов заказчика	3,1	3,4
4	Риск несвоевременного завершения работы	4,8	3,9
5	Риск отсутствия связи с субподрядом и (или) поставщиком	4,3	3,2
6	Риск низкого качества предоставляемых работ	3,7	4,2
7	Риск того, что фактическое время работы коллектива будет менее 8 часов в день	4,3	2,7
8	Риск отсутствия у коллектива знаний, навыков и опыта, необходимых для реализации требований ИТ-проекта	3,1	4,5
9	Риск отсутствия актуальной информации, необходимой для разработки ИТ-проекта	4,3	4,1
10	Риск отсутствия знаний, навыков и опыта у руководителя ИТ-проекта	3,7	4,9
11	Риск ухода руководителя ИТ-проекта	3,1	4,3
12	Риск ухода ключевых сотрудников	3,6	4,8
13	Риск перегрузки людских ресурсов (переработка, работа сверхурочно и т. п.)	3,8	3,9
14	Риск допущения ошибок коллективом в вопросах управления временем	4,1	3,1
15	Риск нечеткой формулировки целей ИТ-проекта (не по SMART)	3,9	4,9
16	Риск отсутствия плана-графика	2,8	4,1
17	Риск ошибочной оценки сроков, необходимых для реализации ИТ-проекта	4,1	2,9
18	Риск ошибочной оценки ресурсов, необходимых для реализации ИТ-проекта	4,6	3,1
19	Риск ошибочной оценки бюджетов, необходимых для реализации ИТ- проекта	4,6	3
20	Риск занятости руководителя ИТ-проекта на других проектах	4,3	2,6
21	Риск занятости участников коллектива на других ИТ-проектах	4,6	3,5
22	Риск отсутствия устава ИТ-проекта	4,2	4,1

№	НАЗВАНИЕ РИСКА	Вер-ть	Влияние
23	Риск изменения состава участников проектной команды в процессе реализации ИТ-проекта	4,7	4
24	Риск низкой производительности труда руководителя ИТ-проекта	3,5	4,1
25	Риск низкой мотивации руководителя ИТ-проекта	2,8	4,7
26	Риск временной задержки в получении ответов на задаваемые вопросы между участниками проекта	0,4	3
27	Риск поломки оборудования	1,2	3,6
28	Риск неэффективного использования инструментария управления проектами (диаграмма Ганта, Microsoft Project и т. п.)	0,4	2,6
29	Риск применения ранее не используемых технологий	2,3	4
30	Риск отсутствия классического способа реализации проекта (agile, waterfall и др.)	2,3	3,7
31	Риск низкого качества разработанного продукта	2,3	4,5
32	Риск допущения ошибок при заключении договора(-ов) и других юридических документов	1,4	4,6
33	Риск промышленного шпионажа	0,3	3,9
34	Риск ограбления	1,5	4,9
35	Риск утечки конфиденциальных данных	1,3	4,8
36	Риск судебного иска от заказчика(-ов)	1,4	3,5
37	Риск судебного иска от субподрядчика(-ов), поставщика(-ов) и т.п.	1,2	3,8
38	Риск получения штрафа(-ов) со стороны фискальных государственных органов	1,4	4,8
39	Риск влияния от действий конкурентов	2	2,7
40	Риск отсутствия спроса у конечного потребителя	1,7	4,1
41	Риск использования чужих авторских прав	0,3	4,8
42	Риск неудовлетворенности заказчика работой руководителя проекта	1,1	3,6
43	Риск неудовлетворенности заказчика качеством разработанного продукта	1,7	5
44	Риск неудовлетворенности заказчика сроками реализации ИТ-проекта	2,1	4,8
45	Риск неудовлетворенности заказчиком содержанием ИТ-продукта	0,6	5
46	Риск влияния геополитических факторов	0,2	5

№	НАЗВАНИЕ РИСКА	Вер-ть	Влияние
47	Риск влияния стихийных бедствий (пожар, наводнение, ураган и т. п.)	0,2	5
48	Риск отсутствия необходимых ресурсов	2,4	3,7
49	Риск умышленного вредительства ИТ-проекту	1,1	3,5
50	Риск низкой загрузки человеческих ресурсов	0,6	3,6
51	Риск того, что заказчик не сможет оплатить трудозатраты коллектива, работающего по системе оплаты T&M	2,1	3
52	Риск отсутствия финансирования	1,4	4,1
53	Риск задержки выплаты заработных плат	0,8	4,2
54	Риск неправильного ранжирования задач руководителем ИТ-проекта	2,1	3,7
55	Риск отсутствия технического задания	2,1	3,8
56	Риск выявления скрытых, не обнаруженных на этапе планирования источников дополнительных затрат	4,3	2,2
57	Риск завышения качества руководителем ИТ-проекта	4,4	1,7
58	Риск изменения в налоговом законодательстве	3,1	1,8
59	Риск изменения валютного курса	4,2	0,6
60	Риск изменения банковских процентных ставок	3,8	0,8
61	Риск отсутствия связи с заказчиком	3,8	2,1
62	Риск временной задержки в получении ответов на задаваемые заказчику проекта вопросы	3,6	1,9
63	Риск непонимания у коллектива того, какой продукт должен получиться по завершении ИТ-проекта	4,2	2,3
64	Риск ухода на «больничный»	4,7	1,3
65	Риск форс-мажоров	4,4	M
66	Риск неэффективного использования инструментария управления проектами (диаграмма Ганта, Microsoft Project и т.п.)	2,8	1,7
67	Риск отсутствия спецификации ИТ-проекта	4,1	2,2
68	Риск отставания от запланированных сроков	5	2,1
69	Риск не учета отпусков и государственных праздников при создании плана-графика ИТ-проекта	4	2,1
70	Риск нескоординированных действий проектной команды	3,5	2,1

№	НАЗВАНИЕ РИСКА	Вер-ть	Влияние
71	Риск низкой производительности труда проектной команды	3	0,9
72	Риск низкой мотивации проектной команды	3,4	0,6
73	Риск негативной социально-психологической атмосферы внутри коллектива	2,6	2,2
74	Риск допущения ошибок при реализации ИТ-проекта (bugs)	4,4	2,1
75	Риск недостатка коммуникаций между участниками проекта	2,6	2,1
76	Риск длительного согласования заинтересованными сторонами информации при выработке управленческих решений	3,4	2,1
77	Риск использования устаревших технологий	1,5	2,4
78	Риск отключения электричества	0,3	2,1
79	Риск отключения интернета	0,2	1,9
80	Риск переизбытка каналов коммуникаций, доносящих актуальную информацию	1,4	0,8
81	Риск отсутствия у коллектива заинтересованности в успешном завершении ИТ-проекта	2,1	1,8
82	Риск отсутствия общего видения конечного ИТ-продукта	1,4	2,2
83	Риск отсутствия полной (частичной) предоплаты	0,4	1,7

Приложение 2.

Структурное изображение процесса управления рисками

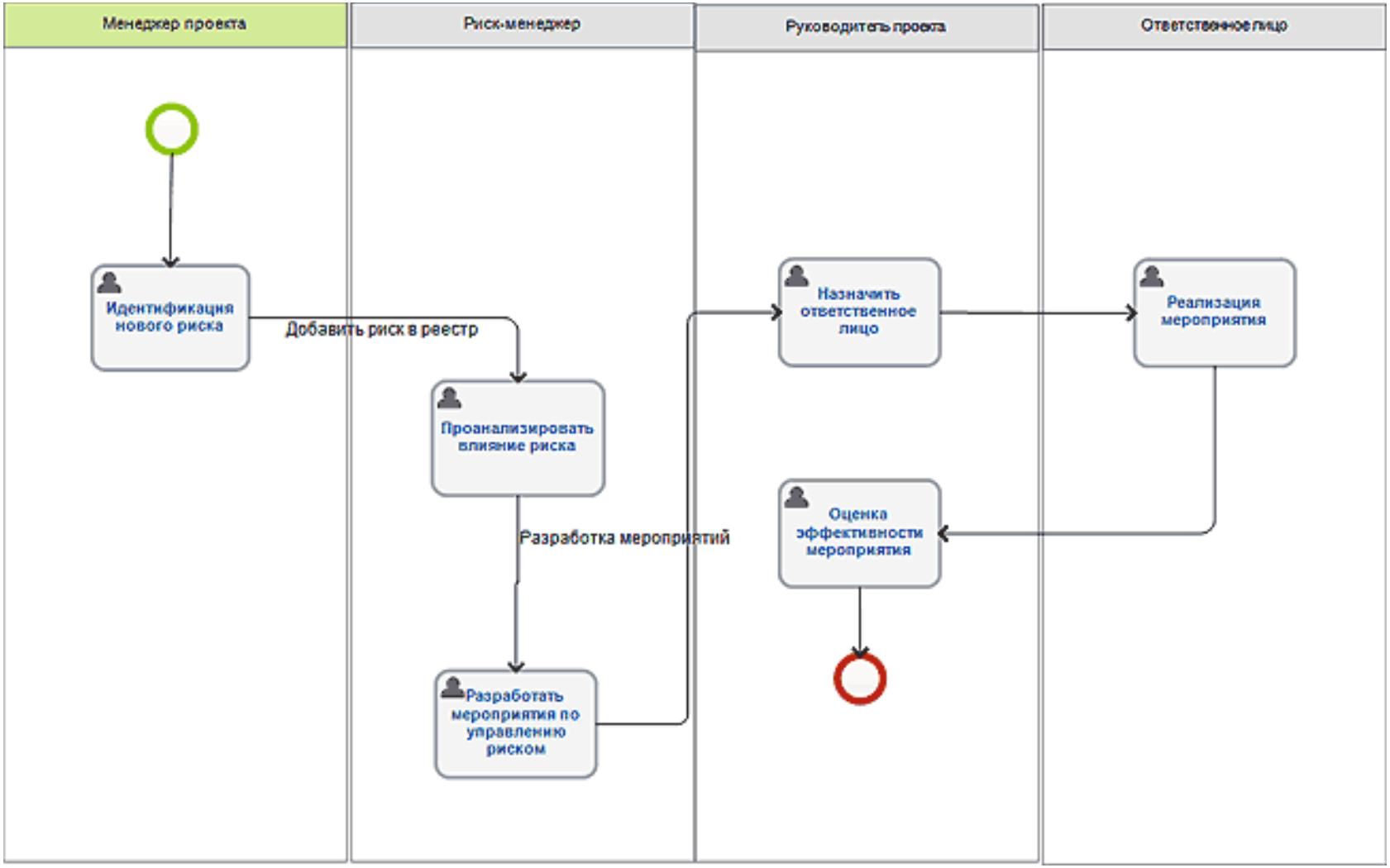

Рис.1. BPMN диаграмма процесса управления новым риском.

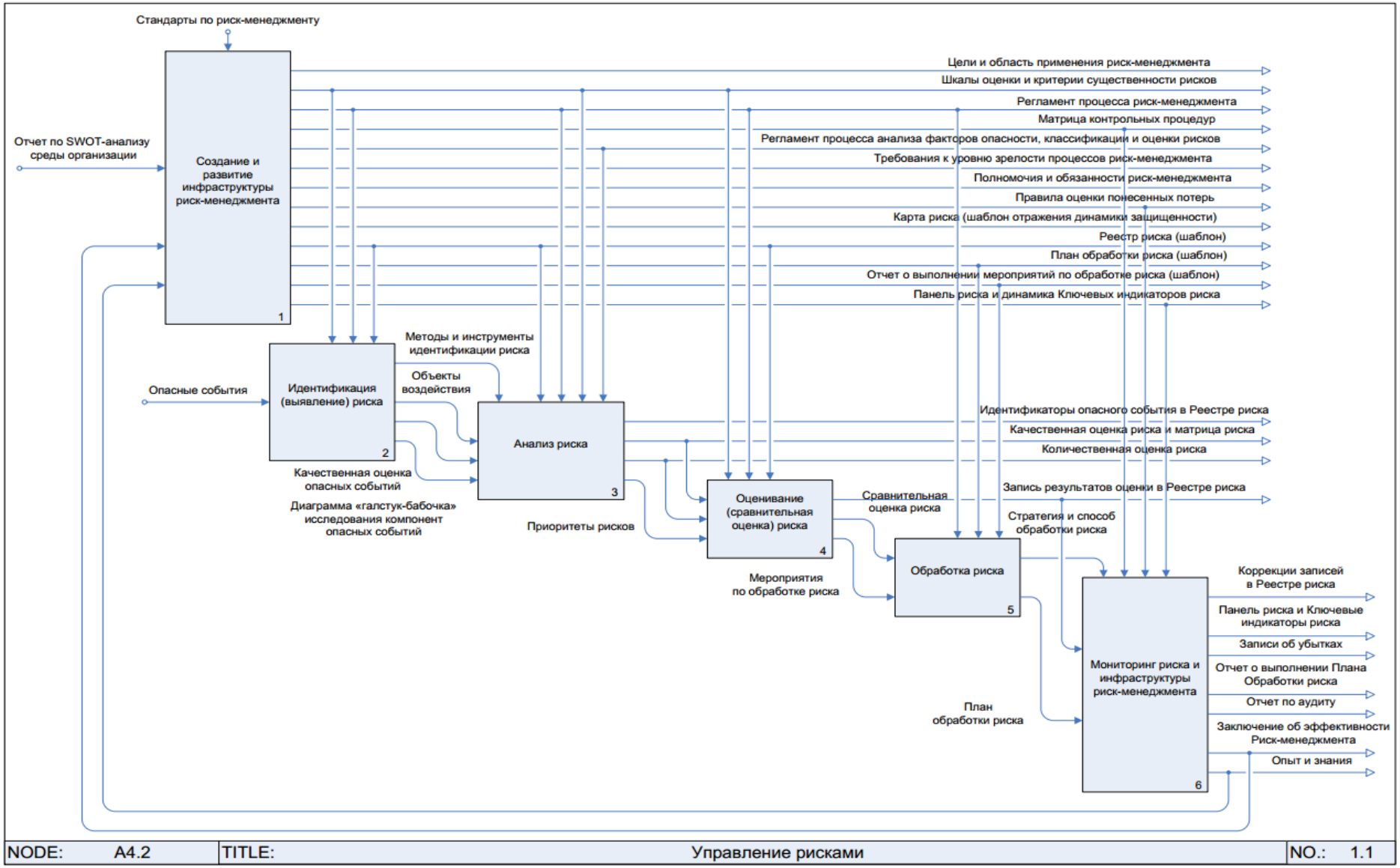

Рис.2. *DEF0-модель процесса менеджмента риска*

Литература

1. [i] Schwalbe K. Information technology project management /K. Schwalbe //Cengage Learning, 2018
2. [ii] ISO 31000:2018 Risk management Guidelines
3. iii Project Management Body Of Knowledge, PMBOK
4. iv ГОСТ Р 51897-2011
5. v Николаенко В.С. Управление рисками ИТ- проектов в организациях, дис. канд. экон. наук: 08.00.05: , Томск, 2021.