УПРАВЛЕНИЕ РИСКОМ

ПОДГОТОВИЛИ АГЕЕВА ЕЛЕНА И МЕКАЕВ АНДРЕЙ
ФМЭСИ, ГР.437

ЭТАПЫ УПРАВЛЕНИЯ РИСКАМИ

1. Идентификация риска
2. Анализ риска
3. Ранжирование риска
4. Планирование управления риском
5. Разрешение риска
6. Наблюдение риска

ПЛАНИРОВАНИЕ УПРАВЛЕНИЯ РИСКОМ

Управление рисками - это определенная деятельность, которая выполняется в проекте от его начала до завершения. Как и любая другая работа в проекте управление рисками требует времени и затрат ресурсов. Поэтому эта работа обязательно должна планироваться.

Планирование управления рисками — это процесс определения подходов и планирования операций по управлению рисками проекта. Тщательное и подробное планирование управления рисками позволяет:

- выделить достаточное количество времени и ресурсов для выполнения операций по управлению рисками
- определить общие основания для оценки рисков
- повысить вероятность успешного достижения результатов проекта

Планирование управления рисками должен быть завершено на ранней стадии планирования проекта, поскольку оно крайне важно для успешного выполнения других процессов.

ПЛАНИРОВАНИЕ УПРАВЛЕНИЯ РИСКОМ

Рис.1. Пример иерархической структуры рисков проекта

ИДЕНТИФИКАЦИЯ РИСКА

Риск – сочетание вероятности и последствий наступления неблагоприятных событий.

Идентификация рисков — это выявление рисков, способных повлиять на проект, и документальное оформление их характеристик.

Исходные данные для выявления и описания характеристик рисков могут браться из разных источников.

- база знаний организации
- информация из открытых источников, научных работ, маркетинговая аналитика и другие исследовательские работы в данной области

Каждый проект задумывается и разрабатывается на основании ряда гипотез, сценариев и допущений. Как правило, в описании содержания проекта перечисляются принятые допущения.

ИДЕНТИФИКАЦИЯ РИСКА

Для сбора информации о рисках могут применяться различные подходы. Среди этих подходов наиболее распространены:

- Опрос экспертов
- Мозговой штурм
- Метод Дельфи
- Карточки Кроуфорда

Результатом идентификации рисков должен стать список рисков с описанием их основных характеристик: причины, условия, последствий и ущерба.

АНАЛИЗ РИСКА

Существует два подхода к анализу рисков:

- Качественный
- Количественный

Качественный анализ рисков включает в себя расстановку рангов для идентифицированных рисков. При анализе вероятности и влияния предполагается, что никаких мер по предупреждению рисков не производится.

Качественный анализ рисков включает в себя:

- Определение вероятности реализации рисков.
- Определение тяжести последствий реализации рисков.
- Определения ранга риска по матрице «вероятность — последствия».
- Определение близости наступления риска.
- Оценка качества использованной информации.

АНАЛИЗ РИСКА

Табл.1. Матрица рангов главных выявленных рисков проекта (пример)

Причина	Вероятность	Воздействие	Ранг
Требования не ясны	Очень вероятно	Катастрофические	9
Недостаток квалифицированных кадров	Очень вероятно	Критичные	6
Текучесть кадров	Возможно	Критичные	4

АНАЛИЗ РИСКА

Рис.2. Ранг риска и матрица вероятностей и последствий

АНАЛИЗ РИСКА

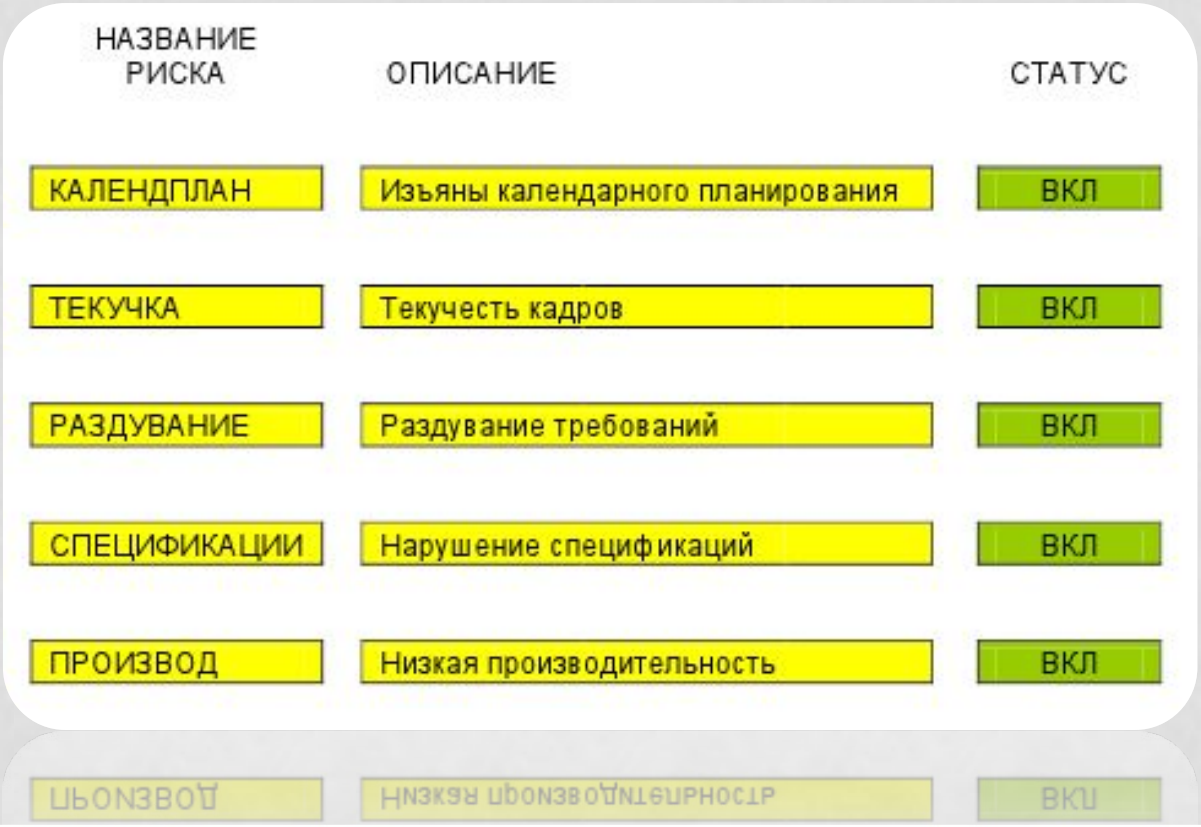
Количественный анализ производится в отношении тех рисков, которые в процессе качественного анализа были квалифицированы как имеющие высокий и средний ранг.

Для количественного анализа рисков могут быть использованы следующие методы:

- Анализ чувствительности.
- Анализ дерева решений.
- Моделирование и имитация.

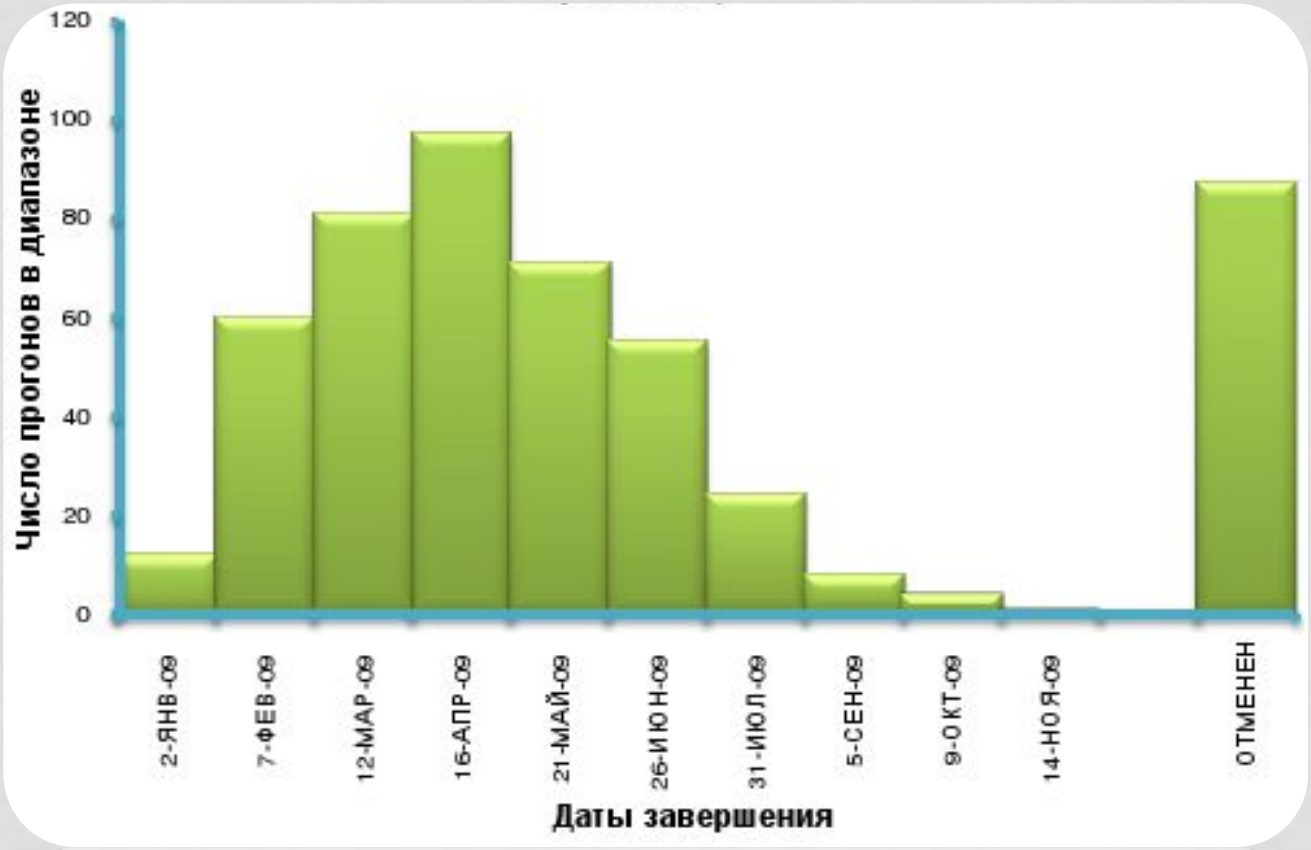
АНАЛИЗ РИСКА

Рис.3. Пять основных факторов риска программного проекта, учитываемые в модели Riskology



АНАЛИЗ РИСКА

Рис.4. Гистограмма распределения возможного срока завершения проекта, рассчитанная по результатам моделирования методом Монте-Карло



ПЛАНИРОВАНИЕ РЕАГИРОВАНИЯ НА РИСКИ

Планирование реагирования на риски — это процесс разработки путей и определения действий по увеличению возможностей и снижению угроз для целей проекта. Данный процесс начинается после проведения качественного и количественного анализа рисков.

Возможны четыре метода реагирования на риски:

- Уклонение от риска
- Передача риска
- Снижение рисков
- Принятие риска

РАЗРЕШЕНИЕ РИСКА

Разрешение риска – это управление проектом, направленное на снижение рисков, что позволяет существенно снизить неопределенность на ранних стадиях проекта.

Снижение степени риска - это сокращение вероятности и объема потерь. Для снижения степени риска применяются различные приемы. Наиболее часто в мировой практике управления бизнесом применяют следующие способы снижения риска:

- диверсификацию
- лимитирование
- страхование
- хеджирование
- резервирование средств

НАБЛЮДЕНИЕ РИСКА

Управление рисками должно осуществляться на протяжении всего проекта.

Мониторинг и управление рисками — это процесс идентификации, анализа и планирования реагирования на новые риски, отслеживания ранее идентифицированных рисков.

Мониторинг и управление рисками включает в себя следующие задачи:

- Пересмотр рисков.
- Аудит рисков.
- Анализ отклонений и трендов.

ПРОГРАММНЫЕ ПРОДУКТЫ

Продукт	Описание
RA2 art of risk **AEXIS Security Consultants** **XiSEC Consultants Ltd**	В RA2 art of risk реализован простой для понимания процессный подход. Процесс управления рисками может настраиваться под потребности конкретной организации. Для успешной оценки и управления рисками необходимо собирать информацию из различных источников в организации. RA2 art of risk включает специальный модуль - RA2 Information Collection Device, который может быть установлен в любом месте в организации для сбора информации для процесса оценки рисков. Когда процесс проектирования и внедрения СУИБ завершается RA2 art of risk позволяет создать архив для хранения результатов этого процесса. Эти результаты могут быть взяты за основу для проведения следующей оценки рисков. RA2 является эффективной системой поддержки принятия решений по управлению информационными рисками для современного бизнеса.
vsRisk **IT Governance** **Vigilant Software**	•Программное обеспечение для оценки рисков информационной безопасности в соответствии с требованиями стандартов ISO 27001 и BS 7799-3. vsRisk Risk Assessment Tool - это совершенно новый и уникальный в своем роде инструмент для оценки рисков: Разработан в четком соответствии с ISO/IEC 27001 •Позволяет оценивать риски нарушения конфиденциальности, целостности, и доступности информации для бизнеса, а также с точки зрения соблюдения законодательства и контрактных обязательств •Поддерживает множество международных стандартов •Содержит интегрированную, регулярно обновляемую базу данных угроз и уязвимостей, соответствующую требованиям BS7799-3

ПРОГРАММНЫЕ ПРОДУКТЫ

Продукт	Описание
Callio Secura 17799 Callio Technologies	Компания Callio Technologies специализируется в области разработки продуктов анализа информационных рисков и управления информационной безопасностью в соответствии с требованиями стандартов BS7799/ISO17799. Callio Secura 17799 представляет собой инструмент для разработки, внедрения, управления и сертификации Системы Управления Информационной Безопасностью (СУИБ) на основе международного стандарта ISO 17799 / BS 7799.
CRAMM Insight Consulting Limited CRAMM User Group	Метод анализа и управления рисками CRAMM и соответствующий программный инструментарий, является правительственным стандартом Великобритании и широко распространен во всем мире. CRAMM реализует комплексный подход к оценке рисков, сочетая количественные и качественные методы оценки. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний. Для коммерческих организаций имеется Коммерческий профиль, для правительственных организаций – Правительственный профиль.
РискМенеджер Институт системного анализа РАН	РискМенеджер - система автоматизации управления рисками, аудита, контроля, мониторинга безопасности банковских и других критических систем, инфраструктур и бизнес-процессов. Система «РискМенеджер-Анализ» автоматизирует: Построение моделей угроз, моделей событий рисков, оценки рискообразующих потенциалов угроз, объектов, организационных структур, бизнес-процесов; Построение моделей защиты, моделей влияния средств защиты на изменение безопасности системы, расчета рископонижающих потенциалов мер защиты, выбора наиболее эффективных комплексов мер защиты по критерию эффективность-стоимость; Расчет рисков нарушения безопасности, расчет остаточных рисков после применения возможных вариантов комплексов мер защиты; Контроль качества требований к безопасности системы на актуальность, полноту, непротиворечивость; отсутствие дублирования, влияния на конкурентоспособность организации и обоснование внесения изменений в системы требований к безопасности.

ПРОГРАММНЫЕ ПРОДУКТЫ

Продукт	Описание
RiskWatch RiskWatch Inc.	RiskWatch фактически является американским стандартом в области анализа и управления рисками. Аналогично методу CRAMM, RiskWatch использует в качестве критериев для оценки и управления рисками предсказания годовых потерь (Annual Loss Expectancy – ALE) и оценку возврата от инвестиций (Return on Investment – ROI).
COBRA Risk Associates	COBRA - Consultative Objective and Bi-Functional Risk Analysis является средством анализа рисков и оценки соответствия стандарту BS7799, реализующим методы количественной оценки рисков, а также инструменты для консалтинга и проведения обзоров безопасности. При разработке инструментария COBRA были использованы принципы построения экспертных систем и обширная база знаний по угрозам и уязвимостям и большое количество вопросников. В семейство программных продуктов COBRA входят также COBRA ISO17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant.
Buddy System Countermeasures Corp.	Buddy System является программным продуктом, позволяющим осуществлять как количественный, так и качественный анализ рисков. Содержит развитые средства генерации отчетов. Основной акцент делается на информационные риски, связанные с нарушением физической безопасности и управление проектами.

ПРОГРАММНЫЕ ПРОДУКТЫ

Продукт	Описание
MethodWare MethodWare	Компания MethodWare разработала свою собственную методику оценки и управления рисками и выпустила ряд соответствующих инструментальных средств. К этим средствам относятся: ПО анализа и управления рисками Operational Risk Builder и Risk Advisor. Методика соответствует австралийскому стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) и стандарту ISO17799. Risk Advisor позиционируется как инструментарий аналитика или менеджера в области информационной безопасности. Реализована методика, позволяющая задать модель информационной системы с позиции информационной безопасности, идентифицировать риски, угрозы, потери в результате инцидентов. Основными этапами работы являются: описание контекста, определение рисков, оценка угроз и возможного ущерба, выработка управляющих воздействий и разработка плана восстановления и действий в чрезвычайных ситуациях.
Proteus InfoGov	Proteus - мощная система для поддержки процессов СУИБ, включающая в себя средства контроля соответствия , оценки влияния на бизнес, оценки рисков, управления непрерывностью бизнеса, управления инцидентами, управления активами и организационными ролями. Движок Контроля соответствия (Compliance engine) поддерживает любые стандарты (международные, отраслевые и корпоративные) и поставляется вместе с набором шаблонов опросников. Система масштабируется от однопользовательской версии до многопользовательской, позволяющей управлять информационной безопасностью в крупнейших международных корпорациях. Все действия, производимые в системе, регистрируются в журнале аудита. Система позволяет проводить онлайн аудиты во внутренних подразделениях и у внешних поставщиков