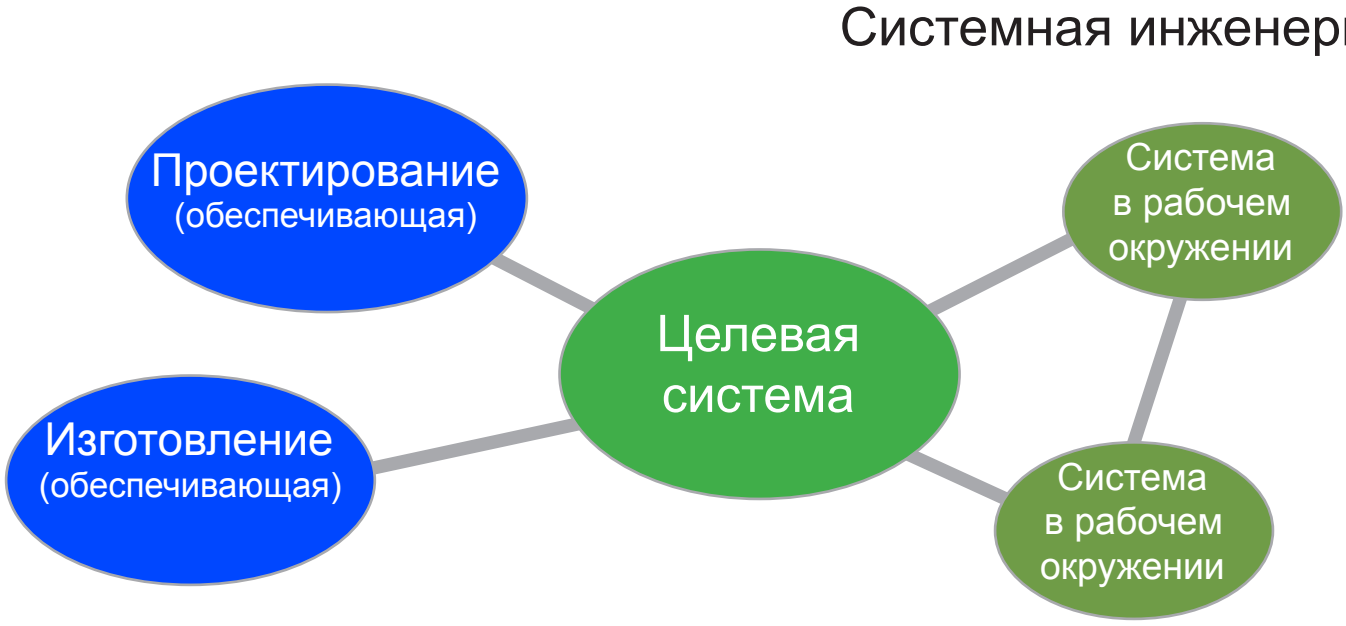
Разработка регламента обеспечения безопасности объектов любой природы

- Что такое “опасность”?
- Что такое “регламент”?
- Что значит “любой природы”?
- Что значит “обеспечить”?



Слайд 1. Постановка задачи

Год назад передо мной была поставлена следующая задача: "Разработать регламент обеспечения безопасности объектов любой природы". В сегодняшнем докладе я расскажу о результатах этой работы.

По формулировке задачи можно сразу поставить ряд важных вопросов:

Что такое "опасность"? Опасность для кого или чего?

Что такое "регламент"? Относится ли он только к проектирующей организации или также нужен регламент для других участников? Зависит ли регламент от устройства объекта?

Что значит "любой природы"? Будет ли регламент одинаков для офисного здания и автомобиля?

Что значит "обеспечить"? Кто ответственен за обеспечение безопасности?

Поиск ответов на эти вопросы привел меня к системной инженерии, которая абстрагируется от физической природы объектов, предоставляя единую дисциплину мышления и практики творения сложных систем.

Системная инженерия

- мыслить о многих связанных системах
- справляться со сложностью объектов
- учитывать множественность точек зрения
- сотрудничать

- сдвигает момент принятия решений на ранние этапы - моделирование

Слайд 2. Системная инженерия

Системная инженерия помогает мыслить о многих связанных системах, справляться со сложностью объектов, учитывать множественность точек зрения и сотрудничать в мультидисциплинарной команде.

Опыт сообщества системных инженеров подтверждает верность изображенной на слайде кривой МакЛими и потому принятие решений стараются сдвинуть на ранние этапы разработки, что приводит к необходимости работы с моделями.

Системная инженерия

Междисциплинарный подход и средства, необходимые для создания успешных систем.

Подразумевается рациональность поведения людей

СИ сосредоточена на определении потребностей клиентов и необходимых функциональных возможностей на ранних этапах разработки, на документировании требований и на последующем синтезе проектных решений и валидации системы при условии рассмотрения проблемы в целом: применение системы, затраты и графики работ, характеристики, обучение и сопровождение, испытания, производство, а также прекращение использования и утилизация. СИ принимает во внимание как деловые, так и технические потребности всех клиентов и ЗС с целью предоставления качественной продукции, отвечающей нуждам и потребностям пользователей

INCOSE Systems Engineering Handbook, v.3.2.2. - October 2011

Слайд 3. Системная инженерия

Актуальное определение системной инженерии звучит так: это «Междисциплинарный подход и средства, необходимые для создания успешных систем»
Подход – это то, как мы мыслим мир, что в нем видим.
Средства – это то, как мы работаем с миром. Это практики, применяемые в инженерных проектах.

В уточняющем определении приведены эти практики: выявление потребностей, управление требованиями, синтез проектных решений, производство, испытания, эксплуатация, прекращение использования – то, что называют жизненным циклом системы.

Успех достигается, когда продукт творчества отвечает нуждам (drive, motive) и потребностям пользователей (demand).

Стоит отметить, что в данном определении есть неявное предположение, что пользователи рациональны и действуют в соответствии со своими нуждами и потребностями.

Состав представления метода (по ISO 24744)

- практики
- рабочие продукты
- языки/нотации моделирования
- жизненный цикл целевой системы
- организация

ISO/IEC 24744 Software Engineering — Metamodel for Development Methodologies

Слайд 4.

Регламент является воплощением метода, который описывает КАК делать.
Согласно стандарту ИСО 24744 состав представления метода следующий:

- практики, выполняемые на протяжении жизненного цикла
- участвующие рабочие продукты
- используемые языки/нотации моделирования информации
- стадии жизненного цикла целевой системы
- организация (профессиональные роли и инструменты)

25 обязательных практик системной инженерии по ISO 15288:2008

Соглашения
- приобретения
- поставки

Предприятия
- управление жизненным циклом
- управление средой предприятия
- управление инвестициями
- управление ресурсами
- управление качеством

Проекта

Управление проектами
- планирование проекта
- оценки и контроля проекта

Поддержка проектов
- управление принятием решений
- управление рисками
- управление конфигурацией
- управление информацией

Технические
- определение требований
- анализ требований
- проектирование архитектуры
- реализация (изготовление) элементов
- комплексирование (сборка)
- верификация (проверка)
- передача в эксплуатацию
- валидация (приёмка)
- функционирование (эксплуатация)
- обслуживание
- изъятие и списание (вывод из эксплуатации)

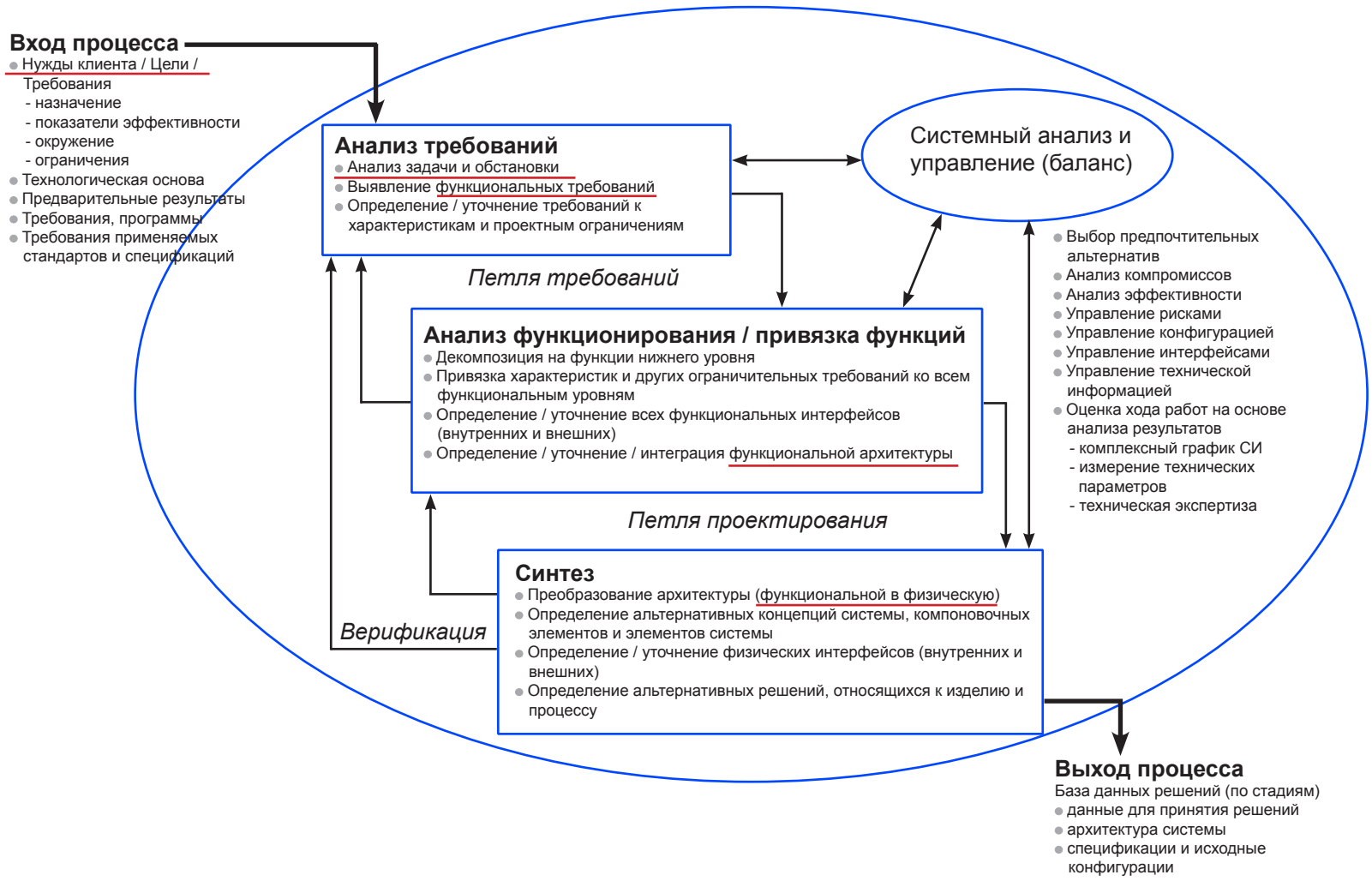
Обеспечивают

ISO/IEC 15288:2008 Systems and software engineering — System life cycle processes. Левенчук А.И.

Слайд 5-6.
Пойдем по порядку, начав с практик.

В ключевом стандарте системной инженерии ИСО 15288 выделено 25 обязательных практик, приведенных на данном слайде. Помимо технических или инженерных практик, таких как сбор и анализ требований, проектирование архитектуры, верификация, сюда включены практики проектного менеджмента и обеспечивающие практики, такие как управление персоналом. В целях разработки регламента мы сосредоточились на технических практиках.

Технические практики проектирования



Legacy DoD Systems Engineering Process Model, MIL-STD-499B (1993г.). Пер. Батоврин В.К.

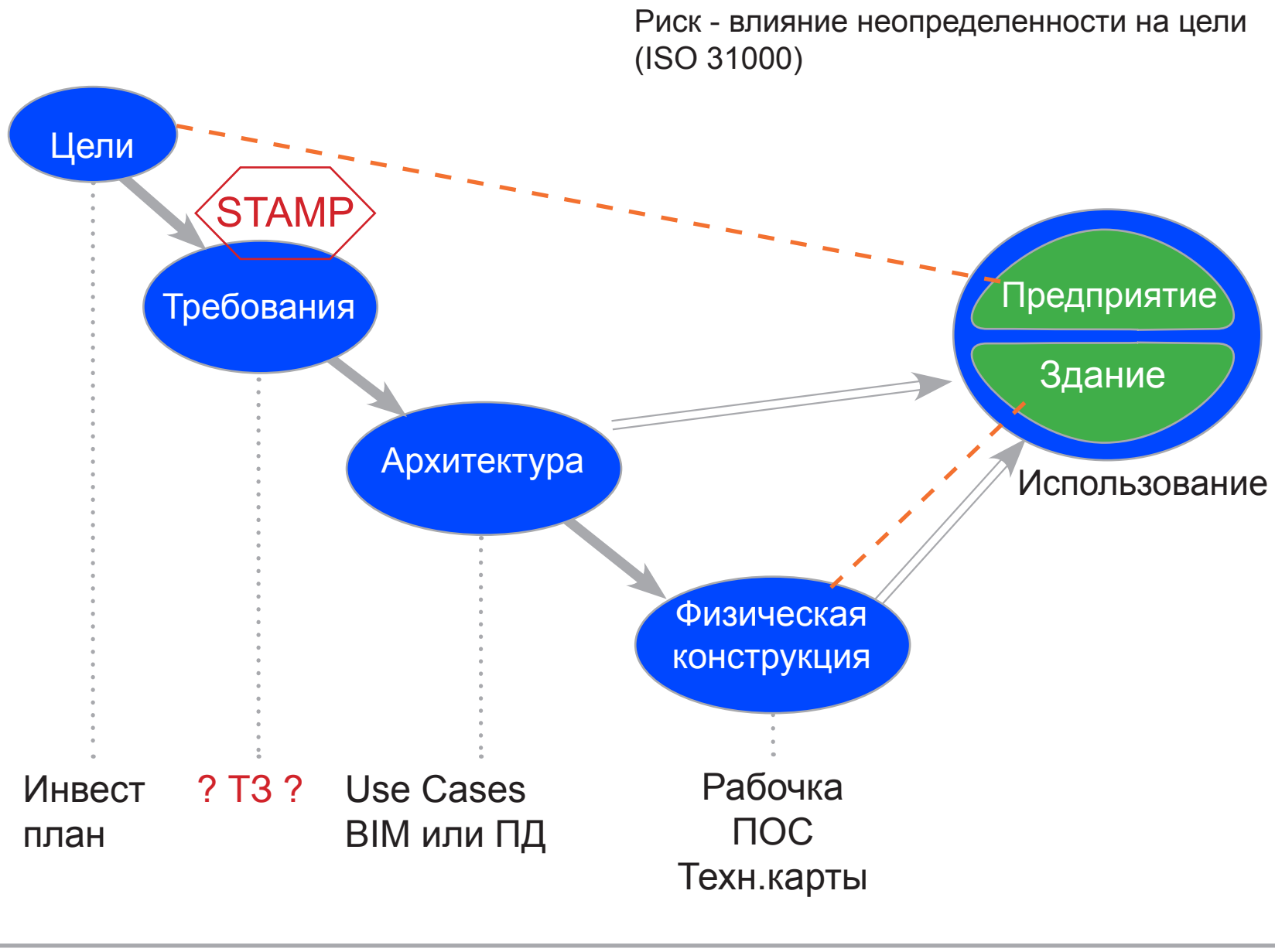
Слайд 7.

На следующем слайде приведена классическая схема процесса проектирования из военного американского стандарта 1993 года.

Читая схему, отметим необходимость тщательного сбора исходных данных, итеративную работу с требованиями и разбиение архитектуры на функциональную часть и физическую конструкцию.

В то же время за пределами проектирования оказывается определение нужд и целей пользователей, определяющие назначение объекта.

Рабочие продукты



Слайд 8-9.
Перейдем к рабочим продуктам.

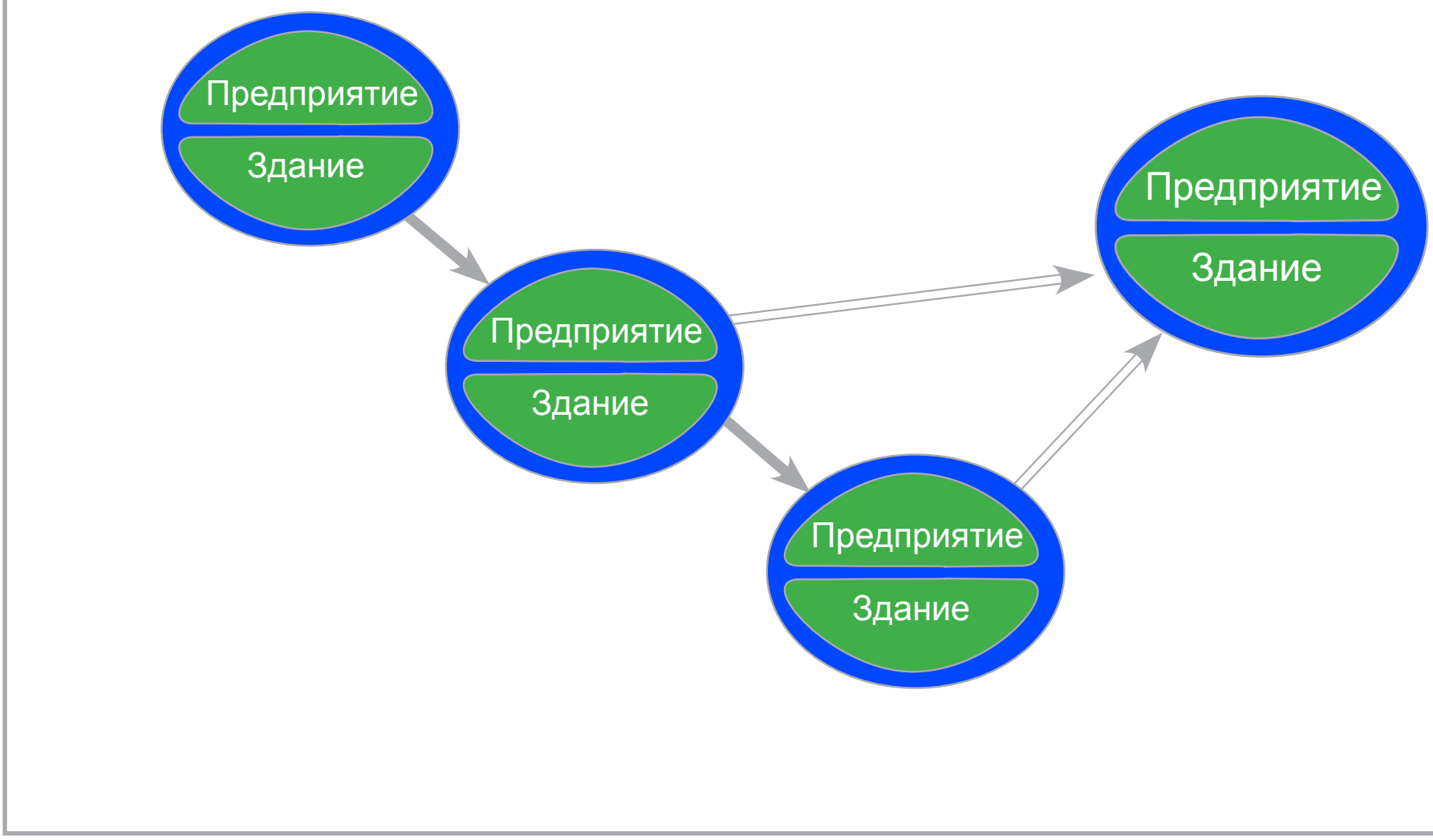
На данном слайде упрощенно изображен жизненный цикл целевой системы в форме Vee-диаграммы. Каждая стадия названа по объекту размышлений (цели, требования, архитектура, конструкция), а вниз вынесены рабочие продукты, описывающие замысленное.

Здесь я в явном виде вынес цели и требования к системе, зная, что согласно стандарту ISO 31000 «риск – это влияние неопределенности на цели» и зная, что метод STAMP (Systems-Theoretic Accident Model and Processes, http://mitpress.mit.edu/books/engineering-safer-world) профессора Левесон работает именно на стадии разработки требований.

И один из вопросов, которые я ставлю перед собой – это насколько существующая практика составления технических заданий обеспечивает достижение целей собственника и других пользователей объекта.

Также нужно понимать двойственность целевой системы. Цели достигаются предприятием, которое использует для этого здание (конструкцию). Потому в целях, требованиях и архитектуре должны учитываться особенности работы этого предприятия. И безопасность нужно обеспечивать предприятия, о котором принято говорить в терминах активов.

Функция и конструкция



Слайд 10.

Ну и нужно учитывать, что все вовлеченные в процесс участники также являются такими «гамбургерами», чья архитектура влияет на конечный успех проекта.

Model-Based Systems Engineering

- Вспомогательный инструмент - **рабочий продукт**

  (BIM в Мосгосэкспертизе, энергетическое моделирование, модели загрязнения атмосферы)
- Модель - абстрактное представление предмета для определенной цели (ISO 24744)
- Язык - понятия и синтаксис
- Domain-Specific Language
- **Какова онтология безопасности предприятий и зданий?**

Слайд 11-12.

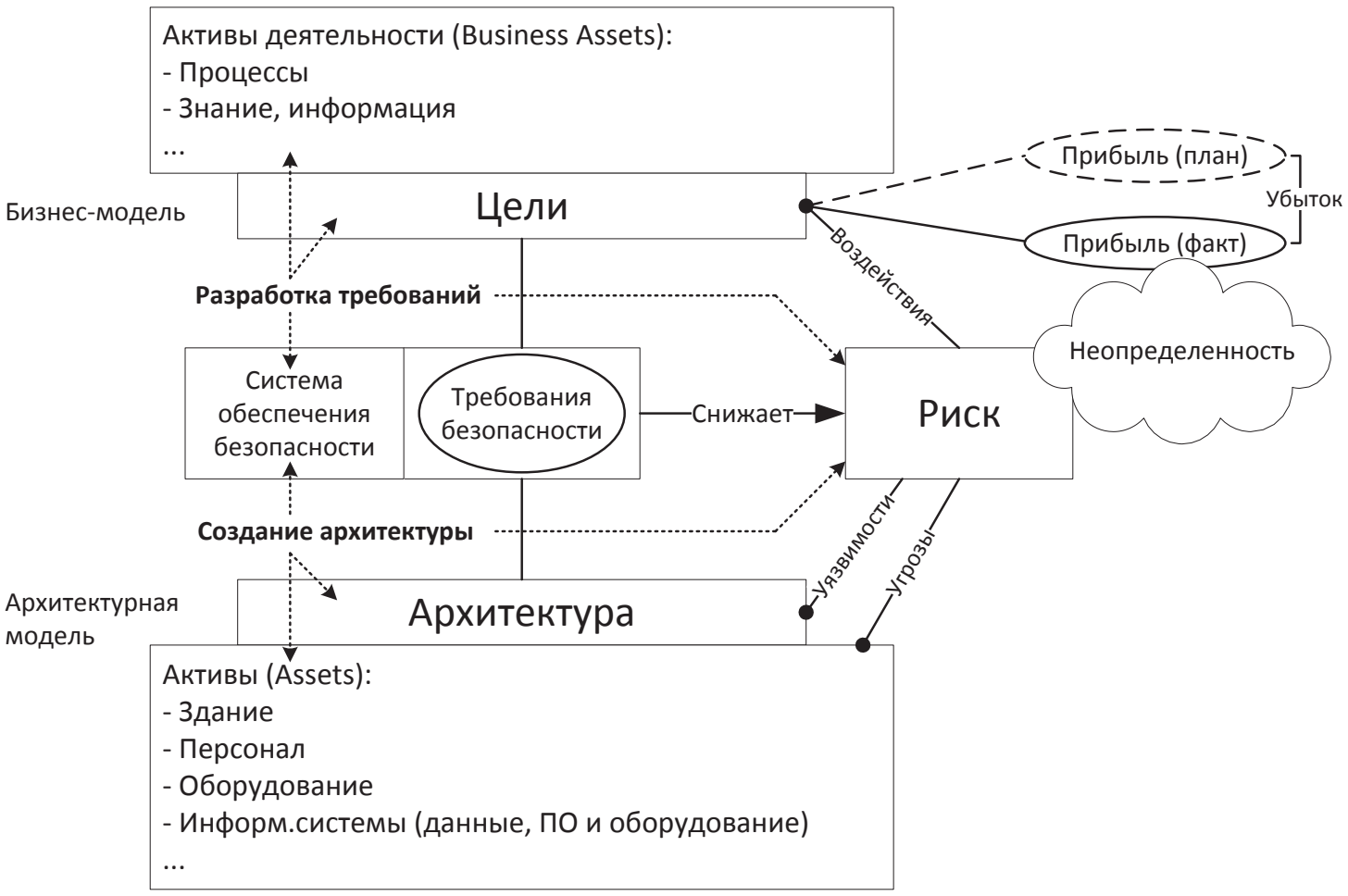
Модели давно используются в проектировании как вспомогательный инструмент: это физические макеты, математические расчеты, Simulink.
Но постепенно модель становится рабочим продуктом, тем, что выпускают, что является результатом работы.

Модель абстрактно представляет предмет для определенной цели пользователя.
И использует для представления определенный язык.

Языков много, их набор понятий и синтаксис зависят от цели моделирования и предметной области. Потому говорят о языках предметных областей.

Чтобы выбрать язык и инструмент моделирования нам нужно было ответить на вопрос, а что есть в нашей предметной области? Какие понятия и отношения? Какова онтология безопасности предприятий и зданий.

Концепт-схема рисковой ситуации



ISO 31000: 2009

Алексей Сидоренко, “Лучший риск-менеджер 2014” по версии РусРиск

Kahneman & Tversky
Dale F. Cooper
Nicolas Mayer

Слайд 13.
Я начал с понятия «риск», связывающего деятельность и опасность.

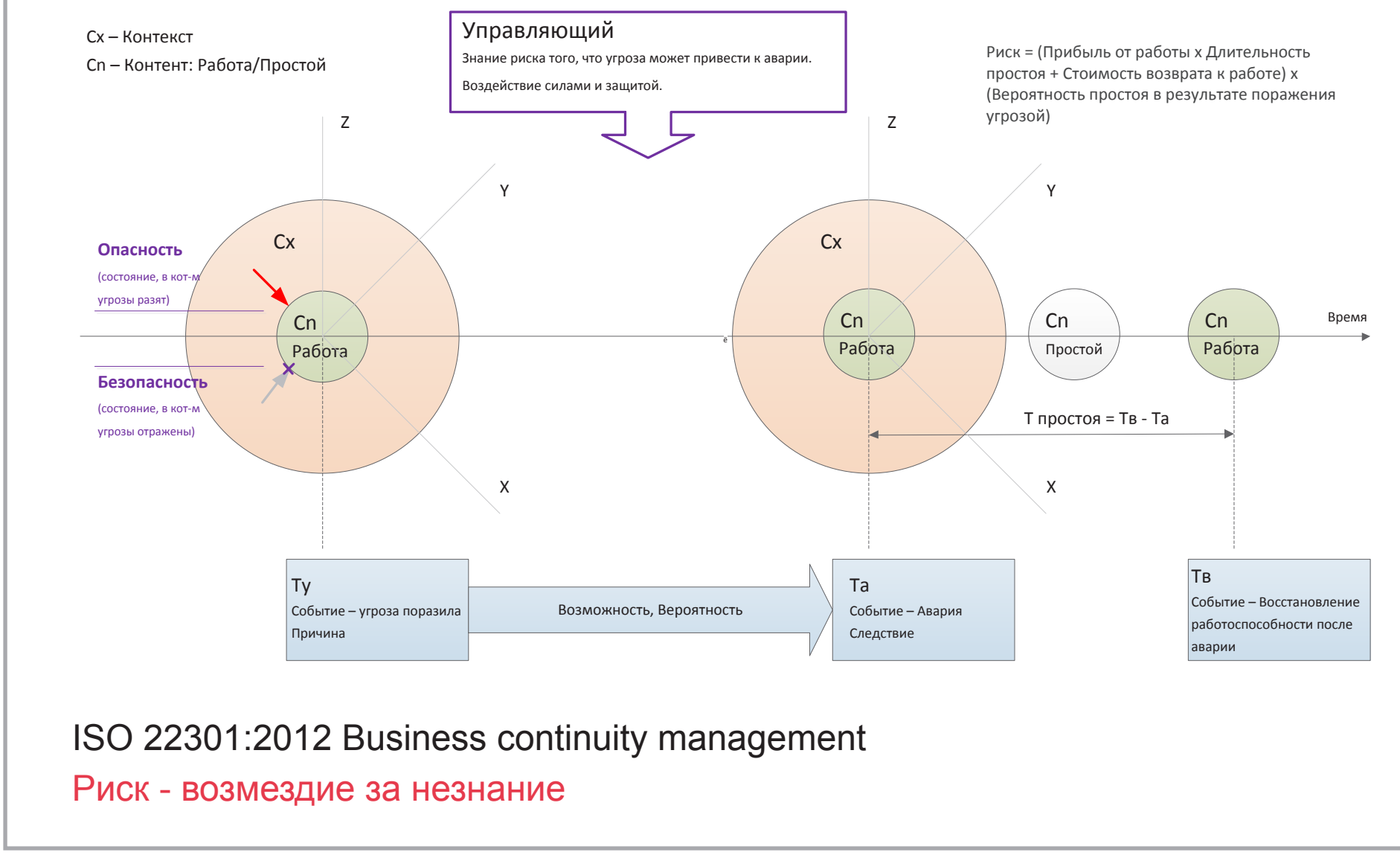
На слайде приведена выработанная концептуальная схема рисковой ситуации.
В своем понимании риска мы опираемся на международный стандарт ИСО 31000, работы Алексея Сидоренко и других авторов.

Схема читается так: Предприниматель в соответствии с бизнес-моделью намерен достигнуть поставленных целей. Риск является мерой воздействия неопределенности на достижение целей. Воздействие оказывается на активы предприятия сквозь уязвимости в архитектуре. Непрерывность деятельности предприятия и получение запланированной прибыли обеспечивается исключением уязвимостей в архитектуре, снижением вероятности поражения угрозой и степени воздействия неопределенности на цели.

Также на схеме можно прочитать следующее:
1. Архитектура призвана для достижения целей.
2. Явно разделены функциональная и конструктивная части системы
3. Схема включает процесс проектирования, так как есть Разработка требований и Создание архитектурной модели.
4. Время задано в бизнес-процессах.
5. Пространство задано размещением активов.

Изучение работ Канемана и Тверски о принятии решений в условиях неопределенности выводит нас к микроэкономике и когнитивной психологии.

Непрерывность деятельности



ISO 22301:2012 Business continuity management

Риск - возмездие за незнание

Слайд 14.

На данной схеме ситуация поражения угрозой развернута во времени, что позволило определить риск через длительность простоя в работе активов, через прерывание бизнеса-процесса.

Аналогичная концепция изложена в стандарте ИСО 22301 об управлении непрерывностью деятельности предприятия.

Для нас целью обработки риска является обеспечение управляющего нужной информацией в нужное время, для того чтобы предупредить и отреагировать на опасное событие. Афористично можно сказать, что риск – это возмездие за незнание, потому важны способности, восприятие и намерения людей.

Онтология безопасности объектов любой природы

Donald Firesmith, Nancy Leveson, Rasmussen, OMG Essense

Более 50 понятий

Пользователи, Активы, Цели и Средства, Требования, Архитектура, Конструкция, Команда, Работы, Уязвимости, Техника обороны, Угроза, Ущерб, Убыток...

На стадии Использование (эксплуатация)

Слайд 15.

Опираясь на работы зарубежных авторов я разработал онтологию безопасности объектов любой природы. В онтологию вошло более 50 понятий, частично приведенных на слайде: Пользователи, Активы, Цели и средства, Требования, Архитектура, Команда и другие…

Наша задача – обеспечить безопасность использования целевой системы, потому онтология разработана только для этой стадии жизненного цикла.

Управляющему нужно знать о...

(1) - изменении Активов в результате Работ Пользователей

Этап ЖЦ / Стейкхолдер	Замысел	Проектирование	Согласование	Строительство	Приемка	Эксплуатация	Ремонт/ Реконструкция	Вывод из эксплуатации
Собственник	Установление верных целей. Сокращение риска.	Установление и соблюдение требований. Соблюдение сметного лимита.	Прохождение процедуры.	Соответствие проекту. Соблюдение бюджета и сроков.	Работоспособность всех систем.	Достижение целей. Высокий доход. Снижение операционных расходов.	Снижение операционных расходов. Сохранение проектных показателей.	Выручка от утилизации.
Застройщик	Увеличение бюджета на работы.	Увеличение бюджета. Привлечение "своих" подрядчиков.	Прохождение процедуры. Сокращение затрат на процедуру.	Увеличение бюджета.	Прохождение процедуры. Сокращение затрат на процедуру.	Снижение расходов на исполнение гарантийных обязательств.		Увеличение бюджета. Привлечение "своих" подрядчиков.
Арендатор						Соблюдение условий договора. Снижение арендной ставки.	Сокращение беспокойства от ремонта/реконструкции.	
Проектировщики		Применение понятных решений.	Прохождение процедуры. Сокращение затрат на					

(2) - деградации Техники безопасности и охраны

(3) - расширении или появлении новых Уязвимостей

(4) - происшествиях, нарушениях защитных барьеров

Слайд 16.
Анализ онтологии позволил ответить на вопрос, какая информация нужна управляющему для обеспечения безопасности. Управляющий должен знать о изменениях состояния системы. Так у нас проявляется время. Мы выделили 4 типа изменений.

Первое и ключевое. Это изменение активов в результате работ пользователей. Работы пользователей (собственника, арендатора, управляющего, регулятора, злоумышленника) направляются их целями. Здесь мы работаем с Людьми.

Цели пользователей мы разложили по всем стадиям жизненного цикла, чтобы понимать, что от них ожидать, и мочь выявить конфликты их целей.
Пример: привязка росреестром налога на имущество к кадастровой стоимости и манипулирование схемой расчета этой стоимости.

Следующее изменение: это деградация Техники безопасности и охраны с течением времени. Речь идет не только о программах и оборудованием, но и о нарушении в цикле управления технологическим процессом (не выполнение инструкций, не обработанные сигналы).

Третий тип изменений: Расширение и появление новых Уязвимостей. Это изменение связано с остальными типами, так как уязвимости используются для поражения угрозами. Нам было важно сохранить этот специфичный фокус на систему, который характерен для информационной безопасности.

И четвертый тип изменений: это знание уже произошедших событий, на которые мы дожны отреагировать.

Принятие решений

- Человек действует в ситуации неудовлетворенности существующим положением дел.
- Направление деятельности определяется доверенным авторитетом и этическими ценностями.
- Человек действует, если готов отдать имеющееся за пользу от результата действия. ср. Return on Attack

Inherent Uncertainty

Hesitancy- колебание в принятии решений (субъектом)

Vagueness - неясность, расплывчатость (объекта)

Доонтологический шаг

- Психология деструктивной деятельности людей

Слайд 17.

Как уже было сказано, ключевым для нас является первый тип изменений, связанный с целями и мотивами действий людей. Нам нужно было ответить на вопрос, как человек принимает решение действовать? Анализ ситуаций из собственной жизни показал, что
• Человек действует в ситуации неудовлетворенности существующим положением дел.
• Направление деятельности определяется доверенным авторитетом и этическими ценностями.
• Человек действует, если готов отдать имеющееся за пользу от результата действия.
Последнее положение нашло отражение в концепции информационной безопасности, в соответствии с которой стоимость хакерской атаки должна превышать пользу от неё.

Мы рассчитываем, что развитие этих положений позволит нам учесть в онтологии безопасности человеческий фактор.

Лингвистический анализ феномена присущей бытию неопределенности показал его двойственность. С одной стороны, неопределенность воплощается в колебании при принятии решений субъектом, с другой – это неясность, расплывчатость объекта действия.

Это диктует нам сделать доонтологический шаг к созданию психологической модели деструктивной деятельности людей (не ожидаемые поступки людей).

Моделирование предприятия

Требования к инструменту моделирования архитектуры предприятия

- Моделирование деятельности людей (социотехническая система)
- Увязать функцию и конструкцию
- Классификация, отношения
- Работа на русском языке
- Выразительные графические средства
- Легкость освоения

ARCHIMATE®

Archi

Слайд 18-19.

О жизненном цикле целевой системы мы уже поговорили выше, теперь перейдем к организации, применяющей метод.

Изучение методов инженерии предприятий позволило предъявить требования к инструменту моделирования их архитектуры

- Мы должны мочь моделировать деятельность людей
- Должны увязать функцию и конструкцию
- Должны задать классификацию понятий и их отношения
- Работать на русском языке
- Инструмент должен обладать выразительными графическими средствами
- И быть легким в освоении

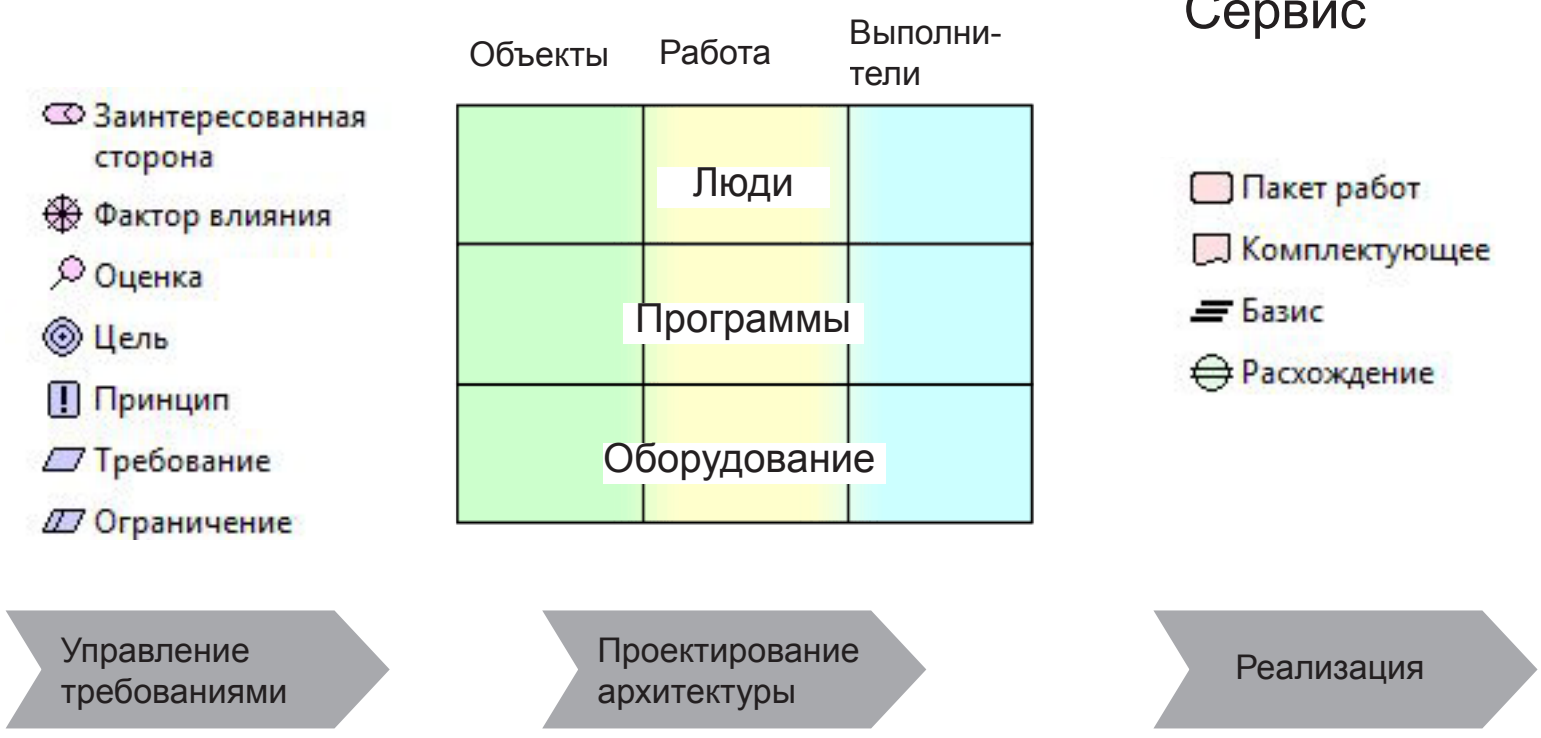
На текущий момент я выбрал язык Archimate с бесплатным русифицированным редактором Archi.

Archimate - Моделирование архитектуры предприятия

The Open Group is a global consortium that enables the achievement of business objectives through IT standards.

THE Open GROUP

Business IT Gap



Слайд 20.

Архимейт - это архитектурный язык, описывающий корпоративную структуру, в удобном для IT-шников виде. Язык развивается консорциумом The Open Group. Последняя версия стандарта датируется 2013 годом.

Архимейт позволяет описать на единой диаграмме бизнес-процессы, организационную структуру и информационные потоки. Но не дает работать с состояниями рабочего продукта. На нем можно описать метод работы, но не объект его приложения.

В ядре языка выделено три уровня: люди, программы и оборудование. Язык факт-ориентированный и факты описываются упорядоченными тройками <субъект, предикат, объект> - Выполнители выполняют работы с объектами.
В версии стандарта 2.0 помимо ядра, описывающего архитектуру предприятия, добавлены расширения для работы с требованиями и для реализации проектов преобразований предприятий, что покрывать все наши потребности.

В стандарте прямо прописано, что проектировать архитектуру предприятия нужно начинать с определения его сервиса, приносящего пользу внешним пользователям. Этим реализуется принцип промышленного дизайна и не явно задается понятие «система», которая определяется не через свои компоненты, а через сервис, функцию, оказываемую вовне.

Программирование пространства

Функция - бизнес-процессы
Конструкция - расположение людей, оборудования

ICS NEO: привязка функции к пространству - графы

Описание вершины графа:
- тип разрешенного использования
- требования к системам жизнеобеспечения

Слайд 21.

Функция выполняется бизнес-процессами, а конструкция задается путем размещения людей, программ и оборудования в пространстве.

В методике проектирования ICS NEO (http://icsgroup.ru/neo/) привязка функции к пространству осуществляется через графы, описание каждой вершины которого посвящено обоим ипостасям.

В языке Archimate привязка к пространству осуществляется при помощи элемента Location, Место, что позволяет нам привязать бизнес-модель к архитектуре пространства. При описании вершины графа задается
- тип разрешенного использования в соответствии с моделью бизнес-процессов, но и
- требования к системам жизнеобеспечения, в том числе и к системам безопасности и защиты

Мы рассчитываем, что Архимейт можно будет использовать для моделирования предприятия в проектируемом здании.

Проектное бюро

- Люди с системным подходом в голове
- Пространство для работы с людьми (переговоры, совещания, brainstorm)

Слайд 22.

Изложенная мною концепция метода предъявляет два требования к проектному бюро, использующему этот метод.

Первое и главное – это наличие людей с системным подходом в голове

Второе – это наличие пространства для работы с людьми, проведения переговоров и совещаний. Это нужно для работы над выявлением целей и требований.

Остальное – кабинеты, компьютеры, софт – понятно и отлично реализовано ICS NEO в других проектах.

Проблематизация

- Изучение инструментов моделирования

  Archimate, IDEF, BPNM, Essence, SysML...

- Модель целевой системы должна описывать переходы между состояниями
- Психологическая модель деятельности людей, целеполагания и принятия решений в условиях неопределенности

  Мыследеятельностный подход, теория принятия решений Канемана, теория практики Бурдьё, австрийская школа экономики, теория фирмы, анатомия человеческой деструктивности Фромма...

- Понимать психологию переговоров, конфликтологию

Слайд 23.

И в заключение обозначу проблематику дальнейшего исследования.

Первое – это необходимость изучения инструментов моделирования, коих множество, и каждый труден в освоении.

При этом модель целевой системы должна описывать переходы между состояниями, чего не позволяет делать Архимейт, чтобы мы могли отмоделировать изменения.

Третье, уже высказанное выше, – нужно разработать психологическую модель деятельности людей, учитывающую механизмы целеполагания и принятия решений. Предварительный набор теорий для изучения в этом направлении приведен на слайде.

И последнее – нам нужно научиться вести переговоры с людьми с упором на разрешение конфликтов их целей.

Спасибо за внимание!