Использование метода структурированного мультиверсного моделирования (МСММ) для решения задач управления безопасностью

Кононов Александр Анатольевич,

к.т.н., с.н.с. Института системного анализа РАН

Цель разработки МСММ

Метод структурированного мультиверсного (мультиверсионного) моделирования предназначен прежде всего для решения задач повышения эффективности автоматизации управления и информационного обеспечения принятия решений.

МСММ является логическим продолжением и развитием подходов заложенных в методах структурного и объектно-ориентированного моделирования.

Проблема, для решения которой предназначен метод МСММ

- Проблема возникла при решении задач принятия решений в управлении безопасностью.
- Проблема заключалась в отсутствии инструментария который бы позволял **с одной стороны** представлять контролируемые структуры (безопасность которых должна обеспечиваться) во всем их многоаспектном многообразии – организационном, функциональном, временном. **С другой стороны** обеспечивал возможность обобщения и получения интегрального образа состояния безопасности контролируемой системы через алгоритмы горизонтального и вертикального агрегирования.

МСММ строился, как метод развивающий методы структурного подхода (МСП) и объектно-ориентированного моделирования (ООМ)

Чтобы понять, то новое, что содержится в МСММ обратимся к основным концепциям МСП и ООМ, то есть рассмотрим:

- Решаемые задачи и проблемы
- Принципы
- Модели
- Средства

Главная проблема решаемая МСП

Проблема сложности является главной проблемой, которую приходится решать при создании больших и сложных систем любой природы. Ни один человек не в состоянии выйти за пределы человеческих возможностей и понять всю систему в целом. Единственный эффективный подход к решению этой проблемы, который выработало человечество за всю свою историю, заключается в построении сложной системы из небольшого количества крупных частей, каждая из которых, в свою очередь, строится из частей меньшего размера и т.д., до тех пор, пока это имеет смысл. Этот подход наиболее известен под названием: **иерархическая декомпозиция**.

Источник: http://www.market-journal.com/metodyjekonomiki/38.html

Основные понятия и принципы МСП

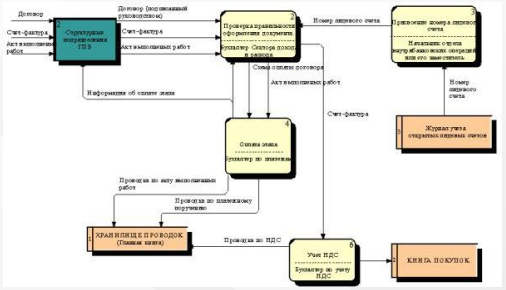
- Принцип иерархического упорядочения – принцип организации составных частей системы в иерархические древовидные структуры с добавлением новых деталей на каждом уровне.
- Принцип структурирования данных – данные должны быть структурированы и иерархически организованы.
- Принцип абстрагирования – выделение существенных аспектов системы и отвлечение от несущественных.
- Принцип непротиворечивости – обоснованность и согласованность элементов системы.
- Количество связей между отдельными подсистемами должно быть минимальным
- Связность отдельных частей внутри каждой подсистемы должна быть максимальной. Структура системы должна быть таковой, чтобы все взаимодействия между ее подсистемами укладывались в ограниченные, стандартные рамки:
- Каждая подсистема должна инкапсулировать свое содержимое (скрывать его от других подсистем);
- Каждая подсистема должна иметь четко определенный интерфейс с другими подсистемами. Инкапсуляция позволяет рассматривать структуру каждой подсистемы независимо от других подсистем. Интерфейсы позволяют строить систему более высокого уровня, рассматривая каждую подсистему как единое целое и игнорируя ее внутреннее устройство.

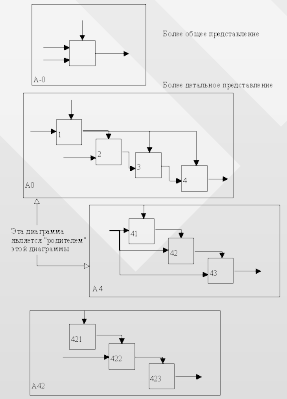
Источник:http://www.market-journal.com/metodyjekonomiki/38.html

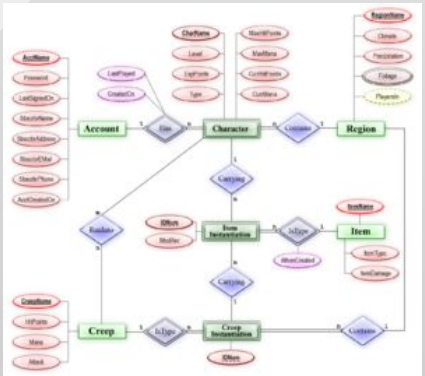
Методы и средства МСП

- В структурном подходе используются в основном две группы средств, описывающих функциональную структуру системы и отношения между данными. Каждой группе средств соответствуют определенные виды моделей (диаграмм), наиболее распространенными среди которых являются:
- DFD (Data Flow Diagrams) – диаграммы потоков данных;
- SADT(Structured Analysis and Design Technique) – метод структурного анализа и проектирования – модели и соответствующие функциональные диаграммы;
- ERD (Entity-Relationship Diargrams) – диаграммы сущность – связь.
- Диаграммы потоков данных и диаграммы сущность–связь – наиболее часто используемые в CASE-средствах виды моделей.
- Конкретный вид перечисленных диаграмм и интерпретация их конструкций зависят от стадии жизненного цикла ПО.
- На стадии формирования требований к ПО SADT-модели и DFD используются для построения модели AS-IS и модели TO-BE, отражая, таким образом, существующую и предлагаемую структуру бизнес-процессов организации и взаимодействие между ними (использование SADT-моделей, как правило, ограничивается только данной стадией, поскольку они изначально не предназначались для проектирования ПО). С помощью ERD выполняется описание используемых в организации данных на концептуальном уровне, не зависимом от средств реализации базы данных (СУБД).
- На стадии проектирования DFD используются для описания структуры проектируемой системы ПО, при этом они могут уточняться, расширяться и дополняться новыми конструкциями. Аналогично ERD уточняются и дополняются новыми конструкциями, описывающими представление данных на логическом уровне, пригодном для последующей генерации схемы базы данных. Данные модели могут дополняться диаграммами, отражающими системную архитектуру ПО, структурные схемы программ, иерархию экранных форм и меню и др.

Источник:http://www.market-journal.com/metodyjekonomiki/38.html







IDEF методологии для решения задач моделирования сложных систем

- В настоящий момент к семейству IDEF методологии семейства ICAMВ настоящий момент к семейству IDEF методологии семейства ICAM (Integrated Computer-Aided Manufacturing) DEFenition для решения задач моделирования сложных систем можно отнести следующие стандарты:
- IDEF0IDEF0 — Function Modeling — методология функционального моделирования. С помощью наглядного графического языка IDEF0 изучаемая система предстает перед разработчиками и аналитиками в виде набора взаимосвязанных функций (функциональных блоков — в терминах IDEF0). Как правило, моделирование средствами IDEF0 является первым этапом изучения любой системы. Методологию IDEF0 можно считать следующим этапом развития хорошо известного графического языка описания функциональных систем SADT (Structured Analysis and Design Technique);
- IDEF1 — Information Modeling — методология моделирования информационных потоков внутри системы, позволяющая отображать и анализировать их структуру и взаимосвязи;
- IDEF1XIDEF1X (IDEF1 Extended) — Data Modeling — методология построения реляционных структур (баз данных), относится к типу методологий «Сущность-взаимосвязь» (ER — Entity-Relationship) и, как правило, используется для моделирования реляционных баз данных, имеющих отношение к рассматриваемой системе;
- IDEF2 — Simulation Model Design — методология динамического моделирования развития систем. В связи с весьма серьезными сложностями анализа динамических систем от этого стандарта практически отказались, и его развитие приостановилось на самом начальном этапе. В настоящее время присутствуют алгоритмы и их компьютерные реализации, позволяющие превращать набор статических диаграмм IDEF0 в динамические модели, построенные на базе «раскрашенных сетей Петри» (CPN — Color Petri Nets);
- IDEF3 — Process Description Capture — Документирование технологических процессов, IDEF3 — методология документирования процессов, происходящих в системе (например, на предприятии), описываются сценарий и последовательность операций для каждого процесса. IDEF3 имеет прямую взаимосвязь с методологией IDEF0 — каждая функция (функциональный блок) может быть представлена в виде отдельного процесса средствами IDEF3;
- IDEF4 — Object-Oriented Design — методология построения объектно-ориентированных систем, позволяют отображать структуру объектов и заложенные принципы их взаимодействия, тем самым позволяя анализировать и оптимизировать сложные объектно-ориентированные системы;
- IDEF5IDEF5 — Ontology Description Capture — Стандарт онтологического исследования сложных систем. С помощью методологии IDEF5онтология системы может быть описана при помощи определенного словаря терминов и правил, на основании которых могут быть сформированы достоверные утверждения о состоянии рассматриваемой системы в некоторый момент времени. На основе этих утверждений формируются выводы о дальнейшем развитии системы и производится её оптимизация;
- IDEF6 — Design Rationale Capture — Обоснование проектных действий. Назначение IDEF6 состоит в облегчении получения «знаний о способе» моделирования, их представления и использования при разработке систем управления предприятиями. Под «знаниями о способе» понимаются причины, обстоятельства, скрытые мотивы, которые обуславливают выбранные методы моделирования. Проще говоря, «знания о способе» интерпретируются как ответ на вопрос: «почему модель получилась такой, какой получилась?» Большинство методов моделирования фокусируются на собственно получаемых моделях, а не на процессе их создания. Метод IDEF6 акцентирует внимание именно на процессе создания модели;
- IDEF7 — Information System Auditing — Аудит информационных систем. Этот метод определён как востребованный, однако так и не был полностью разработан;
- IDEF8 — User Interface Modeling — Метод разработки интерфейсов взаимодействия оператора и системы (пользовательских интерфейсов). Современные среды разработки пользовательских интерфейсов в большей степени создают внешний вид интерфейса. IDFE8 фокусирует внимание разработчиков интерфейса на программировании желаемого взаимного поведения интерфейса и пользователя на трех уровнях: выполняемой операции (что это за операция); сценарии взаимодействия, определяемом специфической ролью пользователя (по какому сценарию она должна выполняться тем или иным пользователем); и, наконец, на деталях интерфейса (какие элементы управления, предлагает интерфейс для выполнения операции);
- IDEF9 — Scenario-Driven IS Design (Business Constraint Discovery method) — Метод исследования бизнес ограничений был разработан для облегчения обнаружения и анализа ограничений в условиях которых действует предприятие. Обычно, при построении моделей описанию ограничений, оказывающих влияние на протекание процессов на предприятии уделяется недостаточное внимание. Знания об основных ограничениях и характере их влияния, закладываемые в модели, в лучшем случае остаются неполными, несогласованными, распределенными нерационально, но часто их вовсе нет. Это не обязательно приводит к тому, что построенные модели нежизнеспособны, просто их реализация столкнется с непредвиденными трудностями, в результате чего их потенциал будет не реализован. Тем не менее в случаях, когда речь идет именно о совершенствовании структур или адаптации к предсказываемым изменениям, знания о существующих ограничениях имеют критическое значение;
- IDEF10 — Implementation Architecture Modeling — Моделирование архитектуры выполнения. Этот метод определён как востребованный, однако так и не был полностью разработан;
- IDEF11 — Information Artifact Modeling. Этот метод определён как востребованный, однако так и не был полностью разработан;
- IDEF12 — Organization Modeling — Организационное моделирование. Этот метод определён как востребованный, однако так и не был полностью разработан;
- IDEF13 — Three Schema Mapping Design — Трёхсхемное проектирование преобразования данных. Этот метод определён как востребованный, однако так и не был полностью разработан;
- IDEF14 — Network Design — Метод проектирования компьютерных сетей, основанный на анализе требований, специфических сетевых компонентов, существующих конфигураций сетей. Также он обеспечивает поддержку решений, связанных с рациональным управлением материальными ресурсами, что позволяет достичь существенной экономии.

Источник: http://ru.wikipedia.org/wiki/DFD

Основные понятия и принципы ООМ

- Основные понятия объектно-ориентированного подхода – объект и класс. Объект определяется как осязаемая реальность – предмет или явление, имеющие четко определяемое поведение. Объект обладает состоянием, поведением и индивидуальностью; структура и поведение схожих объектов определяют общий для них класс. Термины экземпляр класса и объект являются эквивалентными. Состояние объекта характеризуется перечнем всех возможных (статических) свойств данного объекта и текущими значениями (динамическими) каждого из этих свойств. Поведение характеризует воздействие объекта на другие объекты и, наоборот, относительно изменения состояния этих объектов и передачи сообщений. Иначе говоря, поведение объекта полностью определяется его действиями. Индивидуальность – это свойства объекта, отличающие его от всех других объектов.
- Концептуальной основой объектно-ориентированного подхода является объектная модель. Основными ее элементами являются:
- абстрагирование;
- инкапсуляция;
- модульность;
- иерархия;
- полиморфизм;
- наследование.
- Кроме основных, имеются еще три дополнительных элемента, не являющихся в отличие от основных строго обязательными:
- типизация;
- параллелизм;
- устойчивость.
- Класс – это множество объектов, связанных общностью структуры и поведения. Любой объект является экземпляром класса. Определение классов и объектов – одна из самых сложных задач объектно-ориентированного проектирования.
- Абстрагирование – это выделение существенных характеристик некоторого объекта, которые отличают его от всех других видов объектов и, таким образом, четко определяют его концептуальные границы относительно дальнейшего рассмотрения и анализа. Абстрагирование концентрирует внимание на внешних особенностях объекта и позволяет отделить самые существенные особенности его поведения от деталей их реализации. Выбор правильного набора абстракций для заданной предметной области представляет собой главную задачу объектно-ориентированного проектирования.
- Инкапсуляция – это процесс отделения друг от друга отдельных элементов объекта, определяющих его устройство и поведение. Инкапсуляция служит для того, чтобы изолировать интерфейс объекта, отражающий его внешнее поведение, от внутренней реализации объекта. Объектный подход предполагает, что собственные ресурсы, которыми могут манипулировать только методы самого класса, скрыты от внешней среды. Абстрагирование и инкапсуляция являются взаимодополняющими операциями: абстрагирование фокусирует внимание на внешних особенностях объекта, а инкапсуляция (или, иначе, ограничение доступа) не позволяет объектам пользователям различать внутреннее устройство объекта.
- Модульность – это свойство системы, связанное с возможностью ее декомпозиции на ряд внутренне связных, но слабо связанных между собой модулей. Инкапсуляция и модульность создают барьеры между абстракциями.
- Иерархия – это ранжированная или упорядоченная система абстракций, расположение их по уровням. Основными видами иерархических структур применительно к сложным системам являются структура классов (иерархия по номенклатуре) и структура объектов (иерархия по составу). Примерами иерархии классов являются простое и множественное наследование (один класс использует структурную или функциональную часть соответственно одного или нескольких других классов), а иерархии объектов – агрегация.
- Следующую группу важных понятий объектного подхода составляют наследование и полиморфизм. Понятие полиморфизма может быть интерпретировано как способность класса принадлежать более чем одному типу. Наследование означает построение новых классов на основе существующих с возможностью добавления или переопределения данных и методов.
- Типизация – это ограничение, накладываемое на класс объектов и препятствующее взаимозаменяемости различных классов (или сильно сужающее ее возможность). Типизация позволяет защититься от использования объектов одного класса вместо другого или по крайней мере управлять таким использованием.
- Параллелизм – свойство объектов находиться в активном или пассивном состоянии и различать активные и пассивные объекты между собой.
- Устойчивость – свойство объекта существовать во времени (вне зависимости от процесса, породившего данный объект) и/или в пространстве (при перемещении объекта из адресного пространства, в котором он был создан).

Источник http://www.market-journal.com/metodyjekonomiki/39.html

Как мы пришли к необходимости разработки МСММ

Задача. Создать инструментарий, который бы позволил при делегировании полномочий и ответственности не терять контроль за состоянием системы. Победить систему «святой лжи».

Путь к решению. Представление контролируемых объектов (структур) во всем их многоаспектном многоуровневом многообразии – организационном, функциональном, временном и возможности обобщения и получения интегрального образа состояния и оценок безопасности контролируемой системы через алгоритмы горизонтального и вертикального агрегирования (свертки).

Как появилось название - MCMM

Напрашивающаяся аналогия с концепцией мультиверса

Зачем альтернативное название : Метод структурированного (1)мультиверсного/ (2) мультиверсионного моделирования

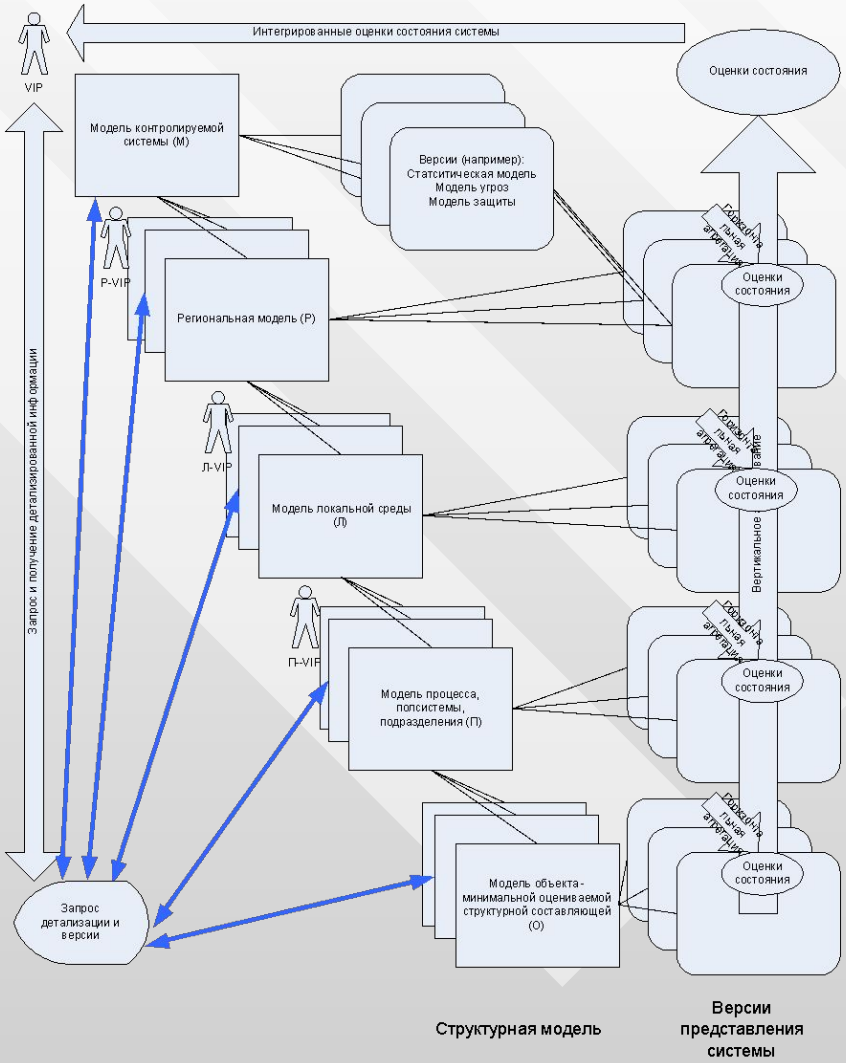
Основные принципы МСММ

- Представление объекта исследования (анализа) во всем его многоаспектном многообразии.
- Возможность переходов от одной версии представления объекта к другой на любом иерархическом уровне.
- Возможность поддержки разных иерархических и методико-математических представлений на каждом иерархическом уровне.
- Поддержка связей между разными иерархическими представлениями.
- Обеспечение вертикального (по иерархическим уровням) и горизонтального (по характеристикам различных аспектов) агрегирования показателей.

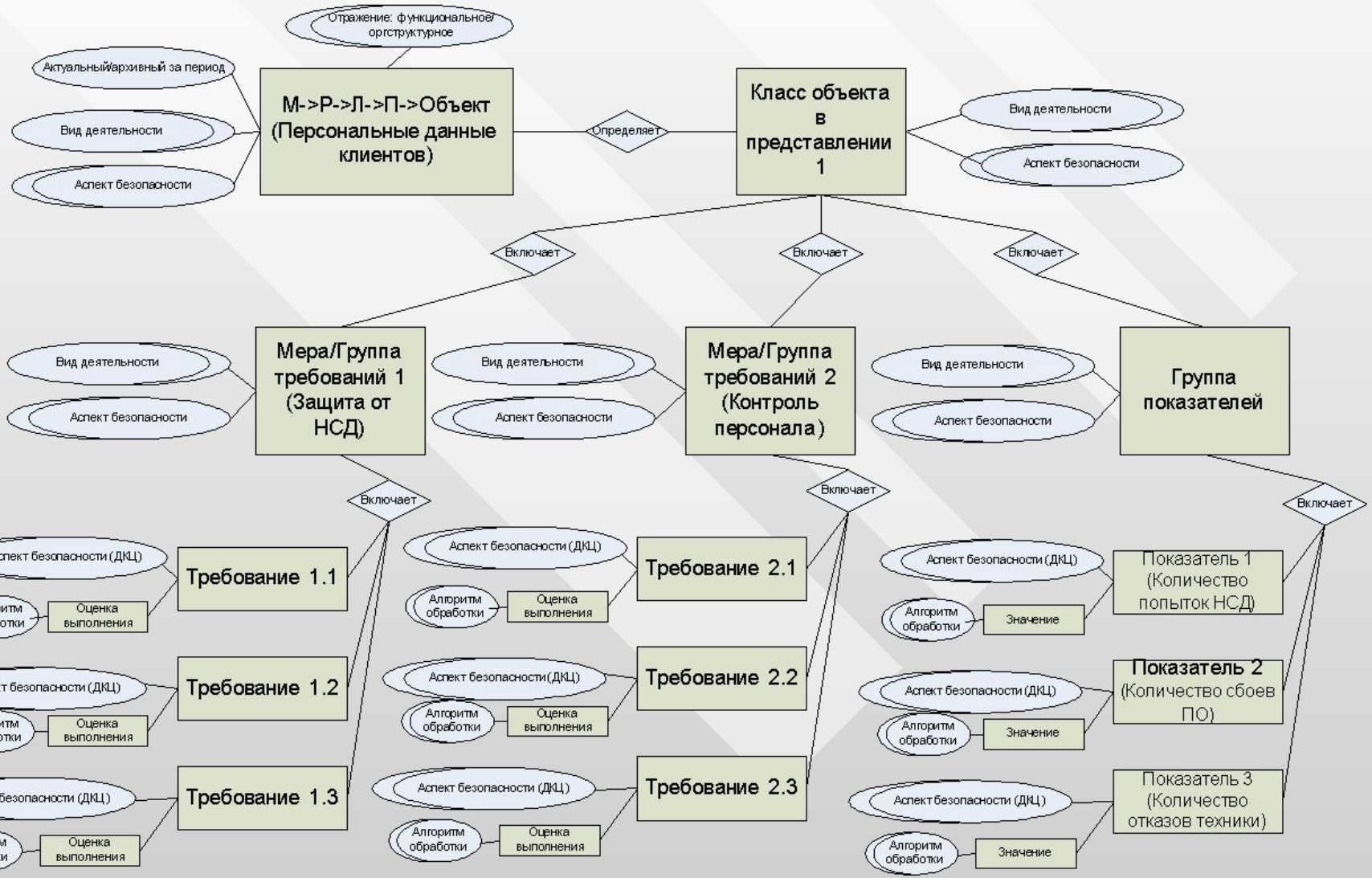
Решение

- Определение множества версий представлений системы.
- Координатная мультиатрибутивность всех объектов, структурных составляющих, их представлений и показателей, определяющая их отнесенность к конкретной иерархической составляющей конкретной версии, к конкретному ее отражению и представлению.
- Определение правил агрегирования.
- Принцип единого остова.

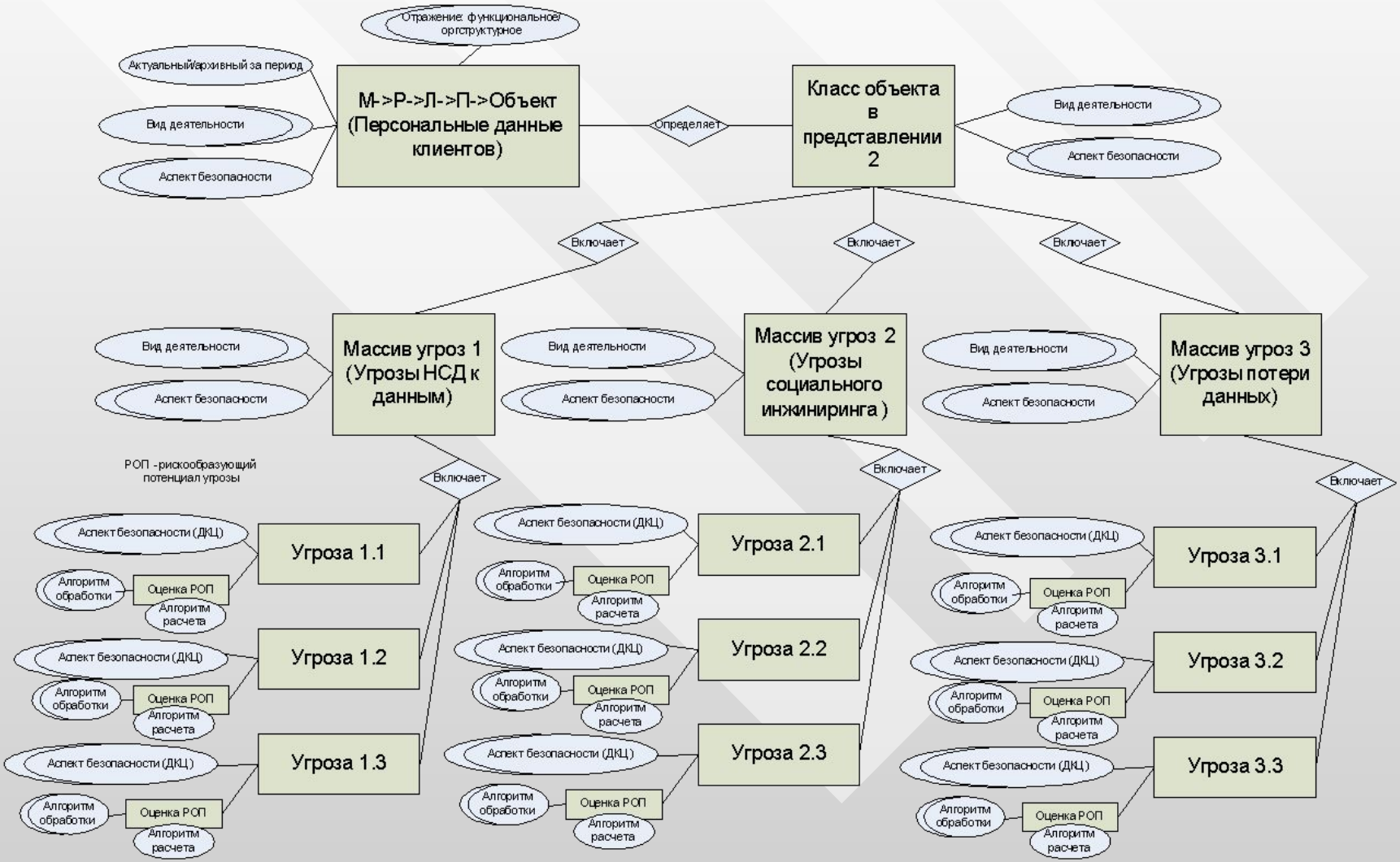
Структурированная мультиверсионная модель



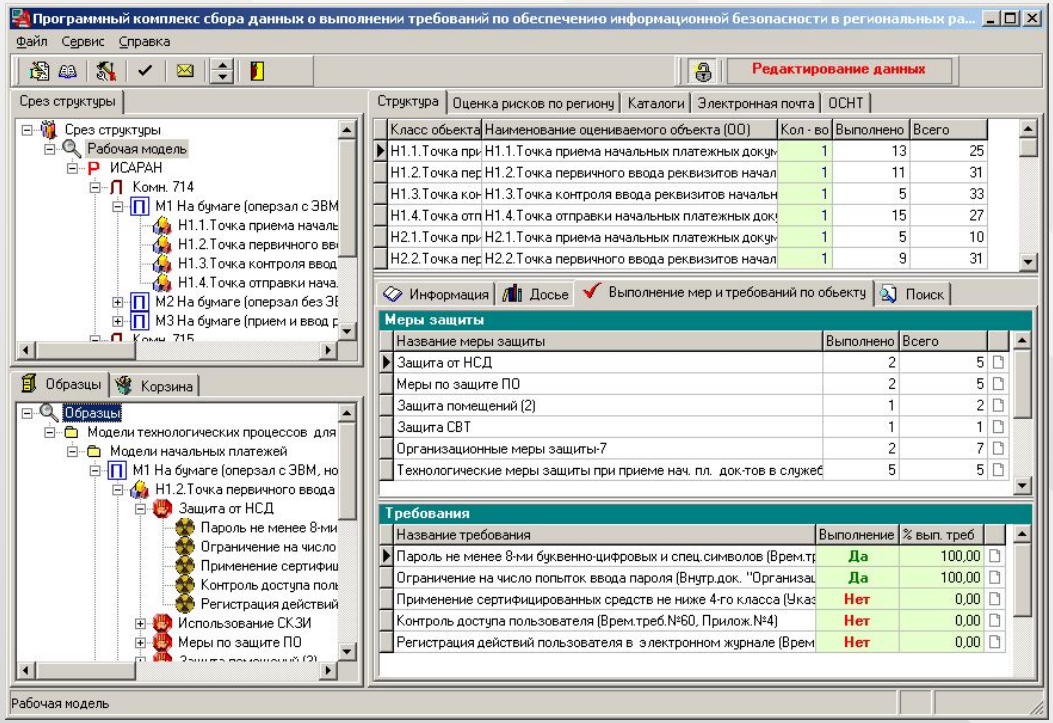
Пример мультиверсионной модели класса объектов в представлении 1 (мер и требований)



Пример мультиверсионной модели класса объектов в представлении 2 (угроз)



Пример работы с 1-ым представлением классов объектов в автоматизированной системе управления безопасностью



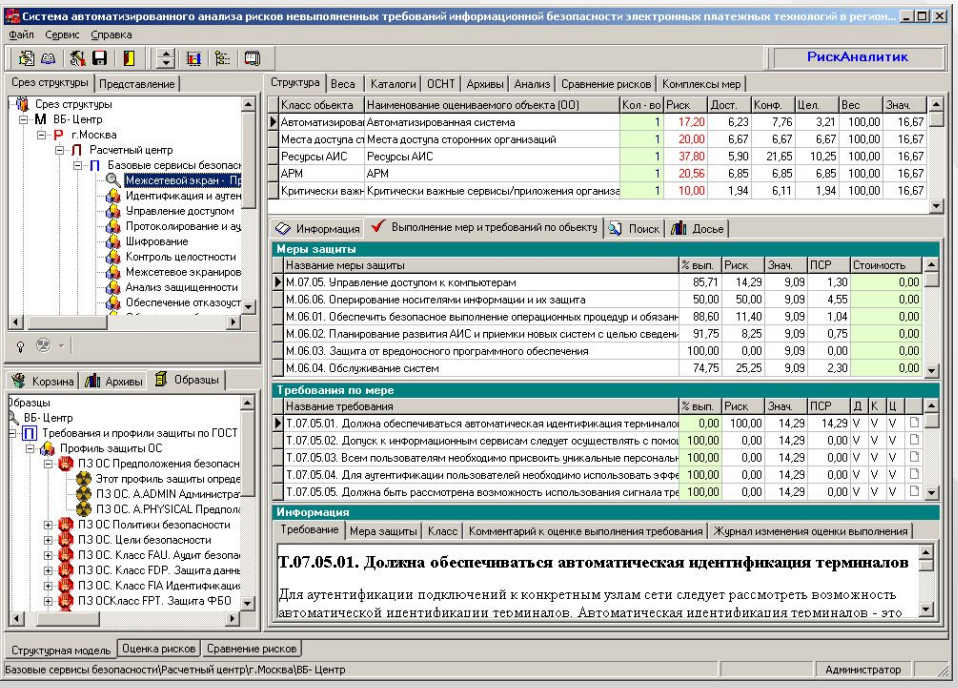
ОУБ-Центр Форма РИСК-ОЗП

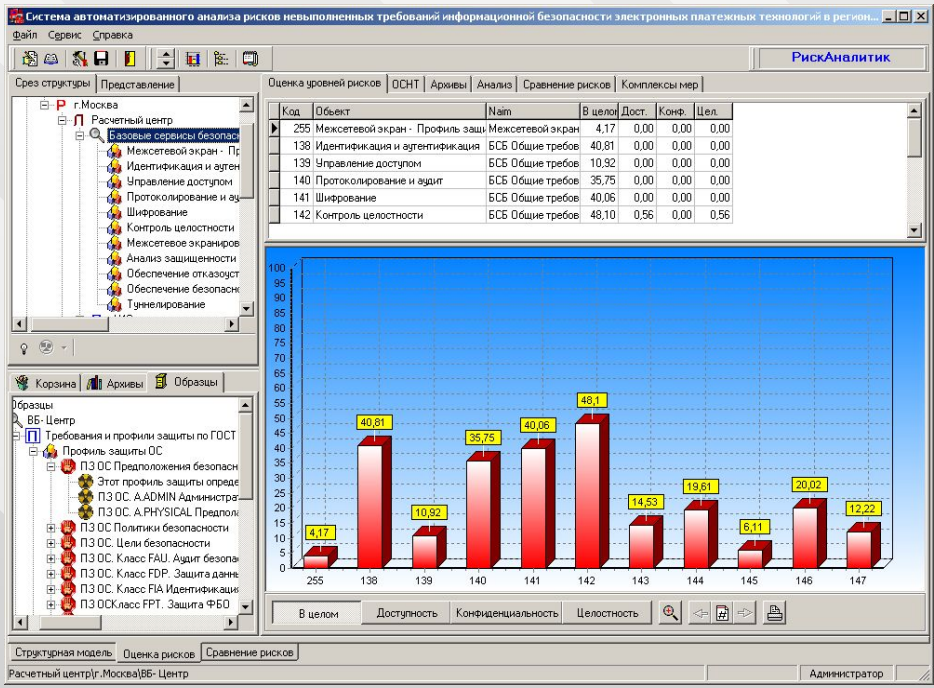
Выполнение требований безопасности

	Выполнение	% вып.	ПСР
ВБ- Центр			
г.Москва			
Расчетный центр			
АИС			
Автоматизированная система			
Мера защиты: М.07.05. Управление доступом к компьютерам	Нет	85,71	1,30
Требования по защите:			
Т.07.05.01. Должна обеспечиваться автоматическая идентификация терминалов	Нет	0,00	
Т.07.05.02. Допуск к информационным сервисам следует осуществлять с помощью надежной процедуры входа в системы	Да	100,00	
Т.07.05.03. Всем пользователям необходимо присвоить уникальные персональные идентификаторы	Да	100,00	
Т.07.05.04. Для аутентификации пользователей необходимо использовать эффективную систему управления паролями	Да	100,00	
Т.07.05.05. Должна быть рассмотрена возможность использования сигнала тревоги, предупреждающего о принуждении	Да	100,00	
Т.07.05.06. Должно устанавливаться время простоя терминалов, после которого сеансы связи должны закрываться	Да	100,00	
Т.07.05.07. Должно обеспечиваться ограничение времени подключения	Да	100,00	
Мера защиты: М.06.06. Оперирование носителями информации и их защита	Нет	50,00	4,55
Требования по защите:			
Т.06.06.01. Должна обеспечиваться безопасность информации на съемных компьютерных носителях	Да	100,00	
Т.06.06.02. Должна быть обеспечена защита конфиденциальности данных во всех операциях с ними	Нет	0,00	
Т.06.06.03. Должна быть обеспечена защита системной документации, содержащей конфиденциальную информацию	Да	100,00	
Т.06.06.04. Должны быть внедрены надежные и проверенные процедуры уничтожения списанных носителей информации	Нет	0,00	
Мера защиты: М.06.01. Обеспечить безопасное выполнение операционных процедур и обязанностей	Нет	88,60	1,04
Требования по защите:			
Т.06.01.01. Должны существовать документированные процедуры обеспечения корректной и надежной работы АИС	Да	100,00	
Т.06.01.02. Необходимо определить управленческие обязанности и процедуры реагирования на события угрожающие ИБ	Нет	65,00	
Т.06.01.03. Должно быть обеспечено разделение обязанностей, снижающее риски НСД и небрежного использования АИС	Да	100,00	
Т.06.01.04. Должно быть обеспечено разделение программных средств разработки и рабочих программ	Нет	78,00	
Т.06.01.05. Необходимо исключить риск нарушения режима безопасности в случае привлечения подрядчика со стороны	Да	100,00	
Мера защиты: М.06.02. Планирование развития АИС и приемки новых систем с целью сведения рисков отказов к минимуму	Нет	91,75	0,75

Пример работы с 1-ым представлением классов объектов в автоматизированной системе управления безопасностью

Оценка рисков доверия по структурным составляющим





Оценки рисков - индексы

- Классическое определение индексов принадлежит Ф. Эджворту:
- «Я предлагаю определить индексное число как число, приспособленное для того, чтобы своими вариациями указывать увеличение или уменьшение величины, не допускающей точного измерения».
- Edgeworth F.Y. The plurality of index numbers. Economic Journal, 1925, v. 35, p. 379)

Аксиоматика оценки рисков доверия к безопасности компьютеризированных систем (1)

При использовании любой ИВС пользователь доверяя этой системе полагается на ее безопасность.

Пусть значение показателя риска доверия пользователя ИВС определяется по 100-балльной (процентной) шкале. Например 100-процентный риск будет означать, что пользователь доверяя ИВС за год теряет 100 процентов своей собственности зависящей от ИВС.

Предположим, что для обеспечения безопасности ИВС должно быть выполнено одно требование. Пусть возможно только два состояния – «выполнено» и «не выполнено» и оценка выполнения требования означает одно из двух - система функционирует «правильно» или «неправильно».

Тогда если требование выполнено, то риск пользователя будет нулевым. Если не выполнено – то риск будет 100-процентным и пользователь все потеряет.

Аксиоматика оценки рисков доверия к безопасности компьютеризированных систем (2)

Предположим, что возможна некоторая интегральная оценка выполнения требования безопасности определяемая по шкале от 0 до 100 процентов.

Предположим также, что от степени (процента) выполнения требования зависит, какая часть собственности пользователя будет сохранена от потери в течение года.

Процент выполнения требования обозначим через q.

Риск доверия (r) пользователя в этом случае определяем по формуле:

$$r = 100 - q \qquad (1)$$

Аксиоматика оценки рисков доверия к безопасности компьютеризированных систем (3)

Положим, что количество требований безопасности системы более чем одно. Обозначим количество таких требований через I. Тогда, если предположить,что значимость выполнения каждого требования одинакова, а степень q_i, выполнения каждого требования можно оценить в диапазоне от 0 до 100 процентов, то риск доверия к безопасности такой системы будет оцениваться как среднее арифметическое значение степени невыполнения указанных требований:

$$r = \frac{\sum_{i=1}^{I} (100 - q_i)}{100 * I} \qquad (2)$$

Аксиоматика оценки рисков доверия к безопасности компьютеризированных систем (4)

Далее предположим, что с каждым требованием связан такой интегральный показатель как вес требования (учитывающий как относительную вероятность нанесения ущерба из-за невыполнения требования, так и относительную величину ущерба), который может быть определен по шкале от 0 до 100.

Таким образом, задавая вес w_i можно определить, в какой степени при оценке риска доверия к безопасности должно учитываться выполнение этого требования. Тогда формула расчета риска доверия принимает следующий вид:

$$r = \sum_{i=1}^{I} \frac{w_i}{\sum_{i=1}^{I} w_i} \times (100 - q_i) \qquad (3)$$

Аксиоматика оценки рисков доверия к безопасности компьютеризированных систем (5)

Будем называть значимостью требования величину z_i рассчитываемую по формуле:

$$z_i = \frac{w_i}{\sum_{i=1}^{I} w_i} \qquad (4)$$

Тогда формулу (3) расчета риска доверия можно переписать в виде:

$$r = \sum_{i=1}^{I} z_i \times (100 - q_i) \qquad (5)$$

Аксиоматика оценки рисков доверия к безопасности компьютеризированных систем (6)

Предположим теперь, что риск доверия к безопасности системы зависит не от одного объекта, а от J объектов для каждого из которых риск доверия был рассчитан по формуле (5). Тогда, если значимость объектов одинакова, то риск доверия к безопасности системы R рассчитывается по формуле:

$$R = \frac{\sum_{j=1}^{J} r_j}{J} \qquad (6)$$

Аксиоматика оценки рисков доверия к безопасности компьютеризированных систем (7)

Если по объектам были определены значимости задающие степень влияния оценок рисков по составляющим на степень риска по системе в целом, то формула (6) должна принять следующий вид:

$$R = \sum_{j=1}^{J} r_j \times z_j \qquad (7)$$

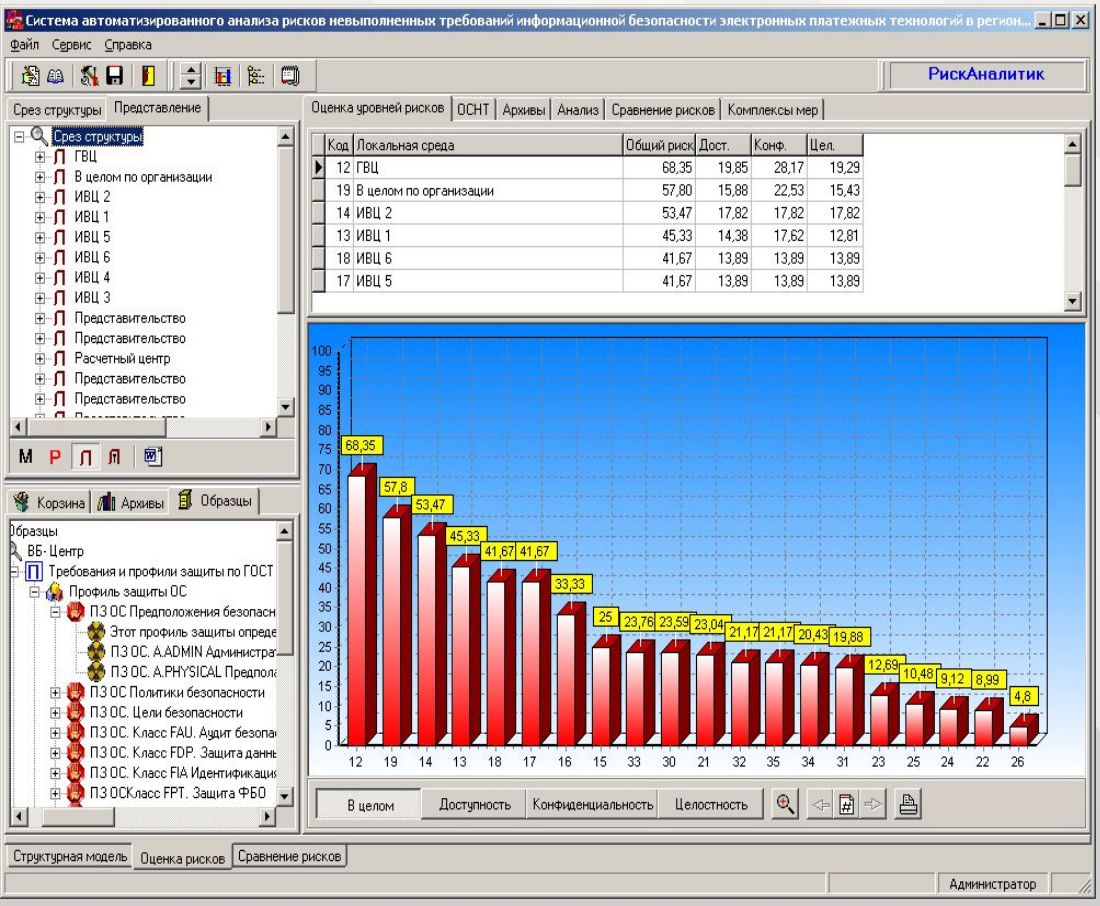
Аксиоматика оценки рисков доверия к безопасности компьютеризированных систем (8)

Приведенную логику рассуждений можно обобщить на случай многоуровневой иерархической системы. Тогда пользуясь формулой $R = \sum_{j=1}^{J} r_j \times z_j$ можно рассчитать оценку риска доверия к каждому следующего иерархического уровню, исходя из знания оценок рисков доверия к безопасности всех его структурных составляющих.

Таким образом, определив требования безопасности ко всем объектам, составляющим систему, оценив их выполнение, а так же определив значимости влияния оценок выполнения отдельных требований и оценок рисков по отдельным структурным составляющим, можно оценивать уровни доверия к безопасности системы любой иерархической сложности.

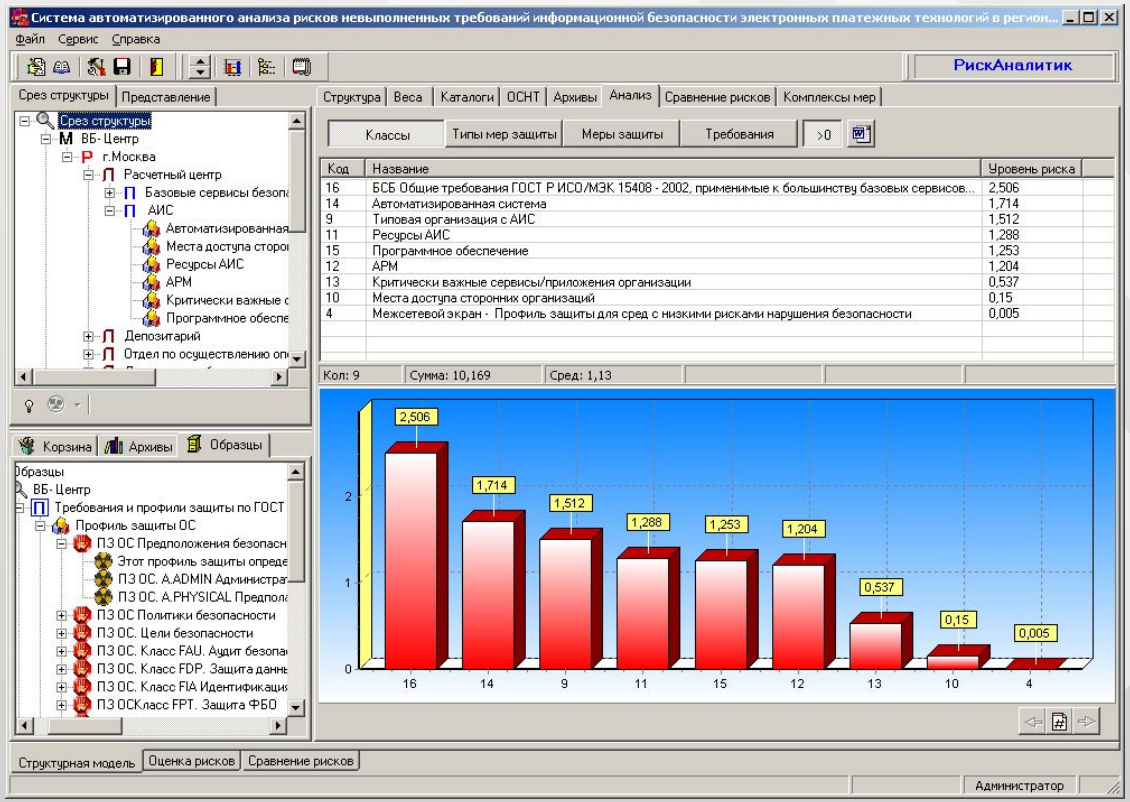
Пример работы с 1-ым представлением классов объектов в автоматизированной системе управления безопасностью

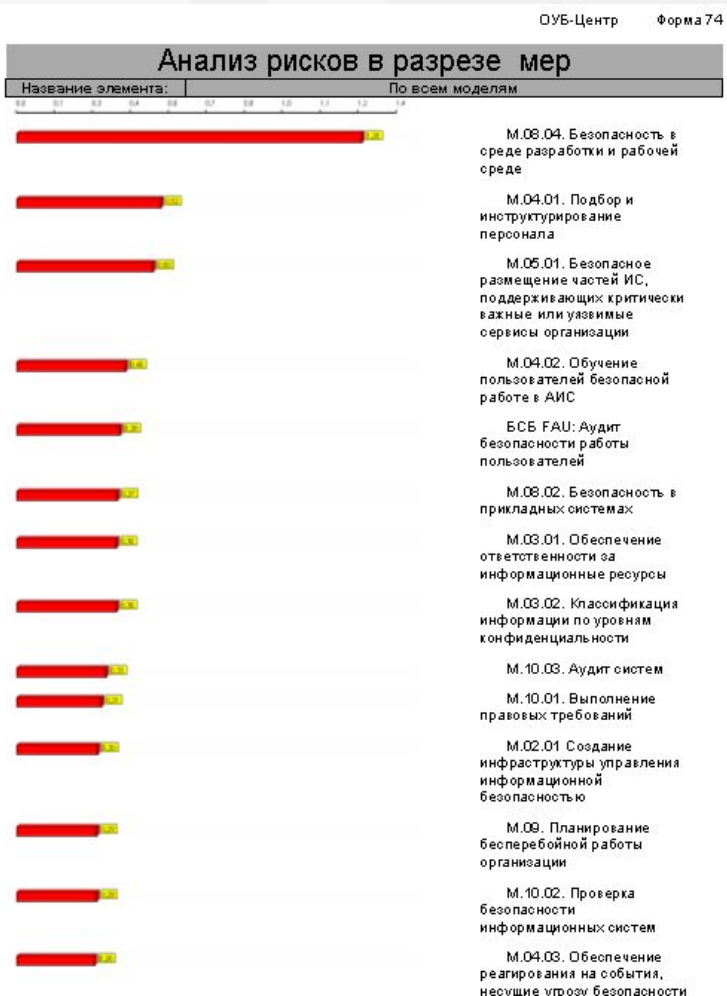
Выявление «узких» мест в обеспечении доверия к безопасности



Пример работы с 1-ым представлением классов объектов в автоматизированной системе управления безопасностью

Выявление источников рисков доверия.





Алгоритмы расчетов при работе со 2-ым представлением классов объектов в автоматизированной системе управления безопасностью. Построение модели угроз

Все множество угроз $\mathbf{Y}^{\mathbf{S}}$, связанных с системой $\mathbf{S}$ и со всеми ее компонентами, может быть представлено как

$$\mathbf{Y}^{\mathbf{S}} = \{\mathbf{Y}^{\mathbf{O}_{i^S}}\}. \qquad (3)$$

Каждому объекту $\mathbf{O}_{i^S}$ сопоставляется некоторое множество угроз $\mathbf{Y}^{\mathbf{O}_{i^S}}$. Таким образом, множество $\mathbf{Y}^{\mathbf{S}}$ представляет собой ничто иное, как модель угроз для системы $\mathbf{S}$.

Определим для системы $\mathbf{S}$ множество возможных событий риска $\mathbf{R}^{\mathbf{S}}$ нарушения ее безопасности. Если множество $\mathbf{Y}^{\mathbf{S}}$ определено достаточно полно, то любое событие $r_{i^R} \in \mathbf{R}^{\mathbf{S}}$ ($i^R \in \mathbf{I}^{\mathbf{R}}$, $\mathbf{I}^{\mathbf{R}}$ — множество индексов событий рисков, входящих в множество $\mathbf{R}^{\mathbf{S}}$) может быть представлено как результат реализации некоторого множества угроз $\mathbf{Y}^{r_{i^R}} \in \mathbf{Y}^{\mathbf{S}}$.

Алгоритмы расчетов при работе со 2-ым представлением классов объектов в автоматизированной системе управления безопасностью. События риска

Каждое событие риска r_{iR} имеет три основных количественных характеристики: c_{iR} — цену риска — оценку ущерба, который может быть нанесен системе **S** событием риска r_{iR}, p_{iR} — вероятность события риска r_{iR} и w_{iR} — величину риска, рассчитываемую по формуле:

$$w_{iR} = c_{iR} \times p_{iR} \qquad (4)$$

При этом важно отметить, что вероятность p_{iR} события риска r_{iR} может быть рассчитана как произведение вероятностей реализации каждой из угроз множества $\mathbf{Y}^{r_{iR}}$:

$$p_{iR} = \prod_{x=1}^{X^{r_{iR}}} p_x^{r_{iR}}, \qquad (5)$$

где $X^{r_{iR}}$ — количество угроз множества $\mathbf{Y}^{r_{iR}}$.

Алгоритмы расчетов при работе со 2-ым представлением классов объектов в автоматизированной системе управления безопасностью. Расчет рискообразующих потенциалов угроз

Каждое из возможных событий риска, в силу самой возможности их реализации с указанными выше параметрами, привносит в систему потенциал риска, и, таким образом, обладает тем, что далее предлагается называть, *рискообразующим потенциалом*. Поскольку событие риска есть результат одновременной реализации множества угроз $\mathbf{Y}^{r_{jR}}$, то можно говорить о том, что это множество угроз в рамках системы $\mathbf{S}$ обладает совокупным рискообразующим потенциалом w_{i^R}. Рискообразующий потенциал каждой из угроз, входящих в множество $\mathbf{Y}^{r_{jR}}$, предлагается рассчитывать по формуле:

$$q_{i^R} = \frac{w_{i^R}}{X^{r_{jR}}}. \qquad (6)$$

Эта формула справедлива постольку, поскольку отражает тот факт, что если бы хоть одна из угроз не была реализована, то событие риска r_{i^R} не произошло. То есть не было бы никакого события риска, либо это было бы совсем другое событие, с совершенно иными показателями цены риска, вероятности этого события и величины риска по этому событию. Поэтому, естественно, предположить, что «вклад» каждой угрозы, из множества тех угроз, которые приводят к рассматриваемому событию риска, характеризуемый ее рискообразующим потенциалом по данному событию, одинаков и может быть рассчитан по формуле (6).

Алгоритмы расчетов при работе со 2-ым представлением классов объектов в автоматизированной системе управления безопасностью. Горизонтальная свертка по угрозам.

При построении моделей всех событий из множества $\mathbf{R}^{ii}$, любая из угроз y_{i^Y} ($i^Y \in \mathbf{I}^Y$, $\mathbf{I}^Y$ — множество индексов угроз, входящих в множество $\mathbf{Y}^{ii}$) из множества $\mathbf{Y}^{ii}$ могла войти в качестве рискообразующей в некоторое подмножество $\mathbf{R}^{i^Y}$ множества моделей событий риска $\mathbf{R}^{ii}$. Соответственно, для нее может быть определено множество $\mathbf{Q}^{i^Y}$ значений ее рискообразующего потенциала по каждому из событий рисков в число рискообразующих угроз которых она входит.

В принципе, как правило, может быть построено неограниченно большое количество моделей событий риска, в которых каждая из угроз играет какую-то рискообразующую роль, но, с точки зрения решения задачи управления рисками, имеют значение только такие модели риска, которые помогают определить реальную значимость той или иной угрозы нарушения безопасности системы **S**. Очевидно, что *реальная значимость угрозы* y_{i^Y} — *ее системный рискообразующий потенциал* $q^{i^{YS}}$ — определяется максимальным значением ее рискообразующего потенциала по всем моделям рисков множества $\mathbf{R}^{i^Y}$:

$$q^{i^{YS}} = \max \mathbf{Q}^{i^Y}. \qquad (7)$$

Постольку поскольку каждая из угроз соотнесена с некоторым компонентом системы **S** и каждому из компонентов $\mathbf{O}_i$ соответствует множество угроз $\mathbf{Y}^{\mathbf{0}_i} = \left\{ y_{i^0}, i^{\mathbf{0}} \in \mathbf{I}^{\mathbf{0}} \right\}$, то для любого из объектов $\mathbf{O}_i$, который не включает в себя компонентов более низкого уровня иерархии, рискообразующий потенциал $q^{\mathbf{0}_i}$ рассчитывается по формуле:

$$q^{\mathbf{0}_i} = \sum_{i^0}^{\mathbf{I}^{\mathbf{0}}} q_{i^0}^S, \qquad (8)$$

где $q_{i^0}^S$ — системный рискообразующий потенциал угрозы $y_{i^0} \in \mathbf{Y}^{\mathbf{0}i}$.

Алгоритмы расчетов при работе со 2-ым представлением классов объектов в автоматизированной системе управления безопасностью. Расчет рисков на основе вертикального агрегирования

Если компонент $\mathbf{O}_i$ j-го иерархического уровня включает в себя множество компонентов $j+1$ уровня иерархии $\mathbf{O}_i^j \supset \left\{ \mathbf{O}_{i^z}^j, i^z \in \mathbf{I}^Z \right\}$, $\mathbf{I}^Z$ - количество объектов на j+1 уровне, входящих в качестве компонентов объекта $\mathbf{O}_i$ то его рискообразующий потенциал $q^{\mathbf{O}_i^j}$ рассчитывается как сумма рискообразующего потенциала угроз для этого компонента и сумма рискообразующих потенциалов компонентов, входящих в его состав:

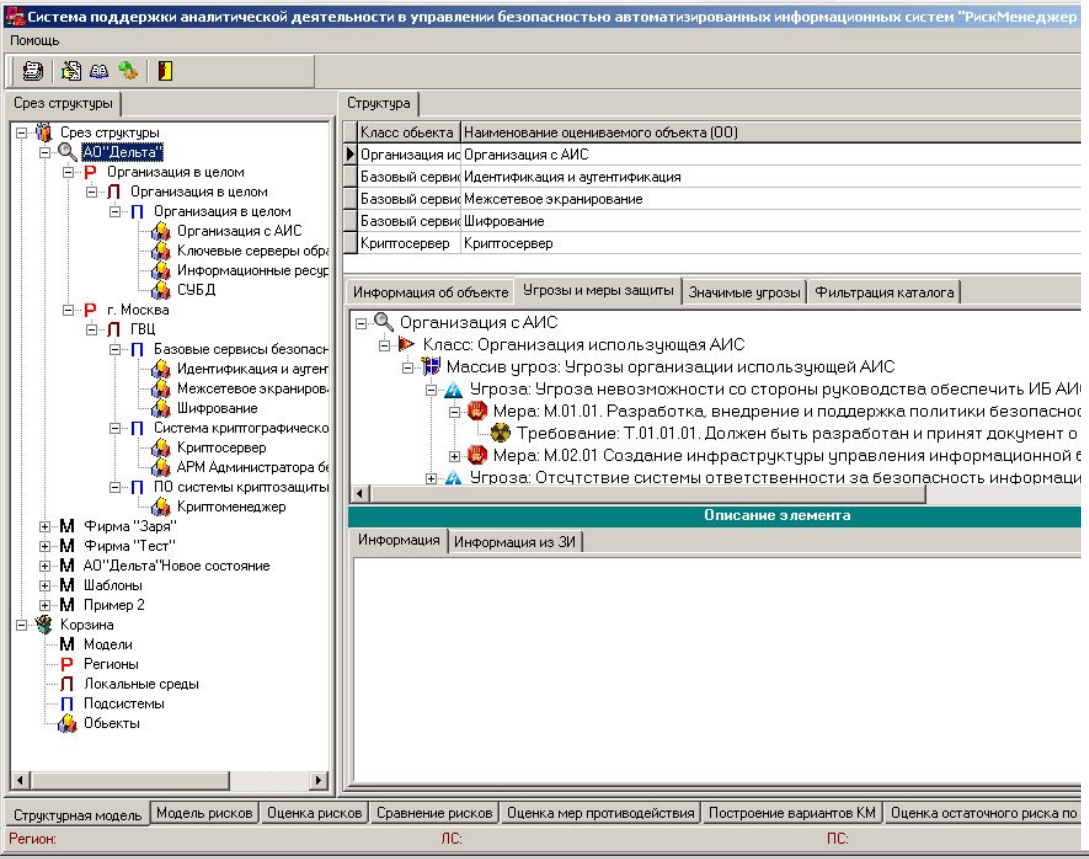
$$q^{\mathbf{O}_i^j} = \sum_{i^0}^{\mathbf{I}^0} q_{i^0}^S + \sum_{i^z}^{\mathbf{I}^Z} q_{i^z}^{\mathbf{O}_i^{j+1}}, \qquad (9)$$

где $q_{i^z}^{\mathbf{O}_i^{j+1}}$ — рискообразующий потенциал компонента $O_{i^z}^{j+1} \subset \mathbf{O}_i^j$.

Таким образом, если учесть, что в предлагаемой системе понятий оценка риска по компоненте есть ни что иное, как ее рискообразующий потенциал, а в качестве компоненты может рассматриваться любая часть (подсистема) системы и система в целом, то формула (9) является общей формулой для расчета оценок риска для системы **S** и всех ее частей (подсистем).

Пример работы с 2-ым представлением классов объектов в автоматизированной системе управления безопасностью

Построение моделей угроз



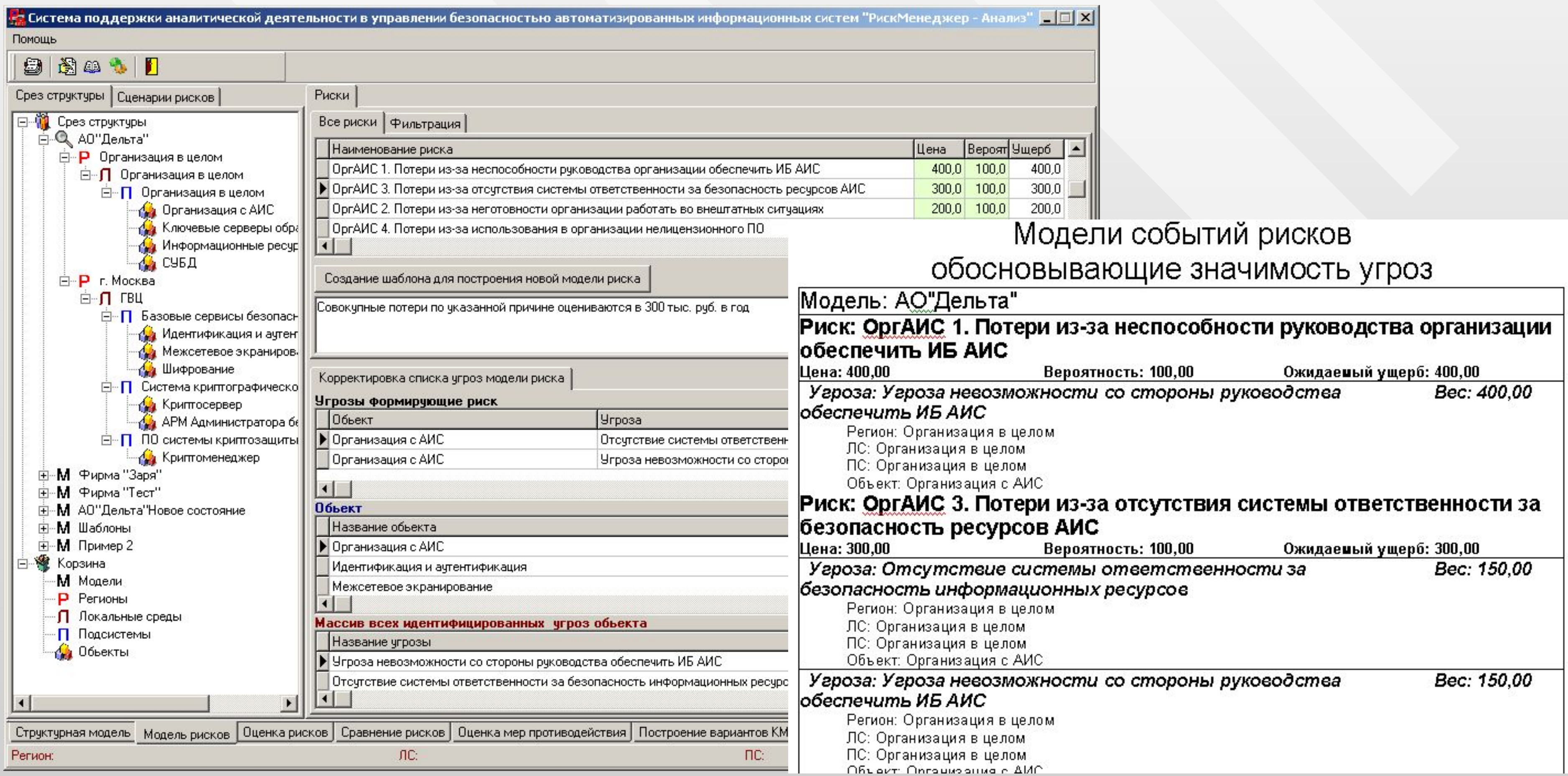
ПК "РискМенеджер" Форма РИСК-02М

Модель угроз информационной безопасности оцениваемой системы

Название модели: АО"Дельта"	
Регион: Организация в целом	
ЛС: Организация в целом	
ПС: Организация в целом	
Объект: Организация с АИС	
Угрозы:	
	Угроза невозможности со стороны руководства обеспечить ИБ АИС
	Отсутствие системы ответственности за безопасность информационных ресурсов
	Неготовность организации к работе во внештатных ситуациях
	Использование нелицензионного ПО
	Игнорирование требований политики безопасности сотрудниками организации
	Нарушение безопасного функционирования АИС при проведении аудита
Объект: Ключевые серверы обработки информации	
Угрозы:	
	Недостаточная надежность системы резервного электроснабжения оборудования АИС
	Отсутствие системы мониторинга и управления ИБП
	Отсутствие системы защиты серверов от скачков напряжения
	Скачки напряжения в электросети
ПТК_1.1.1	Несанкционированный вход в систему с осуществлением НСД к устройствам системы, программам и ИР на МН
ПТК_2.1.1	Анонимный вход/выход из системы или анонимный запуск и прекращение ее работы.
ПТК_2.2	Хищение носителей информации
ПТК_4.1	Встраивание в ПО средств позволяющих обойти или модифицировать систему защиты информации
ПТК_4.2	НСД к ОО посторонних лиц
ПТК_4.4.	Неявная модификация СЗИ НСД, таким образом, что СЗИ НСД перестают выполнять свои функции в полном объеме.
ПТК_4.5	Выход из строя ПО СЗИ НСД
Объект: Информационные ресурсы организации	
Угрозы:	
ИСА_УИР	Уничтожение ИР, в результате пожара, террористического акта и т.п. катастрофических событий приводящих к разрушениям

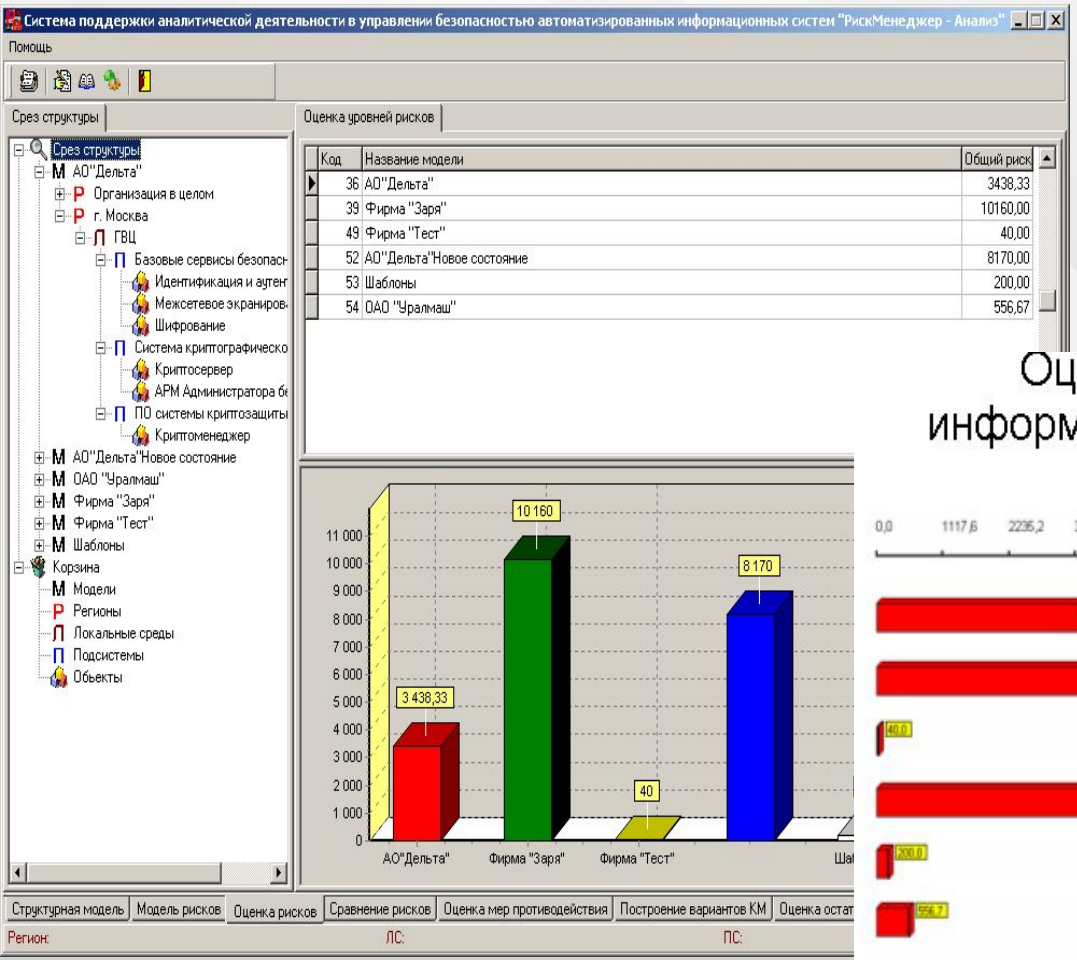
Пример работы с 2-ым представлением классов объектов в автоматизированной системе управления безопасностью

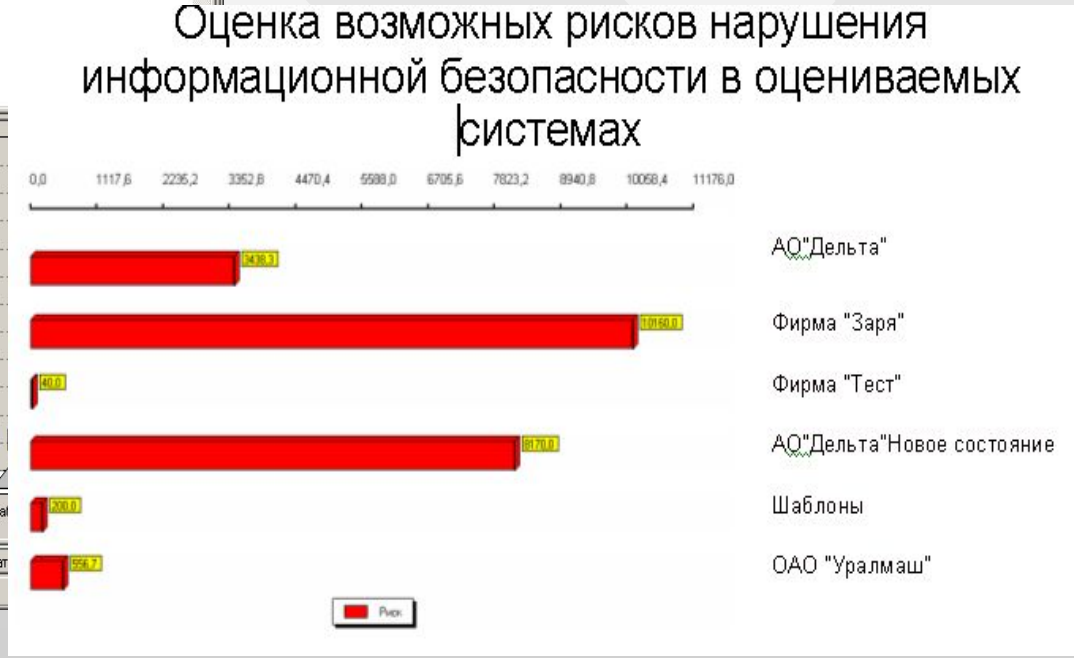
Построение моделей событий риска и расчет рискообразующих потенциалов угроз



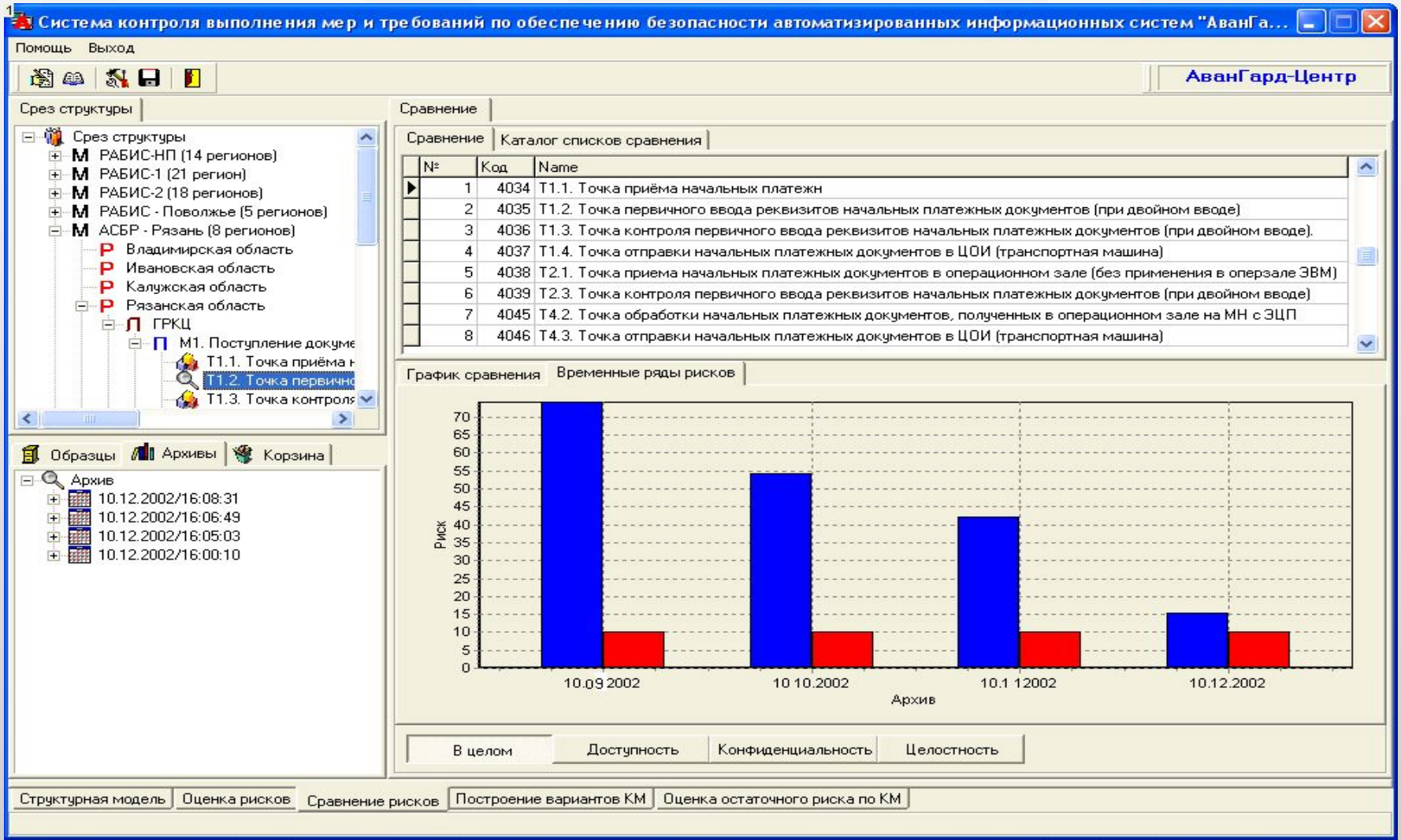
Пример работы с 2-ым представлением классов объектов в автоматизированной системе управления безопасностью

Оценка рисков нарушения безопасности





Использование временных версий (срезов) в автоматизированной системе управления безопасностью для отслеживания динамики состояния безопасности



Разработчик:
Лаборатория системного анализа проблем информатизации Института системного анализа РАН

Наш адрес в Internet:

www.OcenkaRiskov.tk

Телефон для справок:
(499) 135-50-43