Теоретические положения управления критериальными рисками

Кононов А.А.
Лаборатория 0-1 ИСА РАН

Введение понятия критериальных рисков

- Пусть существует некоторая организационная (социально-экономическая) система.
- Для того, чтобы не произошло ЧС, или чтобы ущерб и жертвы при неизбежной природной катастрофе были минимальны, система должна соответствовать некоторому идеальному множеству критериев, или, иными словами, в ней должно выполняться некоторое идеальное множество требований.
- Риски ЧС существующие из-за не полного выполнения идеального множества требований будем называть **критериальными рисками.**

Причины существования критериальных рисков

1. Заданная к исполнению система требований некорректна (отлична от идеальной):
   - Неполна;
   - Избыточна;
   - Требования некорректны;
   - Требования противоречивы;
   - Требования некорректно ранжированы

2. Невыполнение корректных требований заданной к исполнению системы требований.

Пример реализации критериальных рисков возникших из-за некорректной критериальной базы

«Низкий уровень информационного взаимодействия в области мониторинга и прогнозирования ЧС сказывается и на ведомственной нормативной базе. В ряде случаев ЧС, что называется, формируются в полном соответствии с инструкциями. Только один пример: ЗЕЯ. Аномалия осадков в районе Зейской ГЭС привела к затоплению ряда населенных пунктов, только потому, что решение о повышении сбросов воды с водохранилища принимается не на основе оценки складывающейся ситуации, а по достижению определенной отметки. В результате, когда назревает необходимость повысить сбросы, с тем чтобы избежать переполнения водохранилища, их уровень должен быть уже такой, что избежать ЧС уже не представляется возможным.»

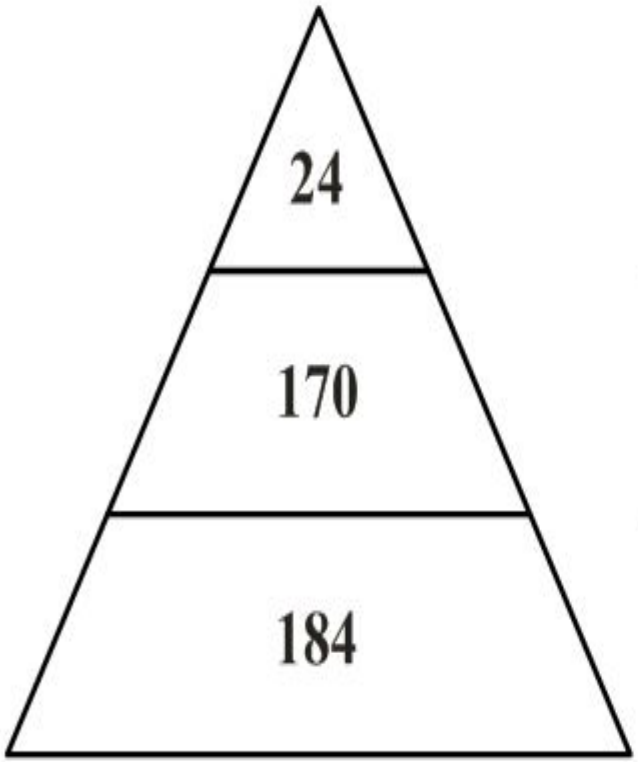
(В.Р. Болов. Основные проблемы повышения эффективности функционирования системы мониторинга и прогнозирования чрезвычайных ситуаций и пути их решения // Проблемы прогнозирования чрезвычайных ситуаций. VII научно-практическая конференция. 2-4 октября 2007 г. Доклады и выступления. – М: «МТП-инвест», 2008. Стр. 15.)

Пример формирования критериальных рисков из-за невыполнения требований:

«Пирамида нарушений» требований безопасности в нефтегазовом комплексе, приведших к катастрофам

Всего при расследовании 118 аварий и несчастных случаев,

зафиксировано 378 нарушений.



Нарушения нормативных актов, принимаемых законодательными органами власти, указов Президента и Постановлений Правительства

Нарушения нормативно-правовых актов, принимаемых федеральными органами исполнительной власти

Нарушения стандартов организаций и предприятий

Таблица 1

Нарушения требований безопасности на объекте, зафиксированные при расследовании аварий или несчастных случаев на этом объекте

Виды деятельности/ Нарушаемые акты	Строительство скважин	Эксплуатация нефтяных месторождений	Добыча и комплексная подготовка нефти, газа и конденсата	Эксплуатация насосных и компрессорных станций	Эксплуатация газоперерабатывающих и гелиевых заводов	Сейсморазведка и эксплуатация нефтяных шахт	Эксплуатация внутрипромысловых трубопроводов	Всего
1. Нарушения нормативных актов, принимаемых законодательными органами власти	3 (2)	14 (12)	4 (4)	-	-	-	3 (2)	24 (20)
2. Нарушения нормативных актов, принимаемых федеральными органами исполнительными власти	19 (11)	78 (37)	23 (13)	2 (2)	8 (4)	24 (14)	16 (8)	170 (89)
3. Нарушения документов предприятий и организаций	22 (11)	86 (38)	27 (13)	1 (1)	5 (2)	29 (13)	14 (5)	184 (83)

( ) – число аварий и несчастных случаев, в которых зафиксированы данные нарушения

Устаревшие правила и нормы создают аварийные ситуации

Многие нормы были установлены более 30 лет тому назад и не соответствуют современному оснащению объектов и менталитету персонала. Более того, следование некоторым требованиям зачастую приводит к аварийной ситуации. К сожалению, проблема своевременного и качественного пересмотра норм за последние 20 лет так и не была решена.

Если система требований такова, что часть ее требований противоречива, избыточна, неисполнима в конкретных условиях, то это может стать источником культивирования безответственного отношения к проблемам безопасности в целом.

Критериальные риски – риски возможных и фактических потерь, являющихся следствием несовершенства систем критериев используемых при принятии решений и/или невыполнения критериальных требований при реализации принимаемых решений

Классы критериальных рисков

Класс 1.
Риски несовершенства критериальной базы

Класс 2.
Риски ошибочных приоритетов критериальной базы

Класс 3.
Риски несоответствия критериям (невыполнения требований)

Задачи оценки критериальных рисков и задачи многокритериального выбора

- **Необходимо отличать задачи оценки критериальных рисков от задач многокритериального выбора**

- **Задачи многокритериального выбора возникают при выборе лучшего из множества вариантов по заданной критериальной базе. Задачи хорошо изучены. Разработана теория выбора Парето-оптимальных решений**

- **Задачи оценки критериальных рисков возникают при оценке качества критериальной базы – ее полноты, непротиворечивости, неизбыточности, а так же при оценке выполнения критериев в задачах контроля.**

Критерии определения безопасности компьютерных систем

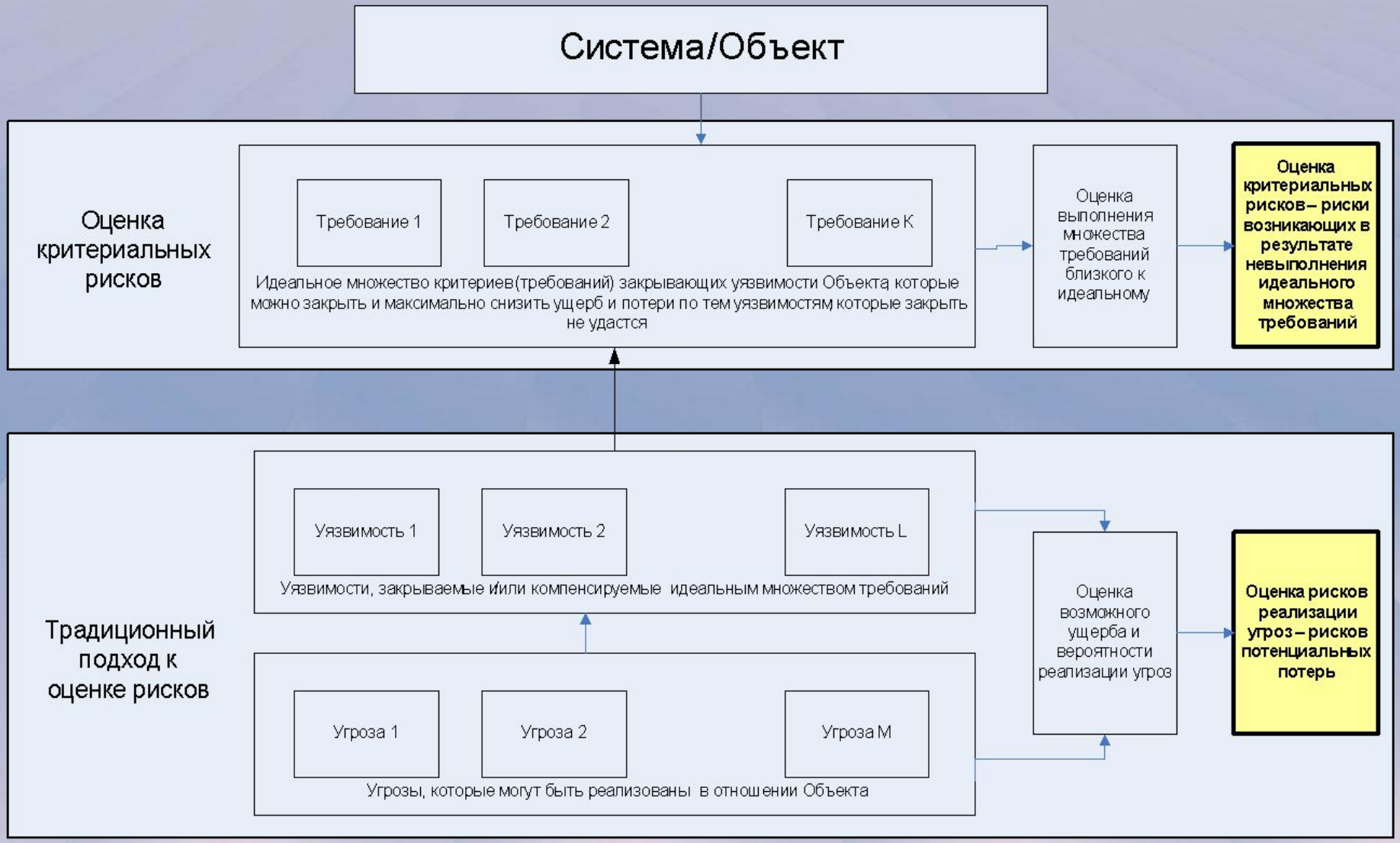
- **Критерии определения безопасности компьютерных систем** (англ. *Trusted Computer System Evaluation Criteria*) — стандарт Министерства обороны) — стандарт Министерства обороны США, устанавливающий основные условия для оценки эффективности средств компьютерной безопасности, содержащихся в компьютерной системе. Критерии используются для определения, классификации и выбора компьютерных систем предназначенных для обработки, хранения и поиска важной или секретной информации.
- **Основные цели и средства**
- **Политики**
- Политики безопасности должны быть подробными, четко определёнными и обязательными для компьютерной системы. Есть две основных политики безопасности:
- Мандатная политика безопасности — обязательные правила управления доступом напрямую основанные на индивидуальном разрешении, разрешении на доступ к информации и уровне конфиденциальности запрашиваемой информации. Другие косвенные факторы являются существенными и окружающими. Эта политика также должна точно соответствовать закону, главной политике и прочим важным руководствам, в которых устанавливаются правила.
  - Маркирование — системы предназначенные для обязательной мандатной политики безопасности должны предоставлять и сохранять целостность меток управления доступом и хранить метки, если объект перемещён.
- Дискреционная политика безопасности — предоставляет непротиворечивый набор правил для управления и ограничения доступа, основанный на идентификации тех пользователей, которые намерены получить только необходимую им информацию.
- **Ответственность**
- Индивидуальная ответственность в независимости от политики должна быть обязательной. Есть три требования по условиям ответственности:
- Аутентификация — процесс используемый для распознавания индивидуального пользователя.
- Авторизация — проверка разрешения индивидуальному пользователю на получение информации определённого рода.
- Аудит — контролируемая информация должна избирательно храниться и защищаться в мере, достаточной для отслеживания действий аутентифицированного пользователя, затрагивающих безопасность.
- **Гарантии**
- Компьютерная система должна содержать аппаратные и/или программные механизмы, которые могут независимо определять обеспечивается ли достаточная уверенность в том, что система исполняет указанные выше требования. В добавок, уверенность должна включать гарантию того, что безопасная часть системы работает только так, как запланировано. Для достижения этих целей необходимо два типа гарантий и соответствующих им элементов:
- Механизмы гарантий
  - Операционная гарантия — уверенность в том, что реализация спроектированной системы обеспечивает осуществление принятой стратегии защиты системы. Сюда относятся системная архитектура, целостность системы, анализ скрытых каналов, безопасное управление возможностями и безопасное восстановление.
  - Гарантия жизненного цикла — уверенность в том, что система разработана и поддерживается в соответствии с формализованными и жестко контролируемыми критериями функционирования. Сюда относятся тестирование безопасности, задание на проектирование и его проверка, управление настройками и соответствие параметров системы заявленным.
- Гарантии непрерывной защиты — надёжные механизмы, обеспечивающие непрерывную защиту основных средств от преступных и/или несанкционированных изменений.
- **Документирование**
- В каждом классе есть дополнительный набор документов, который адресован разработчикам, пользователям и администраторам системы в соответствии с их полномочиями. Эта документация содержит:
- Руководство пользователя по особенностям безопасности.
- Руководство по безопасным средствам работы.
- Документация о тестировании.
- Проектная документация

Общие критерии оценки защищённости информационных технологий —

(англ. *Common Criteria for Information Technology Security Evaluation*)

- Общеизвестным является более короткое название *Общие критерии* (*Common Criteria, CC, или ОК*). Международный стандарт). Международный стандарт (ISO). Международный стандарт (ISO/IEC). Международный стандарт (ISO/IEC 15408, ИСО/МЭК 15408-2002) по компьютерной безопасности). Международный стандарт (ISO/IEC 15408, ИСО/МЭК 15408-2002) по компьютерной безопасности. Common Criteria не приводит списка требований по безопасности или списка особенностей, которые должен содержать продукт. Вместо этого он описывает инфраструктуру (framework), в которой *потребители* компьютерной системы могут описать требования, *разработчики* могут заявить о свойствах безопасности продуктов, а *эксперты* по безопасности определить, удовлетворяет ли продукт заявлениям. Таким образом, Common Criteria позволяет обеспечить условия, в которых процесс описания, разработки и проверки продукта будет произведён с необходимой скрупулёзностью.
- **Функциональные требования**
- Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности, всего 11 функциональных классов (в трёх группах), 66 семейств, 135 компонентов.
- Первая группа определяет элементарные сервисы безопасности:
  - FAU — аудит, безопасность (требования к сервису, протоколирование и аудит);
  - FIA — идентификацияFIA — идентификация и аутентификация;
  - FRU — использование ресурсов (для обеспечения отказоустойчивости).
- Вторая группа описывает производные сервисы, реализованные на базе элементарных:
  - FCO — связь (безопасность коммуникаций отправитель-получатель);
  - FPR — приватность;
  - FDP — защита данных пользователя;
  - FPT — защита функций безопасности объекта оценки.
- Третья группа классов связана с инфраструктурой объекта оценки:
  - FCS — криптографическая поддержка (обслуживает управление криптоключами и крипто-операциями);
  - FMT — управление безопасностью;
  - FTA — доступ к объекту оценки (управление сеансами работы пользователей);
  - FTP — доверенный маршрут/канал;
- **Требования доверия**
- Требования гарантии безопасности (доверия) — требования, предъявляемые к технологии и процессу разработки и эксплуатации объекта оценки. Разделены на 10 классов, 44 семейства, 93 компонента, которые охватывают различные этапы жизненного цикла.
- Первая группа содержит классы требований, предшествующих разработке и оценки объекта:
  - APE — оценка профиля защиты;
  - ASE — оценка задания по безопасности.
- Вторая группа связана с этапами жизненного цикла объекта аттестации:
  - ADV — разработка, проектирование объекта;
  - ALC — поддержка жизненного цикла;
  - ACM — управление конфигурацией;
  - AGD — руководство администратора и пользователя;
  - ATE — тестирование;
  - AVA — оценка уязвимостей;
  - ADO — требования к поставке и эксплуатации;
  - AMA — поддержка доверия-требования, применяется после сертификации объекта на соответствие общим критериям.

Расчет критериальных рисков как альтернатива традиционному подходу к оценке рисков



Аксиоматика оценки критериальных рисков безопасности компьютеризированных систем (1)

- Предположим, что для обеспечения безопасности АИС должно быть выполнено всего лишь одно требование. Пусть возможно только два состояния – «выполнено» и «не выполнено». Таким образом, оценка выполнения требования о корректном функционировании системы будет иметь одно из двух значений – «система функционирует корректно» или «система функционирует некорректно».
- Тогда если требование выполнено, и АИС функционирует корректно, то риск пользователя будет нулевым. Если не выполнено – то риск будет 100-процентным и пользователь все потеряет.

Аксиоматика оценки критериальных рисков безопасности компьютеризированных систем (2)

- Усложним задачу. Предположим, что оценка выполнения требования безопасности определяется по шкале от 0 до 100 процентов и возможна некоторая интегральная оценка возможного ущерба, учитывающая как размер ущерба в случае невыполнения требования, так и вероятность его нанесения. Назовем эту оценку ожидаемым процентом потерь собственности зависящей от АИС. Тогда процент выполнения требования будет определять ожидаемый процент потерь собственности, зависящей от АИС.
- Обозначим через *q* процент выполнения требования.
- Ожидаемый процент потерь собственности, зависящей от АИС, по сути представляющий собой критериальный риск (*r*) пользователя, в этом случае определяется по формуле:
- $$r = 100 - q \qquad (1)$$

Аксиоматика оценки критериальных рисков безопасности компьютеризированных систем (3)

- Далее 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 выполнения каждого требования можно оценить в диапазоне от 0 до 100 процентов, то критериальные риски 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 критериальных рисков безопасности компьютеризированных систем (4)

- Далее предположим, что с каждым требованием связан такой интегральный показатель, как вес требоваия w_i , учитывающий как относительную вероятность нанесения ущерба из-за невыполнения требования, так и относительную величину этого ущерба. Пусть значение w_i также определяется по шкале от 0 до 100.
- Таким образом, задавая вес можно определить, в какой степени при оценке риска доверия к безопасности должно учитываться выполнение этого требования. Тогда формула расчета критериальных рисков принимает следующий вид:
- $$r = \sum_{i=1}^{I} \frac{w_i \times (100 - q_i)}{\sum_{i=1}^{I} w_i} \qquad (3)$$

Аксиоматика оценки критериальных рисков безопасности компьютеризированных систем (5)

- Будем называть <u>значимостью требования</u> величину рассчитываемую по формуле:

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

.

- Тогда формулу (3) расчета критериальных рисков можно переписать в виде:

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

Аксиоматика оценки критериальных рисков безопасности компьютеризированных систем (6)

- Предположим теперь, что безопасность системы зависит не от одного объекта, а от *J* объектов для каждого из которых критериальный риск был рассчитан по формуле (5). Тогда, если значимость объектов одинакова, то критериальные риски системы рассчитываются по формуле:

$$R = \frac{\sum_{j=1}^{J} r_j}{100 * J} \qquad (6)$$

Аксиоматика оценки критериальных рисков 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:

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

Приведенную логику рассуждений можно обобщить и на более общий случай, а именно, на случай многоуровневой иерархической системы. Тогда пользуясь формулой (7) можно рассчитать критериальные риски по каждому следующему иерархическому уровню, исходя из знания оценок критериальных рисков всех его структурных составляющих.

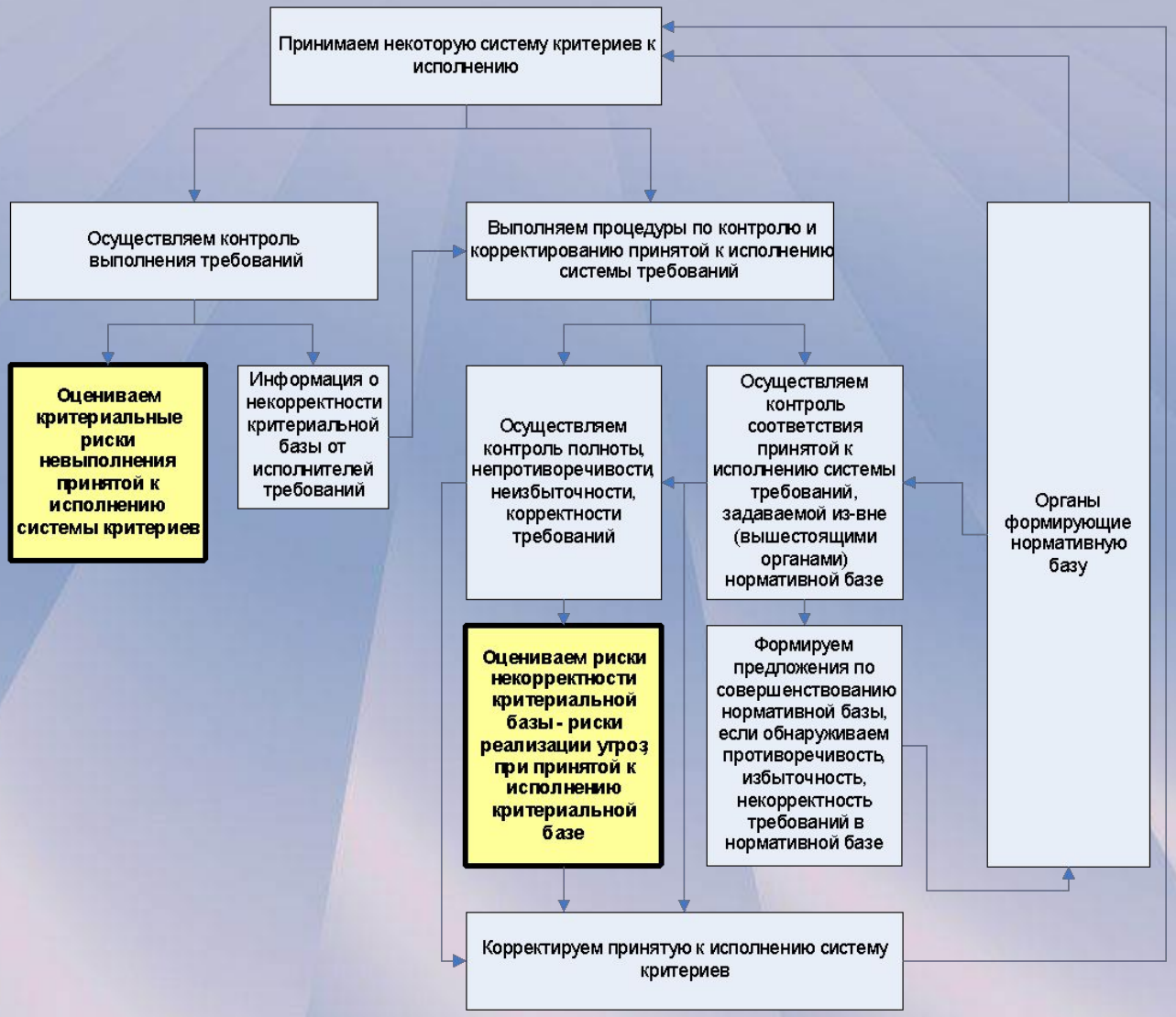
Таким образом, определив требования безопасности ко всем объектам, составляющим систему, оценив их выполнение, а так же определив значимости влияния оценок выполнения отдельных требований и оценок рисков по отдельным структурным составляющим, можно оценивать критериальные риски в системах любой иерархической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

Распределение требований безопасности по структурным составляющим, технологическим и бизнес процессам АИС

Опасные сочетания невыполненных требований (ОСНТ)

При расчете критериальных рисков по предложенной методике полностью игнорируются связи, существующие между отдельными требованиями. Это объясняется тем, что методика ориентирована на решение задач оценки в больших организационных структурах, где количество требований, отнесенных к различным объектам и процессам может исчисляться десятками и сотнями тысяч. Определить зависимости между ними в приемлемые сроки не представляется возможным. К тому же, системы требований безопасности ИВС - это системы с нестабильным составом и структурой, что является следствием частых изменений в используемых технологиях и в средах использования этих технологий, перманентно формирующих новые уязвимости и угрозы, которые в кратчайшие сроки должны парироваться и закрываться новыми требованиями по безопасности. В тоже время, как правило, на практике любая система требований безопасности реализует "эшелонированную оборону" защищаемого объекта. **Будем называть опасным сочетанием невыполненных требований (ОСНТ) такое их сочетание, наличие которого означает полную или повышенную незащищенность объекта во всех "эшелонах обороны" от какого-либо типа угроз.** Наличие ОСНТ должно расцениваться как фактор увеличивающий уровень риска. Однако, предлагаемая методика в изложенном виде не дает гарантий того, что такой уровень риска будет зафиксирован (рассчитан) при наличии ОСНТ. Поэтому предложенная методика при ее реализации должна дополняться специальными процедурами идентификации ОСНТ на основании алгоритмов их распознавания по заданным сигнатурам с целью увеличения оценок рисков в соответствии с заданными векторами увеличения риска по структурным составляющим.

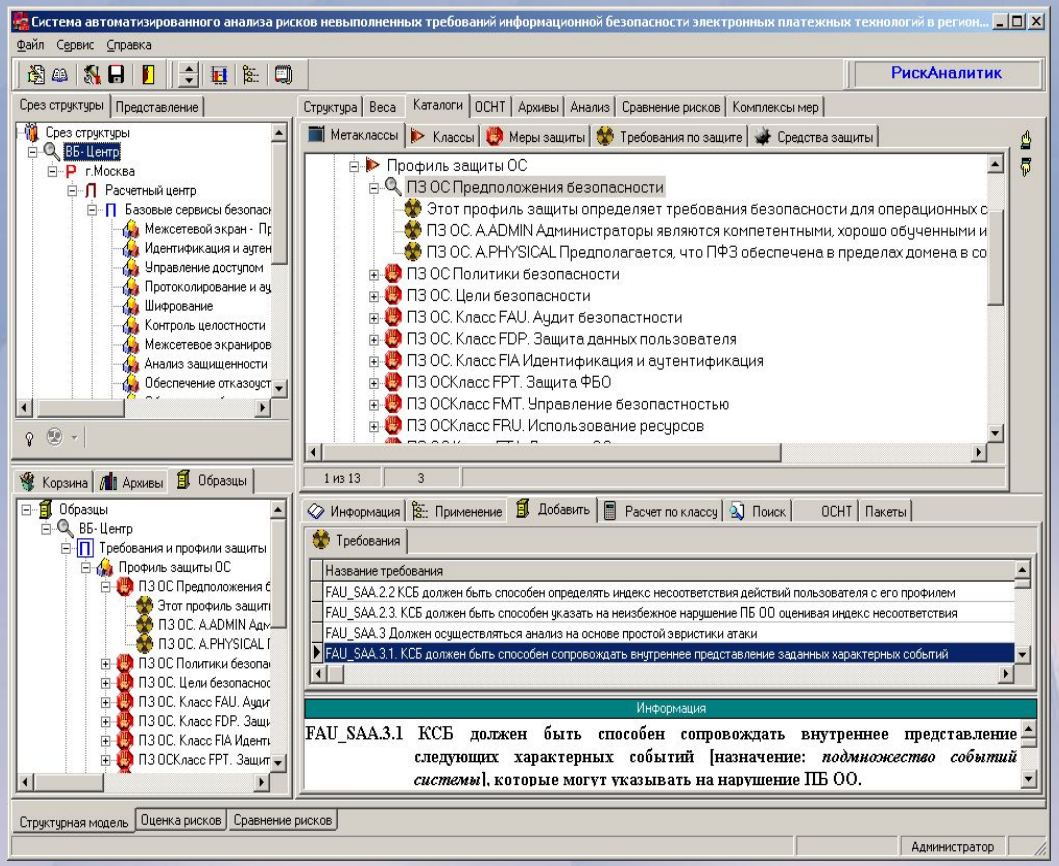
Концепция оценки критериальных рисков

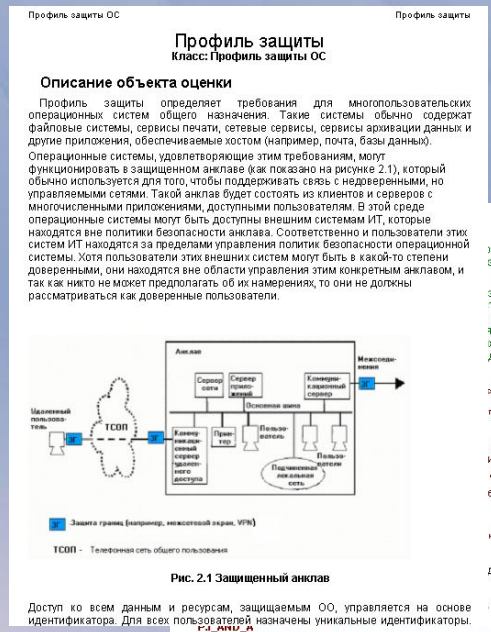


Состав и функциональные возможности системы

Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

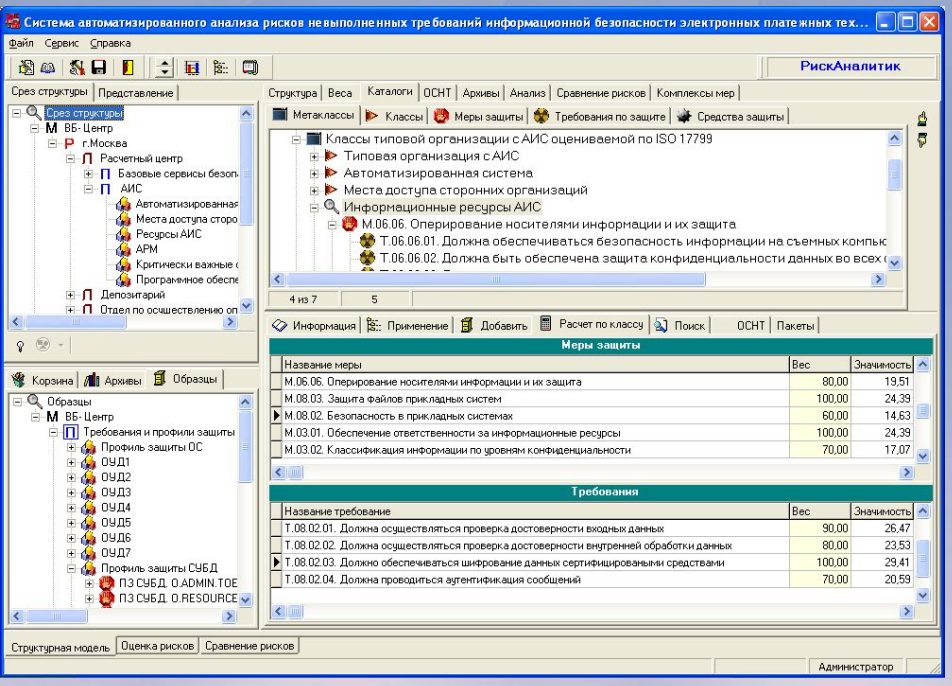
1. Разработка критериальных систем (профилей защиты)

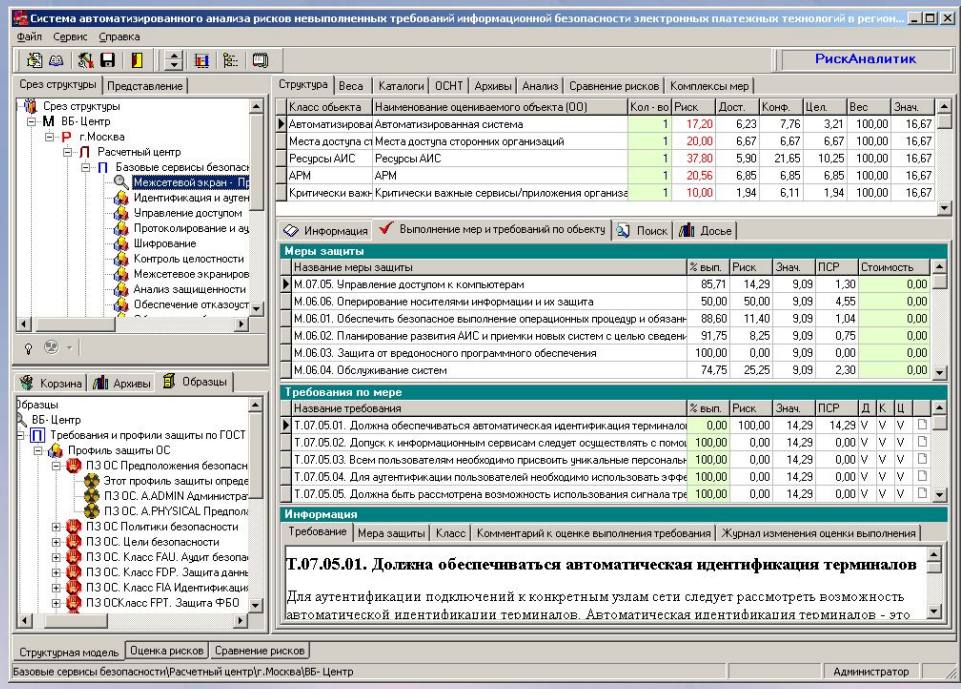




Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

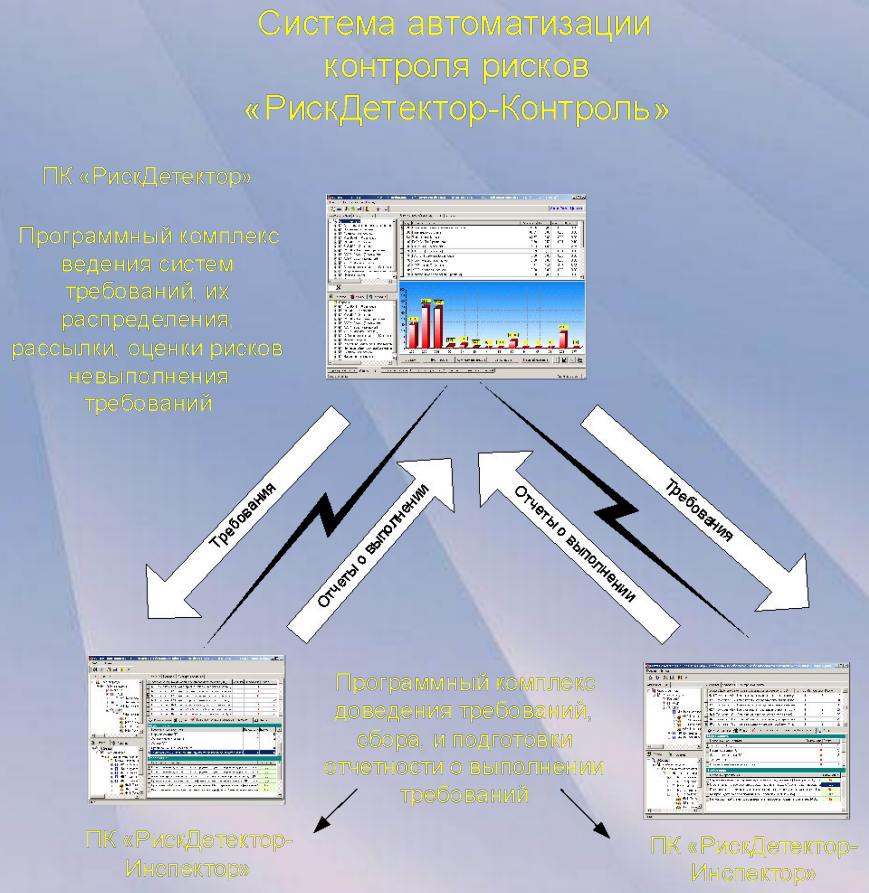
2. Построение структурной модели оцениваемой системы





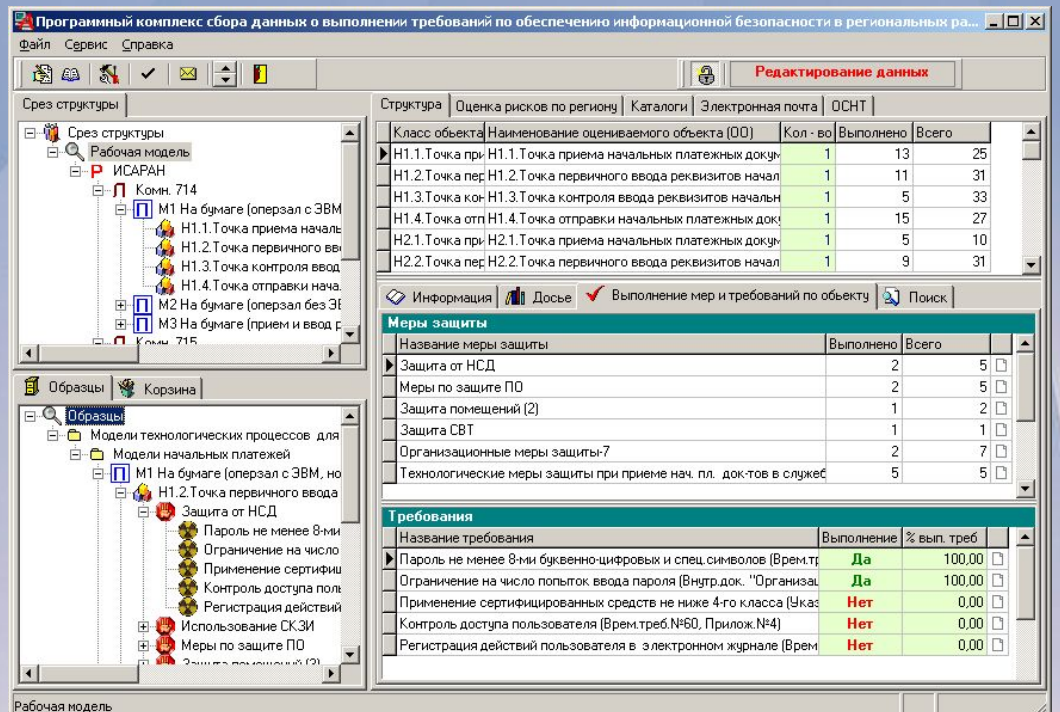
Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

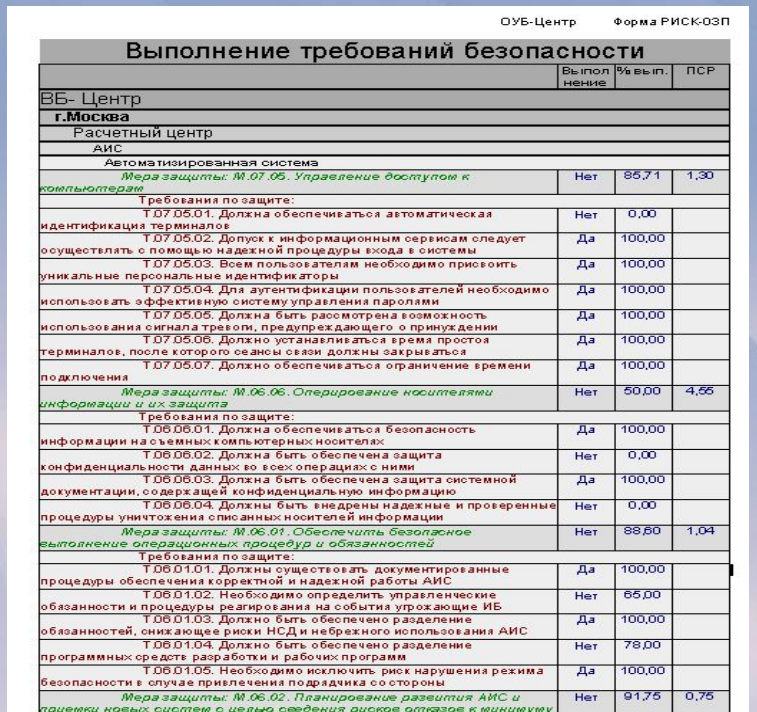
3. Автоматизированное оперативное доведение требований до исполнителей и проведение мониторинг-контроля выполнения требований ИБ.



Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

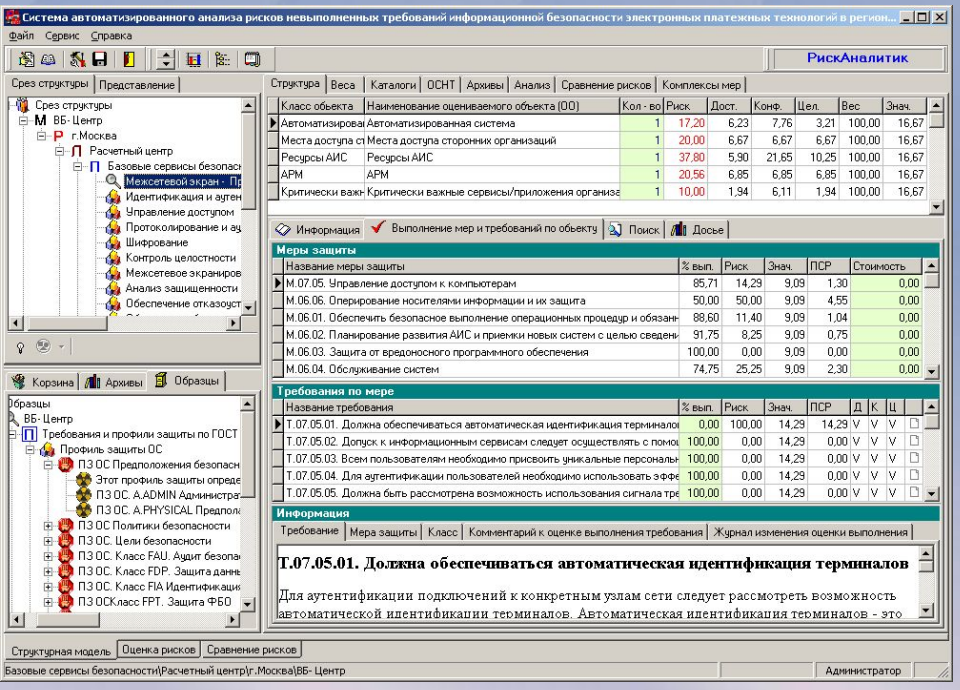
4. Проведение общего аудита информационной безопасности на соответствие требованиям ГОСТ Р ИСО/МЭК 15408, ИСО 17799, СТР-К и другим стандартам и системам требований, на основе которых строятся профили защиты

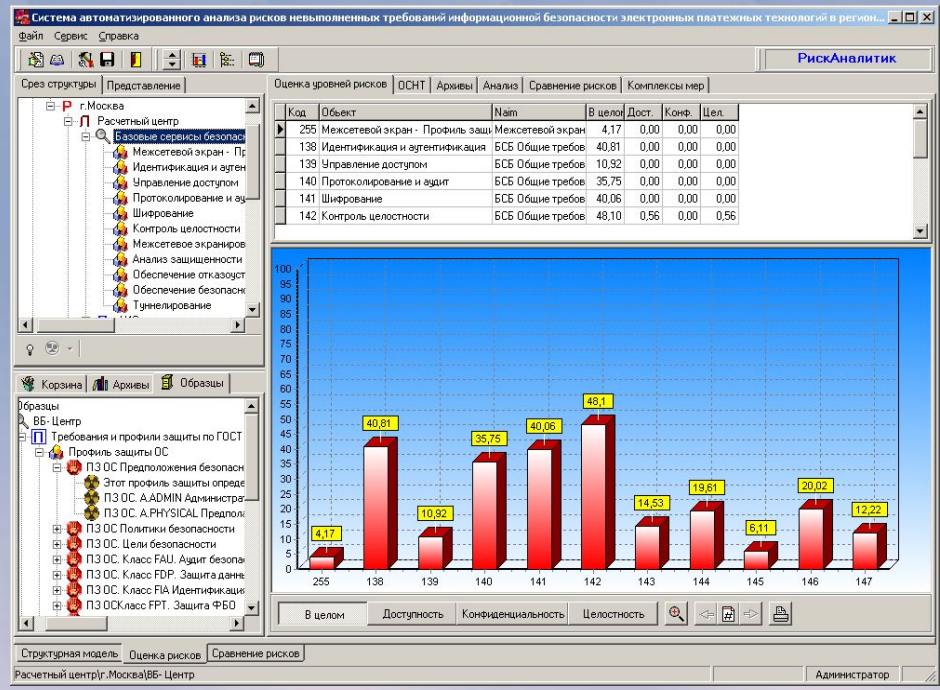




Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

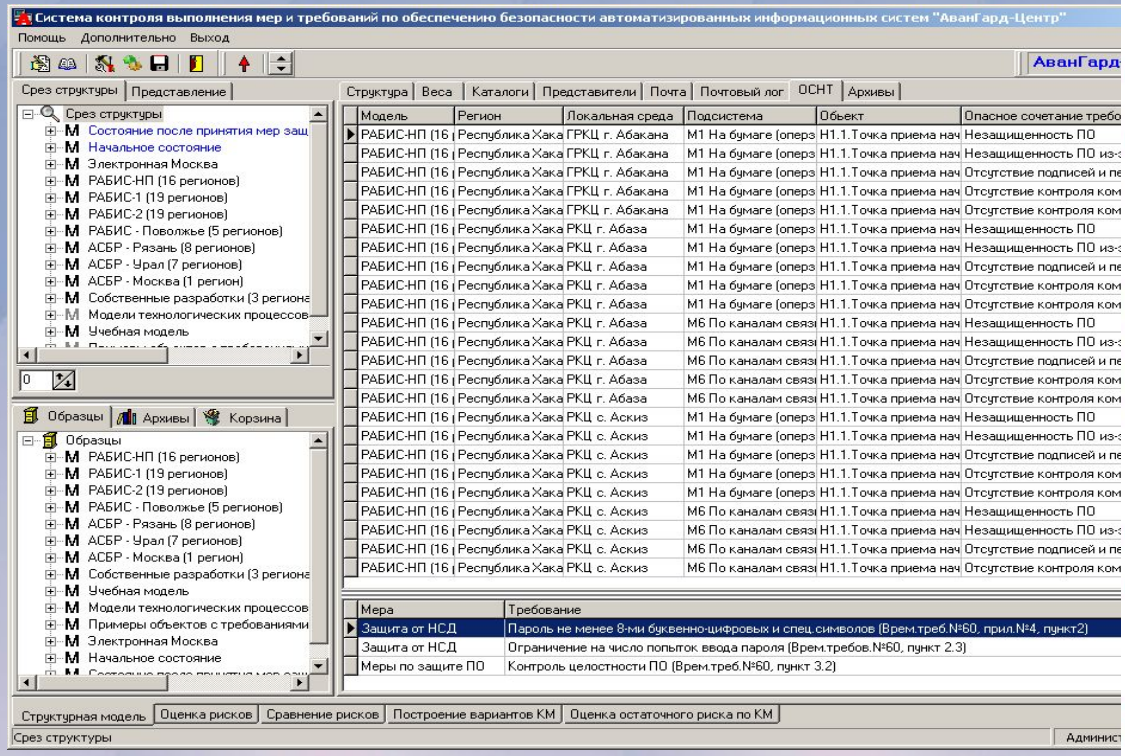
5. Оценка критериальных рисков – рисков невыполнения требований

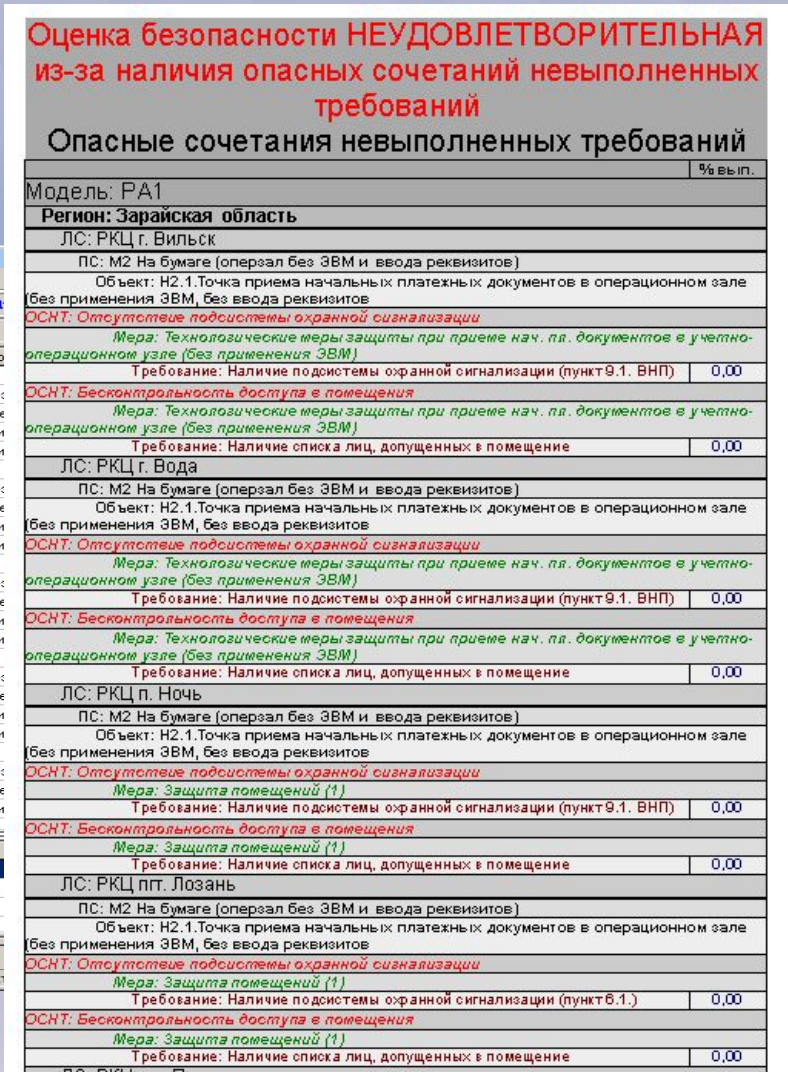




Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

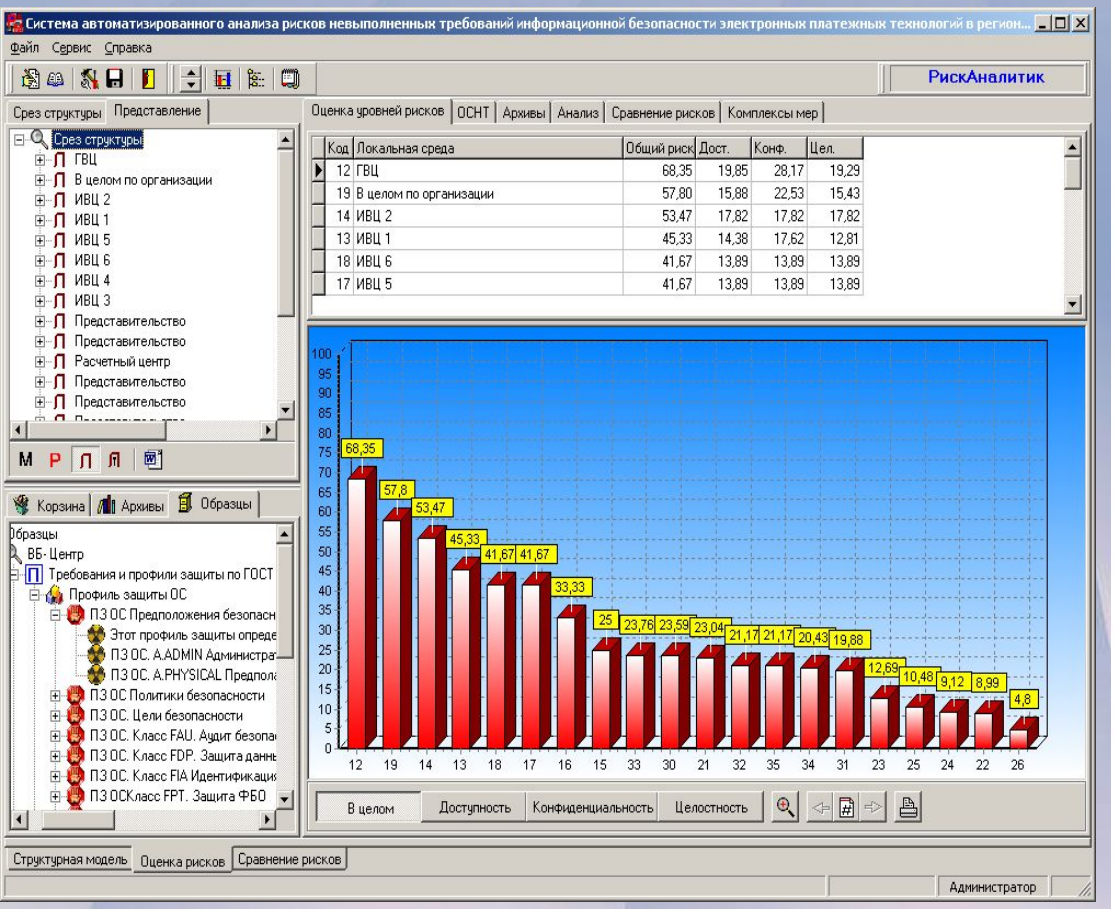
6. Выявление опасных сочетаний невыполненных требований (ОСНТ)

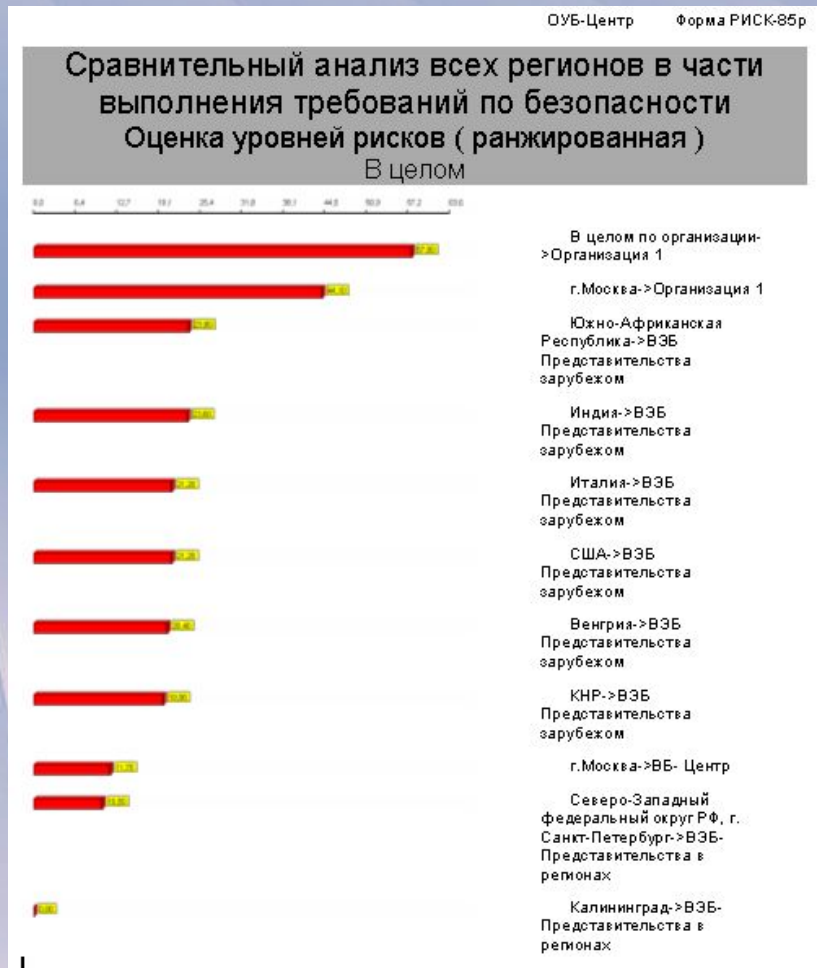




Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

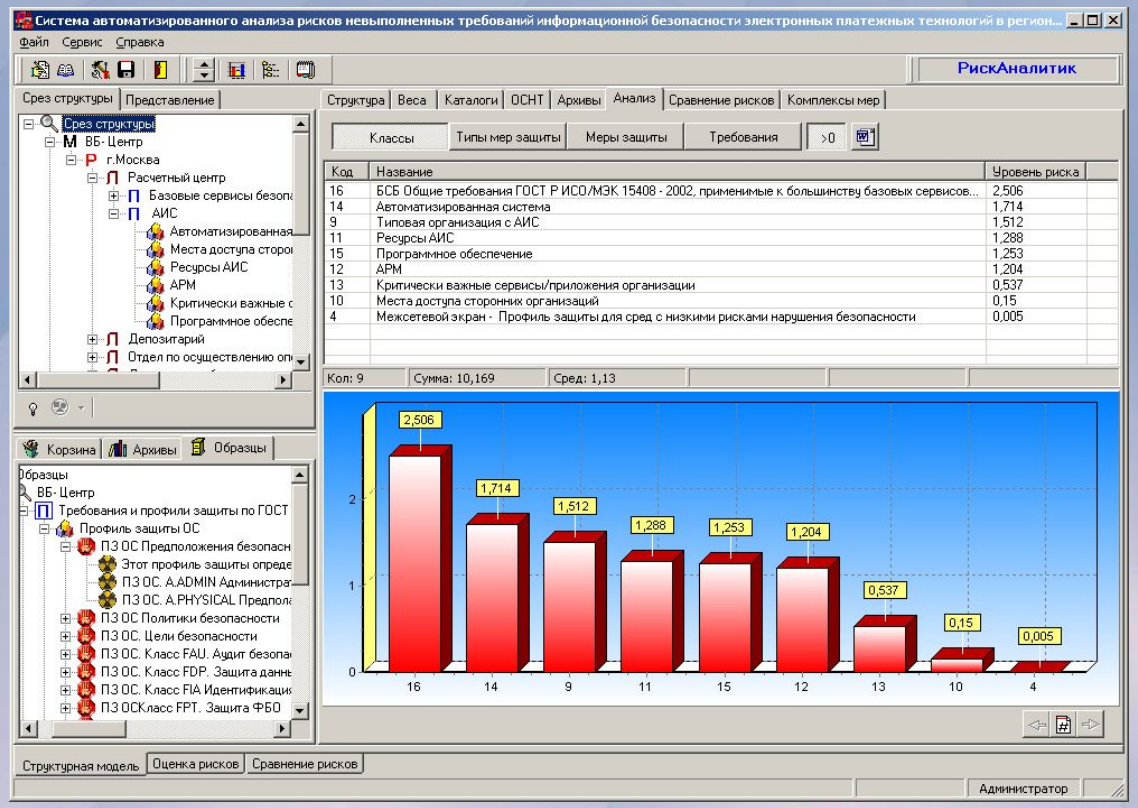
7. Выявление «узких» мест в системе безопасности

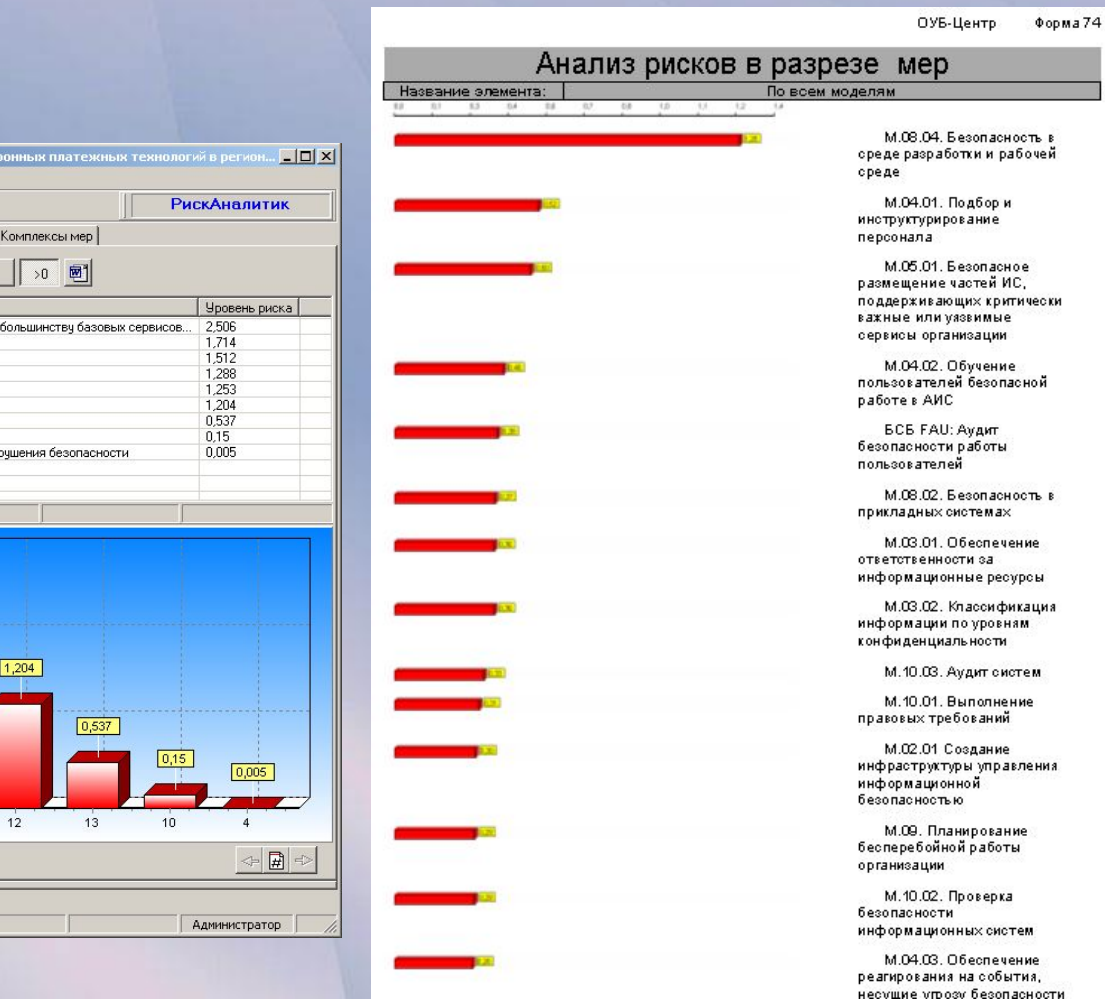




Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

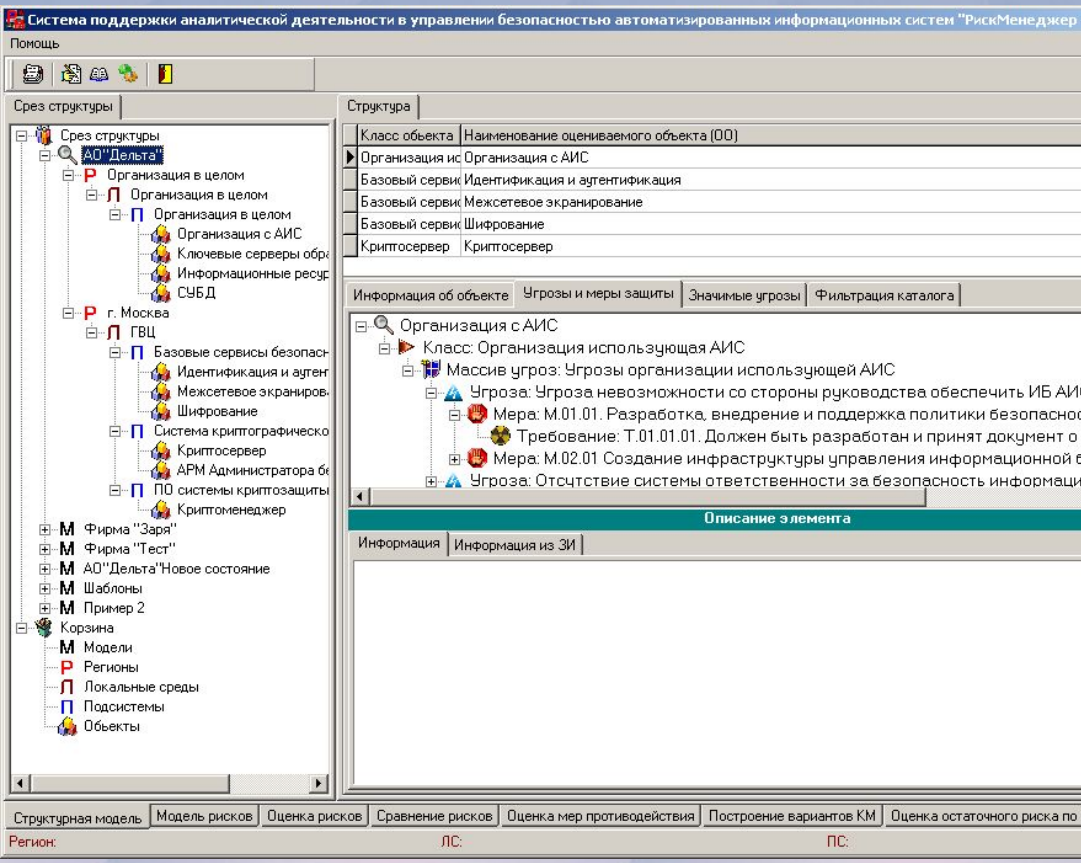
8. Выявление источников рисков





Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

9. Построение моделей угроз существующих из-за некорректности приятой к исполнению критериальной базы



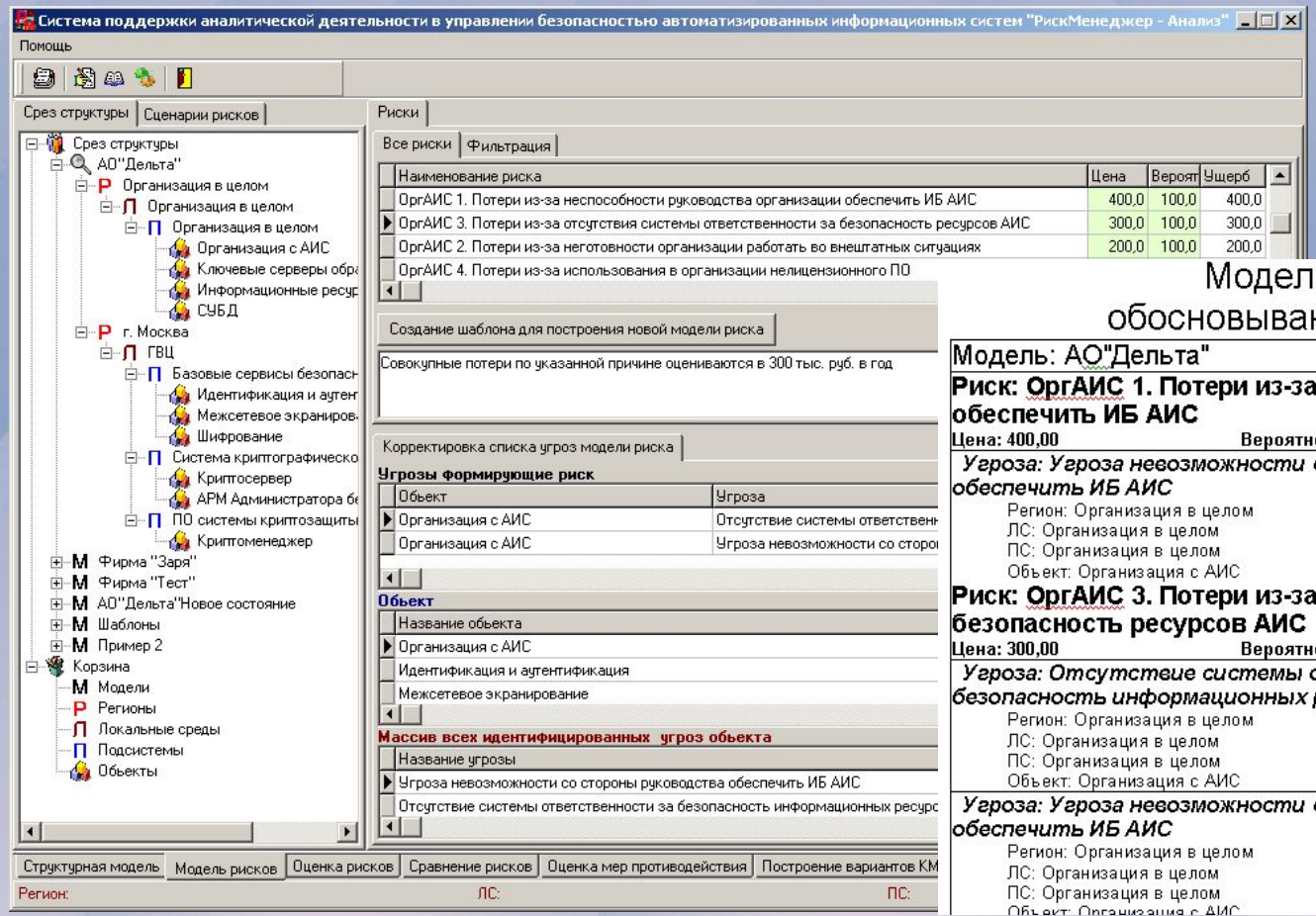
ПК "РискМенеджер" Форма РИСК-02М

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
ГТК_1.1.1	Несанкционированный вход в систему с осуществлением НСД к устройствам системы, программам и ИР на МН
ГТК_2.1.1	Анонимный вход/выход из системы или анонимный запуск и прекращение ее работы.
ГТК_2.2	Хищение носителей информации
ГТК_4.1	Встраивание в ПО средств позволяющих обойти или модифицировать систему защиты информации
ГТК_4.2	НСД к ОО посторонних лиц
ГТК_4.4.	Неявная модификация СЗИ НСД, таким образом, что СЗИ НСД перестают выполнять свои функции в полном объеме.
ГТК_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

Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

10. Построение моделей событий рисков и обоснование значимости угроз существующих в виду некорректности принятой к исполнению критериальной базы. Расчет рискообразующих потенциалов.



Модели событий рисков обосновывающие значимость угроз

Модель: АО"Дельта"

Риск: ОргАИС 1. Потери из-за неспособности руководства организации обеспечить ИБ АИС

Цена: 400,00 **Вероятность: 100,00** **Ожидаемый ущерб: 400,00**

Угроза: Угроза невозможности со стороны руководства обеспечить ИБ АИС *Вес: 400,00*

Регион: Организация в целом
ЛС: Организация в целом
ПС: Организация в целом
Объект: Организация с АИС

Риск: ОргАИС 3. Потери из-за отсутствия системы ответственности за безопасность ресурсов АИС

Цена: 300,00 **Вероятность: 100,00** **Ожидаемый ущерб: 300,00**

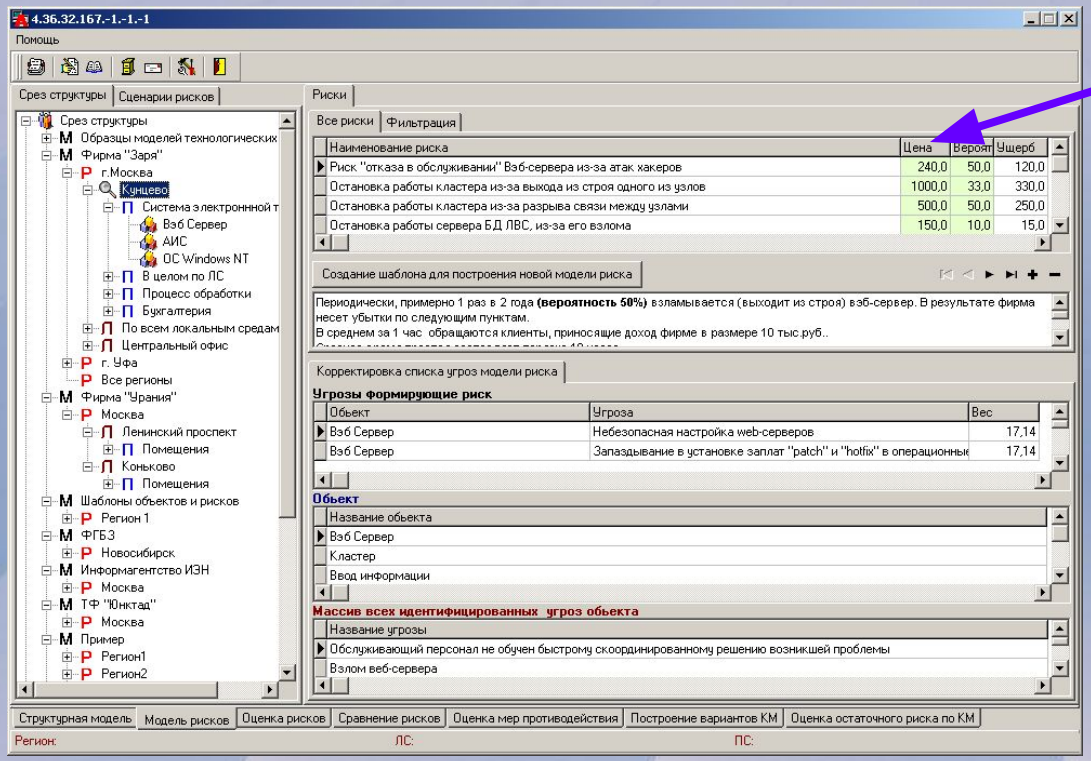
Угроза: Отсутствие системы ответственности за безопасность информационных ресурсов *Вес: 150,00*

Регион: Организация в целом
ЛС: Организация в целом
ПС: Организация в целом
Объект: Организация с АИС

Угроза: Угроза невозможности со стороны руководства обеспечить ИБ АИС *Вес: 150,00*

Регион: Организация в целом
ЛС: Организация в целом
ПС: Организация в целом

Оценки цены риска и вероятности события риска

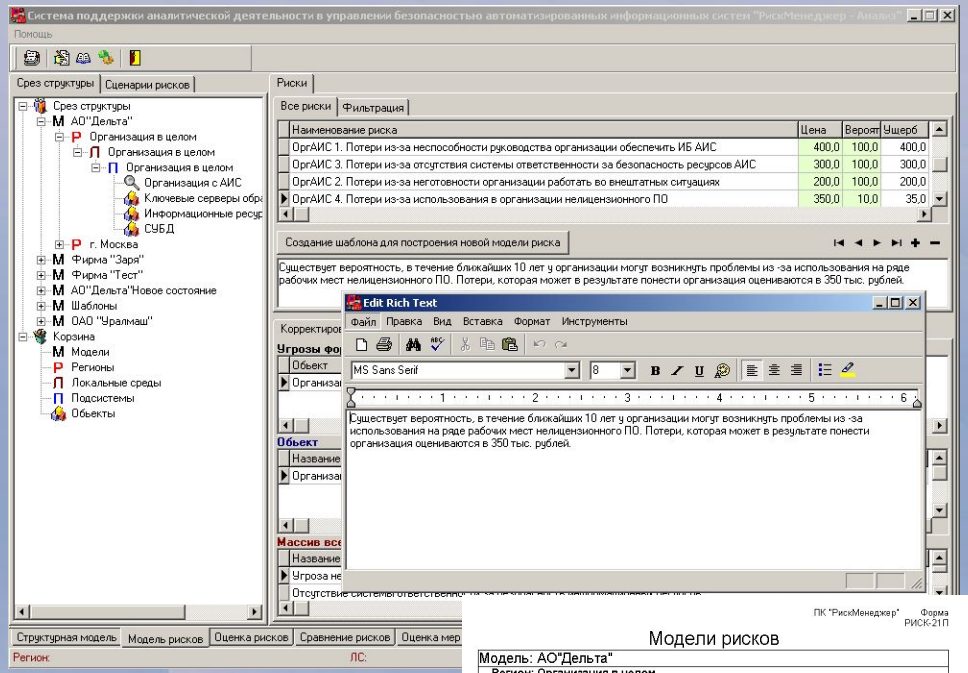


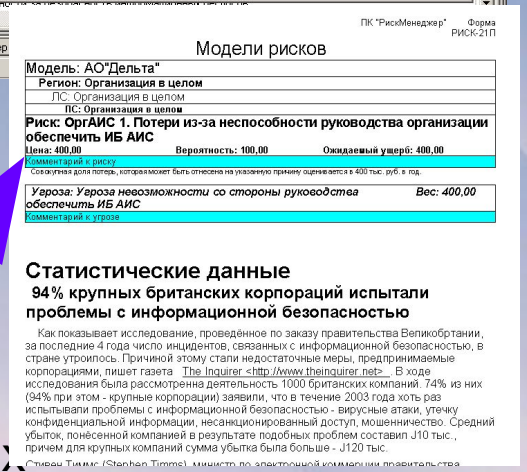
Цена риска определяется в оценочных единицах. Одна оценочная единица равна 1000 рублям. Если риски нельзя оценить в денежном выражении используется механизм кардинального ранжирования оценок опасности событий рисков.

Кардинальное ранжирование используется и для верификации экспертных оценок, как при оценке опасности событий рисков, так и при оценке вероятностей этих событий.

Метод распределенных дельфийских групп

- Еще одним механизмом верификации оценок является использование метода дельфийских групп в распределенном (заочном варианте), и сохранения обоснований даваемых экспертами по оценкам

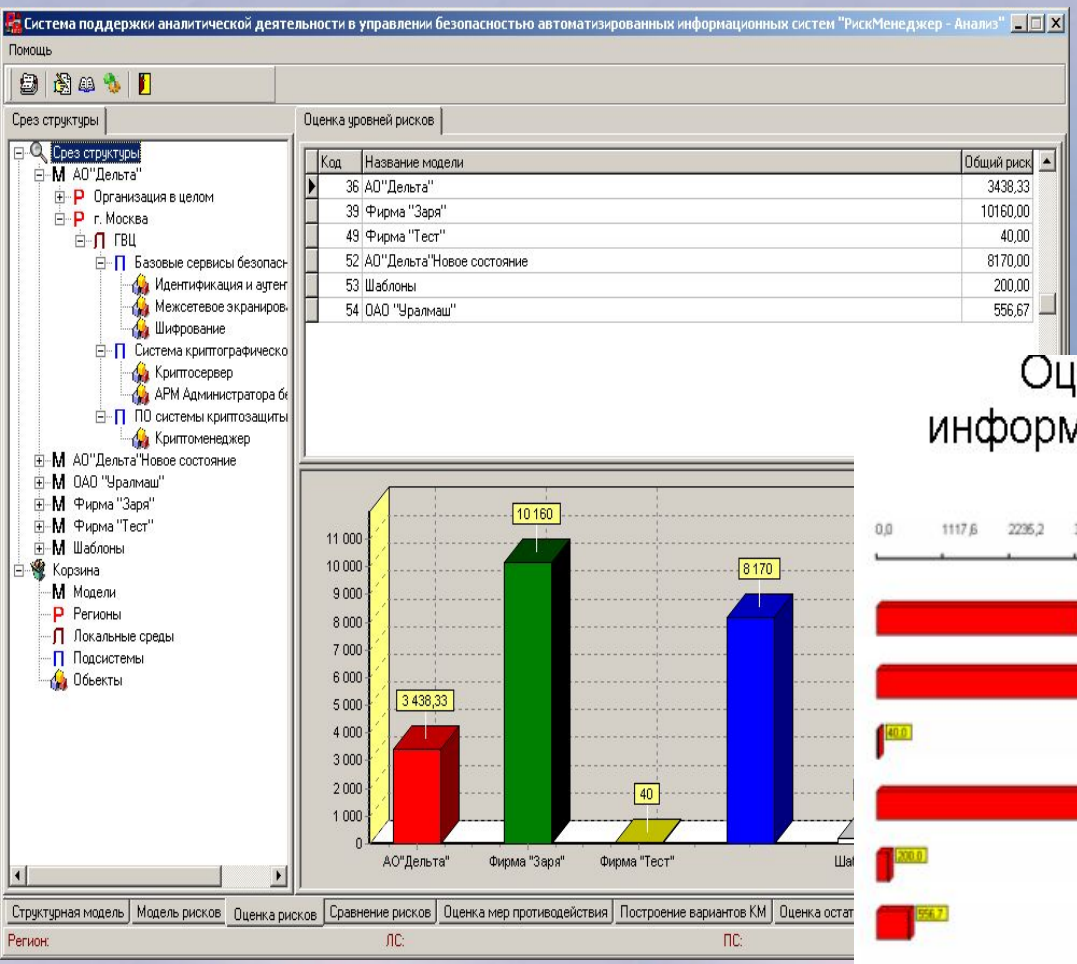


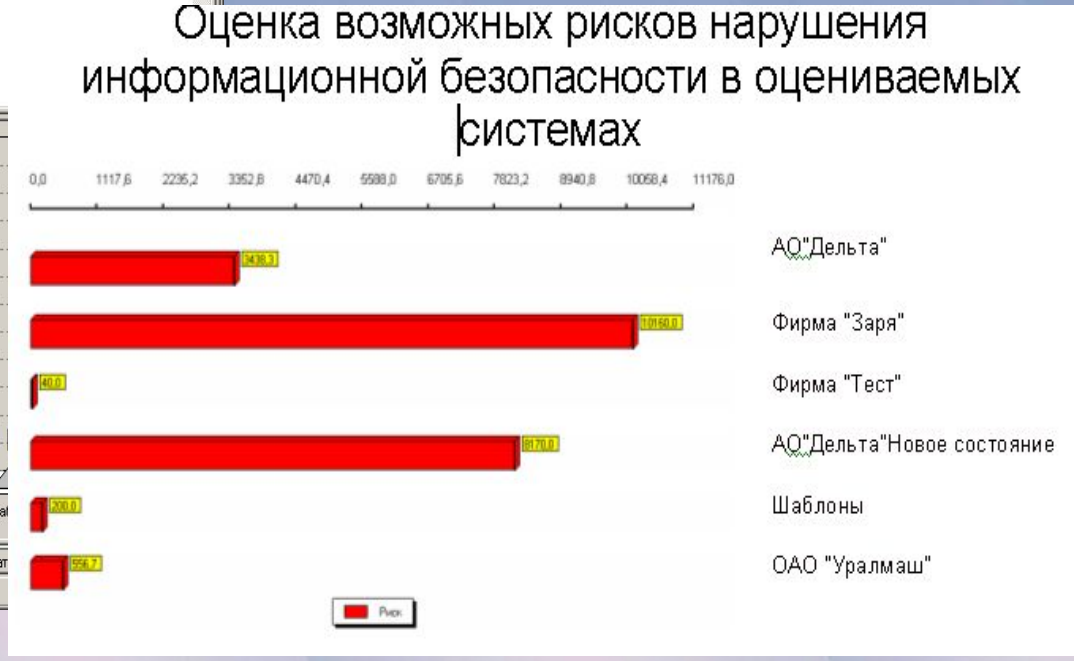


- В распределенном методе дельфийских групп экспертам рассылаются формы с оценками, которые они могут комментировать и править и их ответы принимаются и сохраняются также в электронном виде. В результате формируются некоторые консолидированные оценки с их обоснованиями.

Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

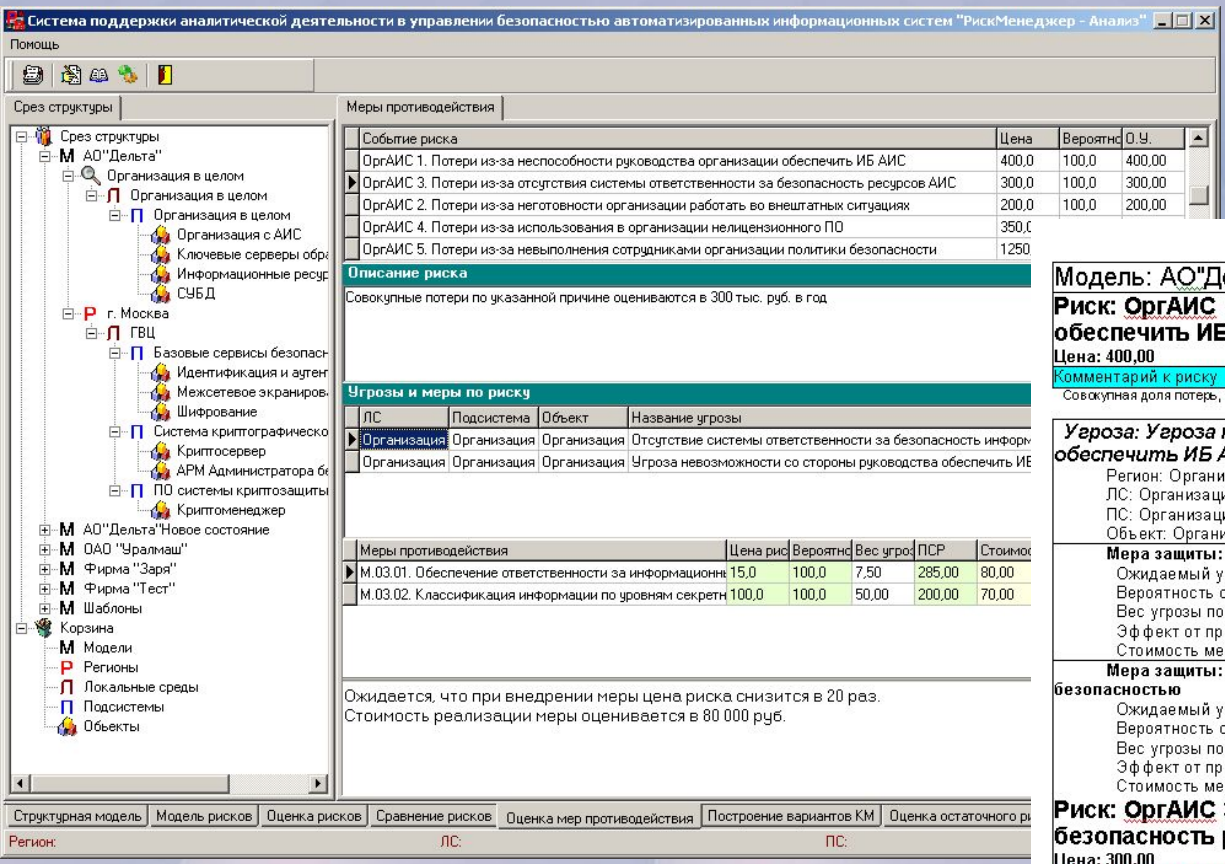
11. Оценка рисков нарушения безопасности из-за некорректности принятой к исполнению критериальной базы





Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

12. Строить модели воздействия мер защиты и обосновывать значимость недостающих критериев (требований).



Модели событий рисков

Модель: АО"Дельта"

Риск: ОргАИС 1. Потери из-за неспособности руководства организации обеспечить ИБ АИС

Цена: 400,00 **Вероятность: 100,00** **Ожидаемый ущерб: 400,00**

Комментарий к риску

Совокупная доля потерь, которая может быть отнесена на указанную причину оценивается в 400 тыс. руб. в год.

Угроза: Угроза невозможности со стороны руководства обеспечить ИБ АИС ***Вес: 400,00***

Регион: Организация в целом
ЛС: Организация в целом
ПС: Организация в целом
Объект: Организация с АИС

Мера защиты: М.01.01. Разработка, внедрение и поддержка политики безопасности

Ожидаемый ущерб после принятия мер:	**100,00**
Вероятность события риска после принятия мер:	**100,00**
Вес угрозы после принятия мер:	**100,00**
Эффект от принятия мер:	**300,00**
Стоимость мер:	**200,00**

Мера защиты: М.02.01 Создание инфраструктуры управления информационной безопасностью

Ожидаемый ущерб после принятия мер:	**100,00**
Вероятность события риска после принятия мер:	**100,00**
Вес угрозы после принятия мер:	**100,00**
Эффект от принятия мер:	**300,00**
Стоимость мер:	**150,00**

Риск: ОргАИС 3. Потери из-за отсутствия системы ответственности за безопасность ресурсов АИС

Цена: 300,00 **Вероятность: 100,00** **Ожидаемый ущерб: 300,00**

Комментарий к риску

Совокупные потери по указанной причине оцениваются в 300 тыс. руб. в год

Угроза: Отсутствие системы ответственности за безопасность информационных ресурсов ***Вес: 150,00***

Регион: Организация в целом
ЛС: Организация в целом
ПС: Организация в целом

Благодарю за внимание!

www.OcenkaRiskov.tk

Телефон для справок:
(499) 135-50-43