

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

Виды деятельности/	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
Нарушаемые акты								
1. Нарушения нормативных актов, принимаемых законодательными органами власти	3 (2)	14 (12)	4 (4)	-	1	-	3 (2)	24 (20)
2. Нарушения нормативных актов, принимаемых федеральными органами исполнительной 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, избыточности, а так же при оценке выполнения критериев в задачах контроля.**

Критерии определения безопасности компьютерных систем

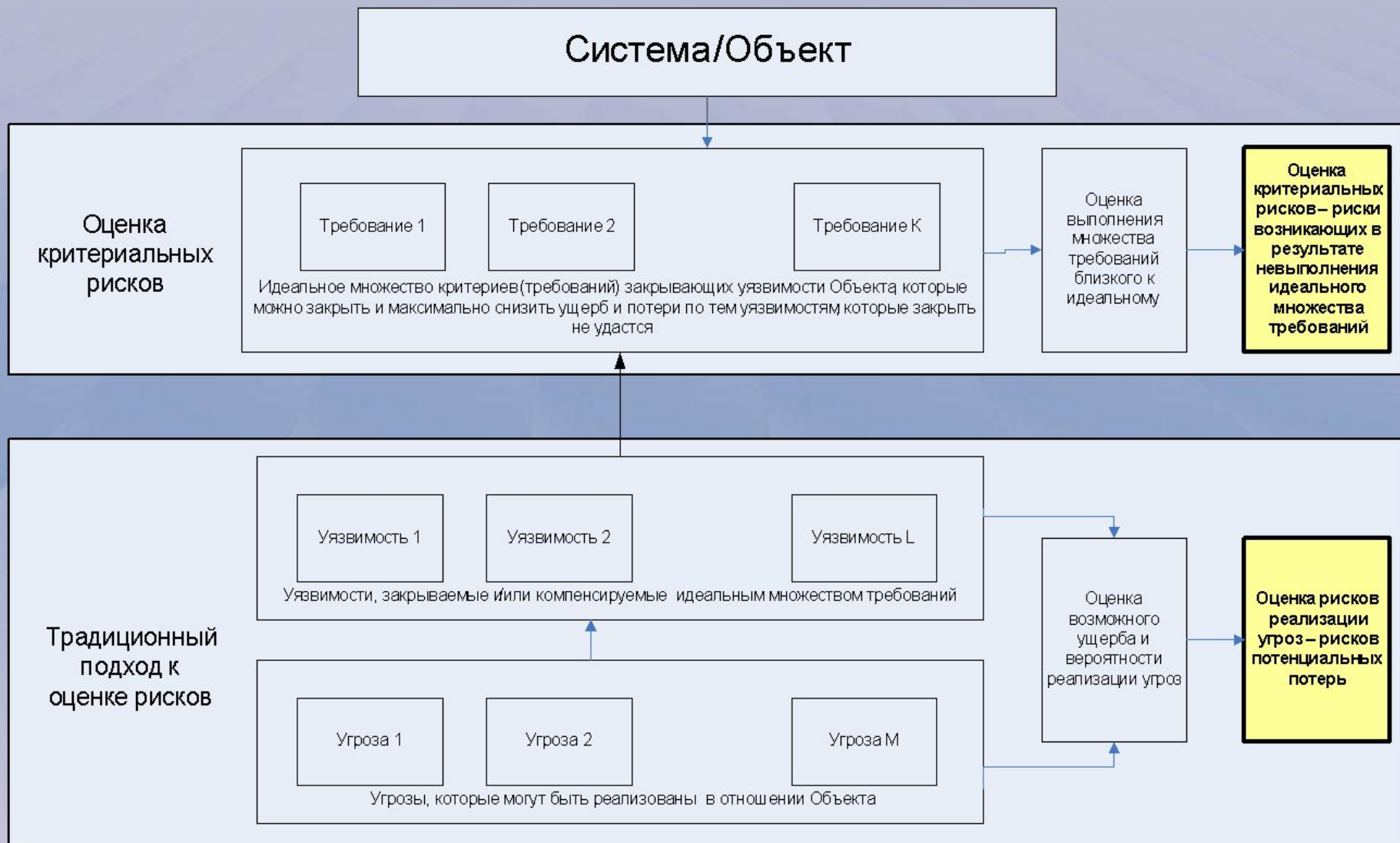
- **Критерии определения безопасности компьютерных систем** ([англ. Trusted Computer System Evaluation Criteria](#)) — стандарт [Министерства обороны](#) — стандарт Министерства обороны [США](#), устанавливающий основные условия для оценки эффективности средств компьютерной безопасности, содержащихся 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 определяются ли 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 контролируруемыми 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 — [идентификация](#); FIA — 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 оценке 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:

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

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:

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

Аксиоматика оценки критериальных рисков безопасности компьютеризированных систем (4)

- Далее предположим, что с каждым требованием связан такой интегральный показатель, как вес требования 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:

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

Аксиоматика оценки критериальных рисков безопасности компьютеризированных систем (5)

- Будем называть значимостью требования величину рассчитываемую по формуле:

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

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

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

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:

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

Аксиоматика оценки критериальных рисков безопасности компьютеризированных систем

(7)

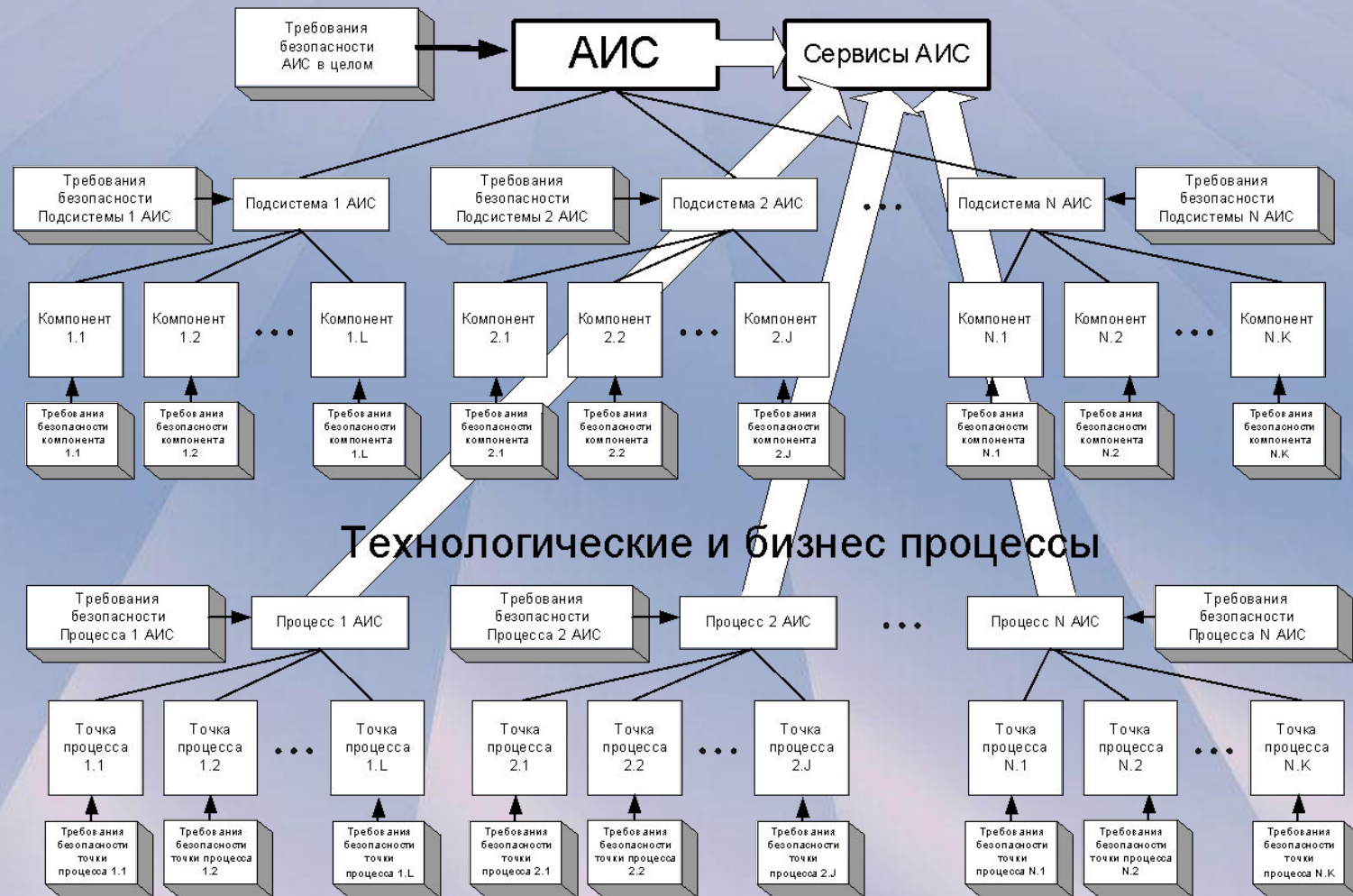
Если по объектам были определены значимости задающие степень влияния оценок рисков по составляющим на степень риска по системе в целом, то формула (6) должна принять следующий вид:

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

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.

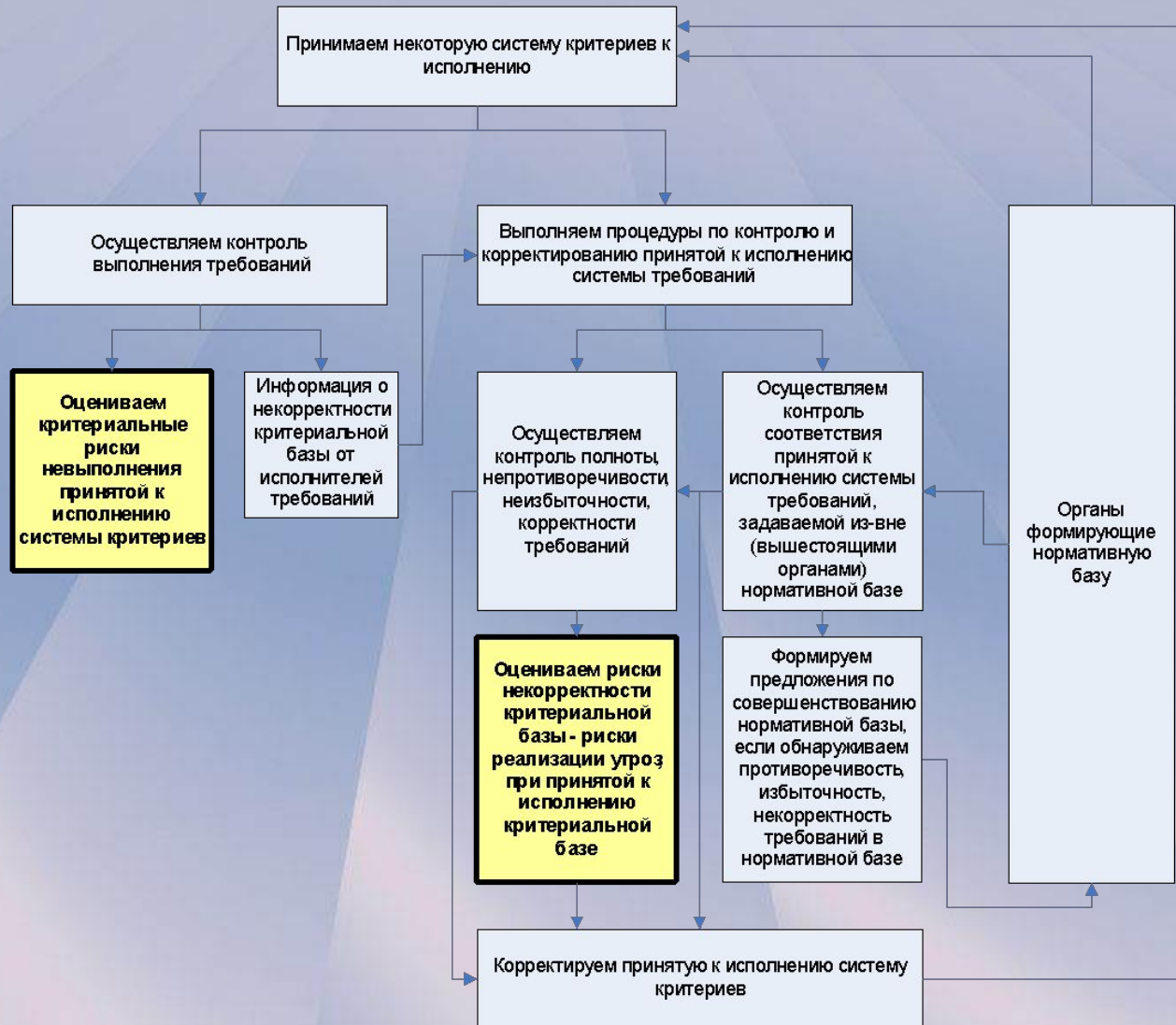
Распределение требований безопасности по структурным составляющим, технологическим и бизнес процессам АИС



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)

The screenshot shows the 'Система автоматизированного анализа рисков невыполненных требований информационной безопасности электронных платежных технологий в регион...' interface. The main window displays a tree structure under 'Профиль защиты ОС' with various security profiles like 'ПЗ ОС. A.ADMIN', 'ПЗ ОС. A.PHYSICAL', etc. The bottom pane shows a detailed view of a requirement: 'FAU_SAA.3.1 КСБ должен быть способен сопровождать внутреннее представление заданных характерных событий следующих характерных событий [назначение: подмножество событий системы], которые могут указывать на нарушение ПБ ОО.'

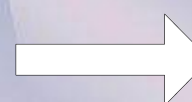
The diagram illustrates a 'Профиль защиты ОС' (OS Protection Profile) for a 'Защищенный анклав' (Protected Enclave). It shows a 'Целевой пользователь' (Target User) interacting with a 'ТСОП' (Telephony Network of the General User) and various services like 'Сервис печати', 'Сервис сканирования', and 'Конверсионный сервис'. The enclave is protected by 'Механизмы защиты' (Protection Mechanisms).

Профиль защиты
 Класс: Профиль защиты ОС

Описание объекта оценки
 Профиль защиты определяет требования для многопользовательских операционных систем общего назначения. Такие системы обычно содержат файловые системы, сервисы печати, сетевые сервисы, сервисы архивации данных и другие приложения, обеспечиваемые хостом (например, почта, базы данных). Операционные системы, удовлетворяющие этим требованиям, могут функционировать в защищенном анклаве (как показано на рисунке 2.1), который обычно используется для того, чтобы поддерживать связь с недовверенными, но управляемыми сетями. Такой анклав будет состоять из клиентов и серверов с многоиспользуемыми приложениями, доступными пользователям. В этой среде операционные системы могут быть доступны внешним системам ИТ, которые находятся вне политики безопасности анклава. Соответственно и пользователи этих систем ИТ находятся за пределами управления политикой безопасности операционной системы. Хотя пользователи этих внешних систем могут быть в какой-то степени доверенными, они находятся вне области управления этим конкретным анклавом, и так как никто не может предполагать об их намерениях, то они не должны рассматриваться как доверенные пользователи.

Рис. 2.1 Защищенный анклав
 Доступ ко всем данным и ресурсам, защищаемым ОО, управляется на основе идентификатора. Для всех пользователей назначены уникальные идентификаторы. Все пользователи должны быть идентифицированы и аутентифицированы до того, как ими будет получен доступ к любым управляемым ресурсам.

Требования: ПЗ ОС. P.NEED_TO_KNOW Система должна ограничивать доступ к ресурсам в соответствии с ССП.
P.NEED_TO_KNOW Система должна ограничивать доступ к ресурсам в соответствии со служебными обязанностями пользователей(СОП).
 Требование: ПЗ ОС. P.REMOTE_ADMIN_ACCESS YA для управления ОС могут получать доступ к своим рабочим станциям дистанционно.
P.REMOTE_ADMIN_ACCESS Уполномоченные администраторы (YA) для управления операционной системой (ОС) могут получать доступ к своим рабочим станциям дистанционно.
 Требование: ПЗ ОС. P.ROLES YA и ОП должны иметь отдельные и различные роли, соответствующие своим функциям.



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

2. Построение структурной модели оцениваемой системы

The screenshot shows the 'РискАналитик' application window. The left sidebar displays a tree view of the organizational structure under 'г.Москва' and 'Расчетный центр'. The main area shows a hierarchical tree of 'Классы типовой организации с АИС оцениваемой по ISO 17799'. Below the tree, there are two tables: 'Меры защиты' and 'Требования'.

Название меры	Вес	Значимость
М.06.06. Оперирование носителями информации и их защита	80,00	19,51
М.08.03. Защита файлов прикладных систем	100,00	24,39
М.08.02. Безопасность в прикладных системах	60,00	14,63
М.03.01. Обеспечение ответственности за информационные ресурсы	100,00	24,39
М.03.02. Классификация информации по уровням конфиденциальности	70,00	17,07

Название требование	Вес	Значимость
Т.08.02.01. Должна осуществляться проверка достоверности входных данных	90,00	26,47
Т.08.02.02. Должна осуществляться проверка достоверности внутренней обработки данных	80,00	23,53
Т.08.02.03. Должно обеспечиваться шифрование данных сертифицированными средствами	100,00	29,41
Т.08.02.04. Должна проводиться аутентификация сообщений	70,00	20,59

The screenshot shows the same application window but with a table of risk assessments and a detailed view of a specific requirement.

Класс объекта	Наименование оцениваемого объекта (ОО)	Кол-во	Риск	Дост.	Конф.	Цел.	Вес	Знач.
М	ВБ-Центр	1	17,20	6,23	7,76	3,21	100,00	16,67
	Автоматизированная система	1	20,00	6,67	6,67	6,67	100,00	16,67
	Места доступа ст Места доступа сторонних организаций	1	37,80	5,90	21,65	10,25	100,00	16,67
	Ресурсы АИС Ресурсы АИС	1	20,56	6,85	6,85	6,85	100,00	16,67
	АРМ АРМ	1	10,00	1,94	6,11	1,94	100,00	16,67

Название меры защиты	% вып.	Риск	Знач.	ПСР	Стоимость
М.07.05. Управление доступом к компьютерам	85,71	14,29	9,09	1,30	0,00
М.06.06. Оперирование носителями информации и их защита	50,00	50,00	9,09	4,55	0,00
М.06.01. Обеспечить безопасное выполнение операционных процедур и обязан	89,60	11,40	9,09	1,04	0,00
М.06.02. Планирование развития АИС и приемы новых систем с целью сведени	91,75	8,25	9,09	0,75	0,00
М.06.03. Защита от вредоносного программного обеспечения	100,00	0,00	9,09	0,00	0,00
М.06.04. Обслуживание систем	74,75	25,25	9,09	2,30	0,00

Название требования	% вып.	Риск	Знач.	ПСР	Д	К	Ц
Т.07.05.01. Должна обеспечиваться автоматическая идентификация терминалов	0,00	100,00	14,29	14,29	V	V	
Т.07.05.02. Допуск к информационным сервисам следует осуществлять с помоч	100,00	0,00	14,29	0,00	V	V	
Т.07.05.03. Всем пользователям необходимо присвоить уникальные персональн	100,00	0,00	14,29	0,00	V	V	
Т.07.05.04. Для аутентификации пользователей необходимо использовать эффе	100,00	0,00	14,29	0,00	V	V	
Т.07.05.05. Должна быть рассмотрена возможность использования сигнала тре	100,00	0,00	14,29	0,00	V	V	

Т.07.05.01. Должна обеспечиваться автоматическая идентификация терминалов

Для аутентификации подключений к конкретным узлам сети следует рассмотреть возможность автоматической идентификации терминалов. Автоматическая идентификация терминалов - это

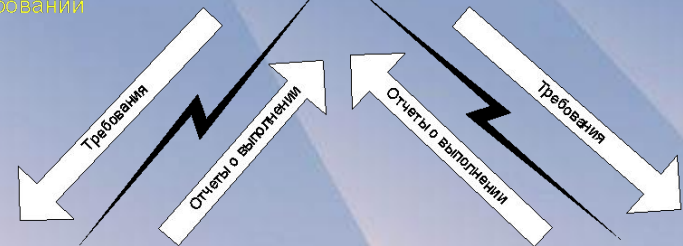
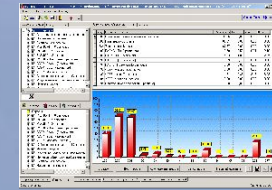
Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

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

Система автоматизации контроля рисков
«РискДетектор-Контроль»

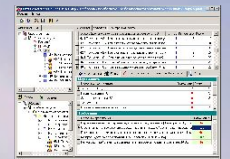
ПК «РискДетектор»

Программный комплекс ведения систем требований, их распределения, рассылки, оценки рисков невыполнения требований



ПК «РискДетектор-Инспектор»

Программный комплекс доведения требований, сбора, и подготовки отчетности о выполнении требований



ПК «РискДетектор-Инспектор»

Принципиальные задачи управления критерияльными 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

The screenshot shows the 'РискДетектор' software interface. The main window displays a risk assessment table with columns for 'Класс объекта', 'Наименование оцениваемого объекта (ОО)', 'Кол-во', 'Выполнено', and 'Всего'. Below this, there are sections for 'Меры защиты' (Security Measures) and 'Требования' (Requirements), each with a table showing their status and completion percentage.

Класс объекта	Наименование оцениваемого объекта (ОО)	Кол-во	Выполнено	Всего
H1.1.	Точка при N1.1.Точка приема начальных платежных докум	1	13	25
H1.2.	Точка пер N1.2.Точка первичного ввода реквизитов начал	1	11	31
H1.3.	Точка кон N1.3.Точка контроля ввода реквизитов начал	1	5	33
H1.4.	Точка отп N1.4.Точка отправки начальных платежных доку	1	15	27
H2.1.	Точка при N2.1.Точка приема начальных платежных докум	1	5	10
H2.2.	Точка пер N2.2.Точка первичного ввода реквизитов начал	1	9	31

Название меры защиты	Выполнено	Всего
Защита от НСД	2	5
Меры по защите ПО	2	5
Защита помещений (2)	1	2
Защита СВТ	1	1
Организационные меры защиты-7	2	7
Технологические меры защиты при приеме нач. пл. док-тов в служеб	5	5

Название требования	Выполнение	% вып. треб
Пароль не менее 8-ми буквенно-цифровых и спец. символов (Врем.т	Да	100,00
Ограничение на число попыток ввода пароля (Внутр.док. "Организ	Да	100,00
Применение сертифицированных средств не ниже 4-го класса (Указ	Нет	0,00
Контроль доступа пользователя (Врем.треб.№60, Прилож.№4)	Нет	0,00
Регистрация действий пользователя в электронном журнале (Врем	Нет	0,00

ОУБ-Центр Форма РИСК-03П

Выполнение требований безопасности

ВБ- Центр	Выполнение	% вып.п.	ПСР
г.Москва			
Расчетный центр			
АИС			
Автоматизированная система			
Мера защиты: М.07.05. Управление доступом к компьютерам	Нет	85,71	1,30
Требования по защите:			
T.07.05.01. Должна обеспечиваться автоматическая идентификация терминалов	Нет	0,00	
T.07.05.02. Допуск к информационным сервисам следует осуществлять с помощью надежной процедуры входа в системы	Да	100,00	
T.07.05.03. Всем пользователям необходимо присвоить уникальные персональные идентификаторы	Да	100,00	
T.07.05.04. Для аутентификации пользователей необходимо использовать эффективную систему управления паролями	Да	100,00	
T.07.05.05. Должна быть рассмотрена возможность использования сигнала тревоги, предупреждающего о принуждении терминалов, после которого сеансы связи должны закрываться	Да	100,00	
T.07.05.07. Должно обеспечиваться ограничение времени подключения	Да	100,00	
Мера защиты: М.06.06. Стерилизация носителей информации и их защита	Нет	50,00	4,55
Требования по защите:			
T.06.06.01. Должна обеспечиваться безопасность информации на съемных компьютерных носителях	Да	100,00	
T.06.06.02. Должна быть обеспечена защита конфиденциальности данных во всех операциях с ними	Нет	0,00	
T.06.06.03. Должна быть обеспечена защита системной документации, содержащей конфиденциальную информацию	Да	100,00	
T.06.06.04. Должны быть внедрены надежные и проверенные процедуры уничтожения носителей информации	Нет	0,00	
Мера защиты: М.06.01. Обеспечение безопасности выполнения операционных процедур и обязанностей	Нет	88,50	1,04
Требования по защите:			
T.06.01.01. Должны существовать документированные процедуры обеспечения корректной и надежной работы АИС	Да	100,00	
T.06.01.02. Необходимо определить управленческие обязанности и процедуры реагирования на события угрожающие ИБ	Нет	65,00	
T.06.01.03. Должно быть обеспечено разделение обязанностей, снижающее риски НСД и нежелательного использования АИС	Да	100,00	
T.06.01.04. Должно быть обеспечено разделение программных средств разработки и рабочих программ	Нет	78,00	
T.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 привлечение новых ресурсов. Создание резерва ИТ-специалистов	Нет	91,75	0,75

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

5. Оценка критериальных рисков – рисков невыполнения требований

Скриншот интерфейса системы «РискДетектор» (рис. 1). В центре экрана отображена таблица с данными по объектам оценки. В левом меню видна структура объектов, включающая «Базовые сервисы безопасности» и «Идентификация и аутентификация». В нижней части экрана выделено требование T.07.05.01.

Класс объекта	Наименование оцениваемого объекта (OO)	Кол-во	Риск	Дост.	Конф.	Цел.	Вес	Знач.
Автоматизированная система	Автоматизированная система	1	17,20	6,23	7,76	3,21	100,00	16,67
Места доступа ст	Места доступа сторонних организаций	1	20,00	6,67	6,67	6,67	100,00	16,67
Ресурсы АИС	Ресурсы АИС	1	37,80	5,90	21,65	10,25	100,00	16,67
АРМ	АРМ	1	20,56	6,85	6,85	6,85	100,00	16,67
Критически важн	Критически важные сервисы/приложения организ	1	10,00	1,94	6,11	1,94	100,00	16,67

Название меры защиты	% вып.	Риск	Знач.	ПСР	Стоимость
M.07.05. Управление доступом к компьютерам	85,71	14,29	9,09	1,30	0,00
M.06.06. Оперирование носителями информации и их защита	50,00	50,00	9,09	4,55	0,00
M.06.01. Обеспечить безопасное выполнение операционных процедур и обязан	88,60	11,40	9,09	1,04	0,00
M.06.02. Планирование развития АИС и приемки новых систем с целью сведени	91,75	8,25	9,09	0,75	0,00
M.06.03. Защита от вредоносного программного обеспечения	100,00	0,00	9,09	0,00	0,00
M.06.04. Обслуживание систем	74,75	25,25	9,09	2,30	0,00

Название требования	% вып.	Риск	Знач.	ПСР	Д	К	Ц
T.07.05.01. Должна обеспечиваться автоматическая идентификация терминалов	0,00	100,00	14,29	14,29	V	V	V
T.07.05.02. Допуск к информационным сервисам следует осуществлять с помо	100,00	0,00	14,29	0,00	V	V	V
T.07.05.03. Всем пользователям необходимо присвоить уникальные персональн	100,00	0,00	14,29	0,00	V	V	V
T.07.05.04. Для аутентификации пользователей необходимо использовать эффе	100,00	0,00	14,29	0,00	V	V	V
T.07.05.05. Должна быть рассмотрена возможность использования сигнала тре	100,00	0,00	14,29	0,00	V	V	V

T.07.05.01. Должна обеспечиваться автоматическая идентификация терминалов
 Для аутентификации подключений к конкретным узлам сети следует рассмотреть возможность автоматической идентификации терминалов. Автоматическая идентификация терминалов - это

Скриншот интерфейса системы «РискДетектор» (рис. 2). В центре экрана отображена таблица с данными по объектам оценки. В левом меню видна структура объектов, включающая «Базовые сервисы безопасности» и «Идентификация и аутентификация». В нижней части экрана выделено требование T.07.05.01. В правой части экрана отображен график, иллюстрирующий уровни рисков по различным критериям.

Код	Объект	Наим	В целом	Дост.	Конф.	Цел.
255	Межсетевой экран - Профиль защ	Межсетевой экран	4,17	0,00	0,00	0,00
138	Идентификация и аутентификация	БСБ Общие требо	40,81	0,00	0,00	0,00
139	Управление доступом	БСБ Общие требо	10,92	0,00	0,00	0,00
140	Протоколирование и аудит	БСБ Общие требо	35,75	0,00	0,00	0,00
141	Шифрование	БСБ Общие требо	40,06	0,00	0,00	0,00
142	Контроль целостности	БСБ Общие требо	48,10	0,56	0,00	0,56

Принципиальные задачи управления критериальными рисками, которые позволяет решать система

«РискДетектор»

6. Выявление опасных сочетаний невыполненных требований (ОСНТ)

Оценка безопасности НЕУДОВЛЕТВОРИТЕЛЬНАЯ из-за наличия опасных сочетаний невыполненных требований

Опасные сочетания невыполненных требований

	% вып.
Модель: РА1	
Регион: Зарайская область	
ЛС: РКЦ г. Вильск	
ПС: М2 На бумаге (оперзал без ЗВМ и ввода реквизитов)	
Объект: Н2.1.Точка приема начальных платежных документов в операционном зале	
без применения ЗВМ, без ввода реквизитов	
ОСНТ: Отсутствие подсистемы охранной сигнализации	
Мера: Технологические меры защиты при приеме нач. пл. документов в учетно-операционном узле (без применения ЗВМ)	
Требование: Наличие подсистемы охранной сигнализации (пункт 9.1. ВНП)	0,00
ОСНТ: Бесконтрольность доступа в помещения	
Мера: Технологические меры защиты при приеме нач. пл. документов в учетно-операционном узле (без применения ЗВМ)	
Требование: Наличие списка лиц, допущенных в помещение	0,00
ЛС: РКЦ г. Вода	
ПС: М2 На бумаге (оперзал без ЗВМ и ввода реквизитов)	
Объект: Н2.1.Точка приема начальных платежных документов в операционном зале	
без применения ЗВМ, без ввода реквизитов	
ОСНТ: Отсутствие подсистемы охранной сигнализации	
Мера: Технологические меры защиты при приеме нач. пл. документов в учетно-операционном узле (без применения ЗВМ)	
Требование: Наличие подсистемы охранной сигнализации (пункт 9.1. ВНП)	0,00
ОСНТ: Бесконтрольность доступа в помещения	
Мера: Технологические меры защиты при приеме нач. пл. документов в учетно-операционном узле (без применения ЗВМ)	
Требование: Наличие списка лиц, допущенных в помещение	0,00
ЛС: РКЦ п. Ночь	
ПС: М2 На бумаге (оперзал без ЗВМ и ввода реквизитов)	
Объект: Н2.1.Точка приема начальных платежных документов в операционном зале	
без применения ЗВМ, без ввода реквизитов	
ОСНТ: Отсутствие подсистемы охранной сигнализации	
Мера: Защита помещений (1)	
Требование: Наличие подсистемы охранной сигнализации (пункт 9.1. ВНП)	0,00
ОСНТ: Бесконтрольность доступа в помещения	
Мера: Защита помещений (1)	
Требование: Наличие списка лиц, допущенных в помещение	0,00
ЛС: РКЦ пгт. Лозань	
ПС: М2 На бумаге (оперзал без ЗВМ и ввода реквизитов)	
Объект: Н2.1.Точка приема начальных платежных документов в операционном зале	
без применения ЗВМ, без ввода реквизитов	
ОСНТ: Отсутствие подсистемы охранной сигнализации	
Мера: Защита помещений (1)	
Требование: Наличие подсистемы охранной сигнализации (пункт 6.1.)	0,00
ОСНТ: Бесконтрольность доступа в помещения	
Мера: Защита помещений (1)	
Требование: Наличие списка лиц, допущенных в помещение	0,00

Срез структуры

Модель	Регион	Локальная среда	Подсистема	Объект	Опасное сочетание требо
РАБИС-НП (16)	Республика Хака ГРКЦ г. Абакана	М1 На бумаге (оперз	Н1.1.Точка приема нач	Незащищенность ПО	
РАБИС-НП (16)	Республика Хака ГРКЦ г. Абакана	М1 На бумаге (оперз	Н1.1.Точка приема нач	Незащищенность ПО из-	
РАБИС-НП (16)	Республика Хака ГРКЦ г. Абакана	М1 На бумаге (оперз	Н1.1.Точка приема нач	Отсутствие подписей и пе	
РАБИС-НП (16)	Республика Хака ГРКЦ г. Абакана	М1 На бумаге (оперз	Н1.1.Точка приема нач	Отсутствие контроля ком	
РАБИС-НП (16)	Республика Хака РКЦ г. Абаза	М1 На бумаге (оперз	Н1.1.Точка приема нач	Незащищенность ПО	
РАБИС-НП (16)	Республика Хака РКЦ г. Абаза	М1 На бумаге (оперз	Н1.1.Точка приема нач	Отсутствие подписей и пе	
РАБИС-НП (16)	Республика Хака РКЦ г. Абаза	М1 На бумаге (оперз	Н1.1.Точка приема нач	Отсутствие контроля ком	
РАБИС-НП (16)	Республика Хака РКЦ г. Абаза	М6 По каналам связи	Н1.1.Точка приема нач	Незащищенность ПО	
РАБИС-НП (16)	Республика Хака РКЦ г. Абаза	М6 По каналам связи	Н1.1.Точка приема нач	Отсутствие подписей и пе	
РАБИС-НП (16)	Республика Хака РКЦ г. Абаза	М6 По каналам связи	Н1.1.Точка приема нач	Отсутствие контроля ком	
РАБИС-НП (16)	Республика Хака РКЦ с. Аскиз	М1 На бумаге (оперз	Н1.1.Точка приема нач	Незащищенность ПО	
РАБИС-НП (16)	Республика Хака РКЦ с. Аскиз	М1 На бумаге (оперз	Н1.1.Точка приема нач	Отсутствие подписей и пе	
РАБИС-НП (16)	Республика Хака РКЦ с. Аскиз	М1 На бумаге (оперз	Н1.1.Точка приема нач	Отсутствие контроля ком	
РАБИС-НП (16)	Республика Хака РКЦ с. Аскиз	М6 По каналам связи	Н1.1.Точка приема нач	Незащищенность ПО	
РАБИС-НП (16)	Республика Хака РКЦ с. Аскиз	М6 По каналам связи	Н1.1.Точка приема нач	Отсутствие контроля ком	
РАБИС-НП (16)	Республика Хака РКЦ с. Аскиз	М6 По каналам связи	Н1.1.Точка приема нач	Отсутствие подписей и пе	
РАБИС-НП (16)	Республика Хака РКЦ с. Аскиз	М6 По каналам связи	Н1.1.Точка приема нач	Отсутствие контроля ком	

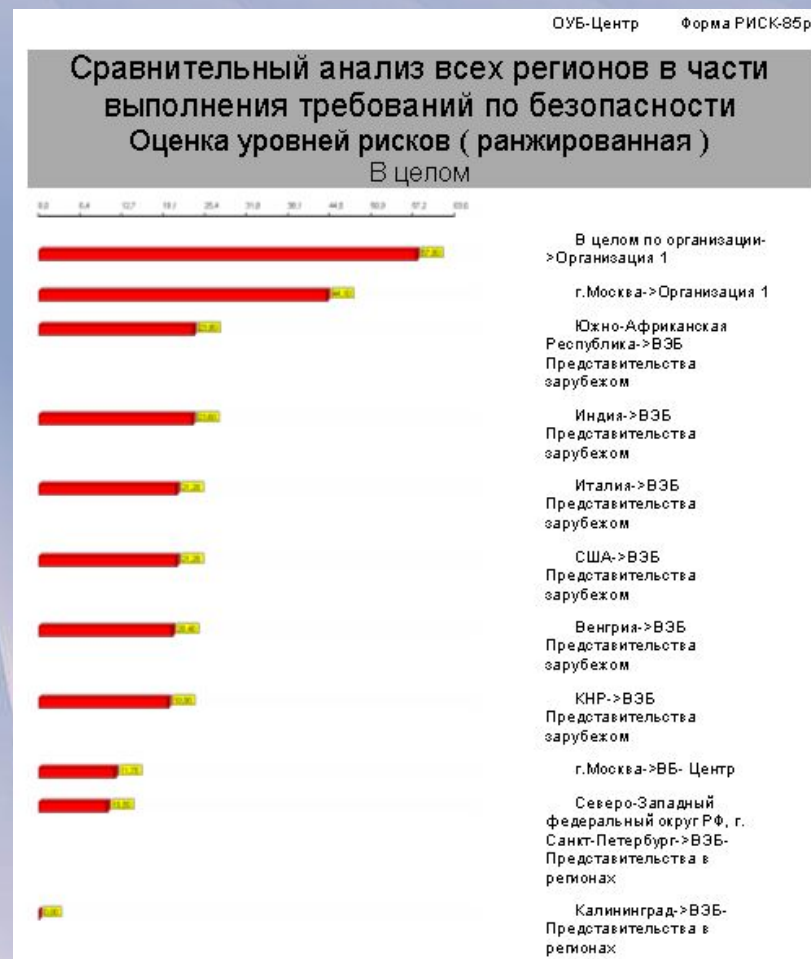
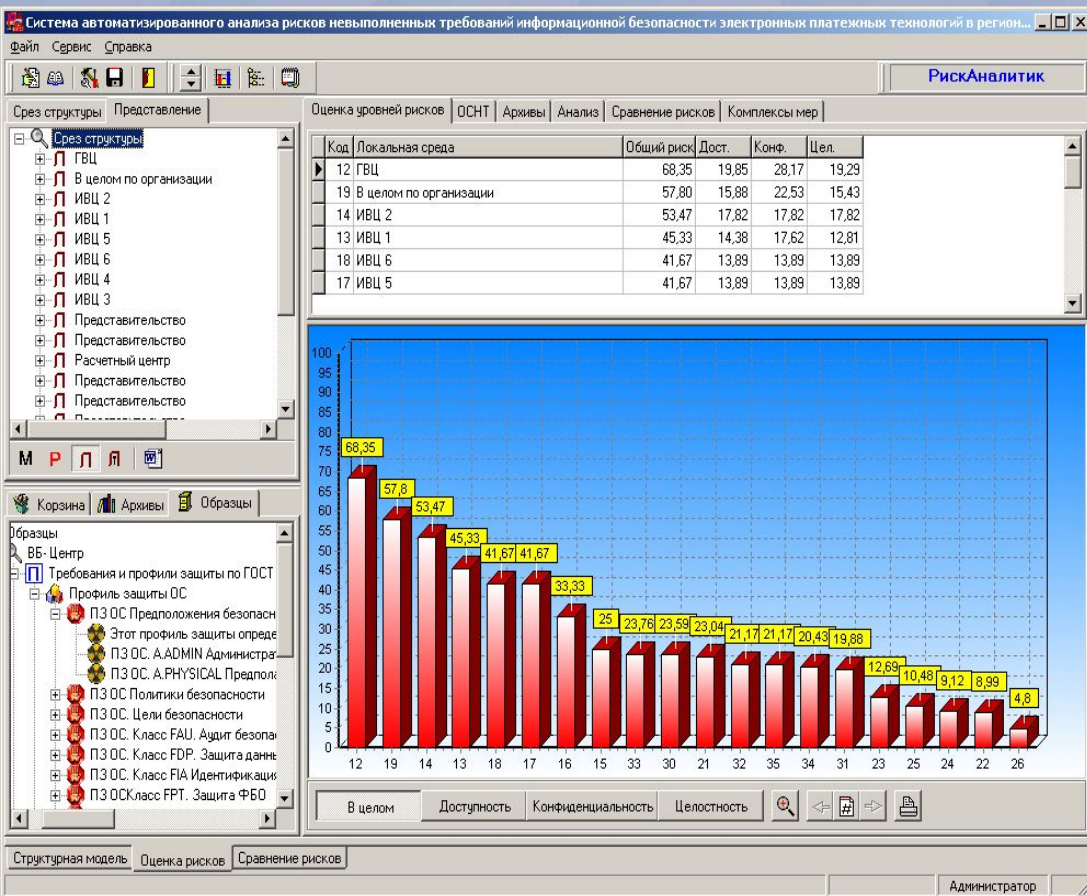
Мера

Мера	Требование
Защита от НСД	Пароль не менее 8-ми буквенно-цифровых и спец. символов (Врем.треб.№60, прил.№4, пункт2)
Защита от НСД	Ограничение на число попыток ввода пароля (Врем.треб.№60, пункт 2.3)
Меры по защите ПО	Контроль целостности ПО (Врем.треб.№60, пункт 3.2)

Структурная модель | Оценка рисков | Сравнение рисков | Построение вариантов КМ | Оценка остаточного риска по КМ

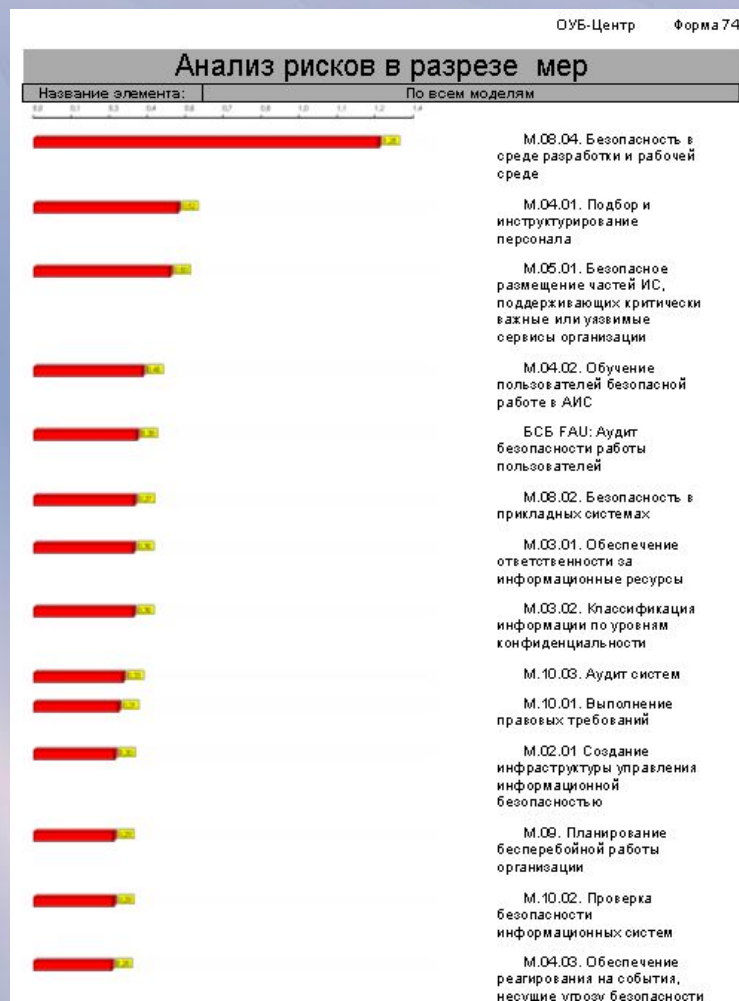
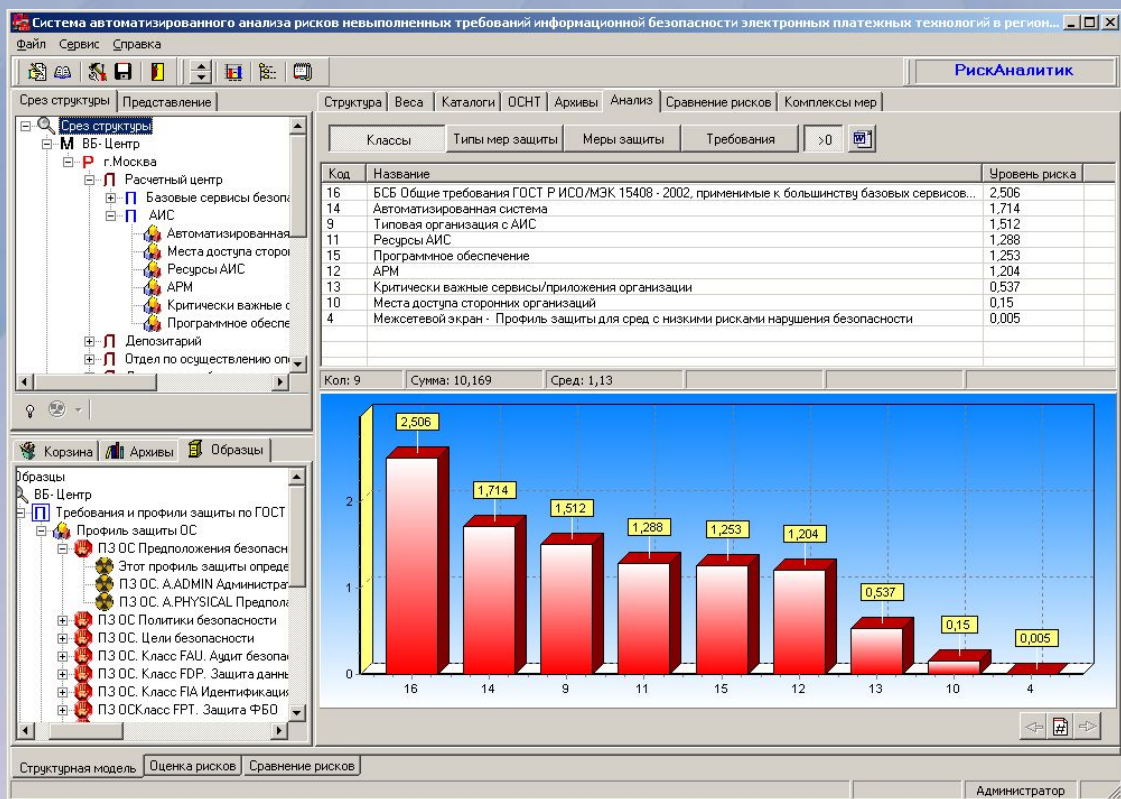
Принципиальные задачи управления критериальными рисками, которые позволяет решать система «РискДетектор»

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 принятой к исполнению критериальной базы

Система поддержки аналитической деятельности в управлении безопасностью автоматизированных информационных систем "РискМенеджер"

Помощь

Срез структуры

Структура

Класс объекта | Наименование оцениваемого объекта (ОО)

Организация и Организация с АИС
 Базовый сервис: Идентификация и аутентификация
 Базовый сервис: Межсетевое экранирование
 Базовый сервис: Шифрование
 Криптосервер | Криптосервер

Информация об объекте | Угрозы и меры защиты | Значимые угрозы | Фильтрация каталога

Организация с АИС
 Класс: Организация использующая АИС
 Массив угроз: Угрозы организации использующей АИС
 Угроза: Угроза невозможности со стороны руководства обеспечить ИБ АИС
 Мера: М.01.01. Разработка, внедрение и поддержка политики безопасности
 Требование: Т.01.01.01. Должен быть разработан и принят документ о
 Мера: М.02.01 Создание инфраструктуры управления информационной с
 Угроза: Отсутствие системы ответственности за безопасность информации

Описание элемента

Информация | Информация из СИ

Структурная модель | Модель рисков | Оценка рисков | Сравнение рисков | Оценка мер противодействия | Построение вариантов КМ | Оценка остаточного риска по

Регион: ЛС: ПС:

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 внетрадных ситуациях Использование нелегального 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 Несанкционированный вход в систему с осуществлением НСД к устройствам системы, программам и ИР на МН	
ГТК_1.1.1	Анонимный вход/выход из системы или анонимный запуск и прекращение ее работы.
ГТК_2.1.1	Хищение носителей информации
ГТК_2.2	Встраивание в ПО средств позволяющих обойти или модифицировать систему защиты информации
ГТК_4.1	НСД к ОО посторонних лиц
ГТК_4.2	Неявная модификация СЗИ НСД, таким образом, что СЗИ НСД перестают выполнять свои функции в полном объеме.
ГТК_4.4	Выход из строя ПО СЗИ НСД
ГТК_4.5	
Объект: Информационные ресурсы организации	
Угрозы:	
ИСА_УИР Уничтожение ИР, в результате пожара, террористического акта и т.п. катастрофических событий приводящих к разрушениям	
ПС: СУБД	

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.

Срез структуры | Сценарии рисков | Риски

Наименование риска	Цена	Вероят	Ущерб
ОргАИС 1. Потери из-за неспособности руководства организации обеспечить ИБ АИС	400,0	100,0	400,0
ОргАИС 3. Потери из-за отсутствия системы ответственности за безопасность ресурсов АИС	300,0	100,0	300,0
ОргАИС 2. Потери из-за неготовности организации работать во внешних ситуациях	200,0	100,0	200,0
ОргАИС 4. Потери из-за использования в организации нелегального ПО			

Создание шаблона для построения новой модели риска

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

Корректировка списка угроз модели риска

Объект	Угроза
Организация с АИС	Отсутствие системы ответственности
Организация с АИС	Угроза невозможности со стороны руководства обеспечить ИБ АИС

Объект

Название объекта

Организация с АИС

Идентификация и аутентификация

Межсетевое экранирование

Массив всех идентифицированных угроз объекта

Название угрозы

Угроза невозможности со стороны руководства обеспечить ИБ АИС

Отсутствие системы ответственности за безопасность информационных ресурсов

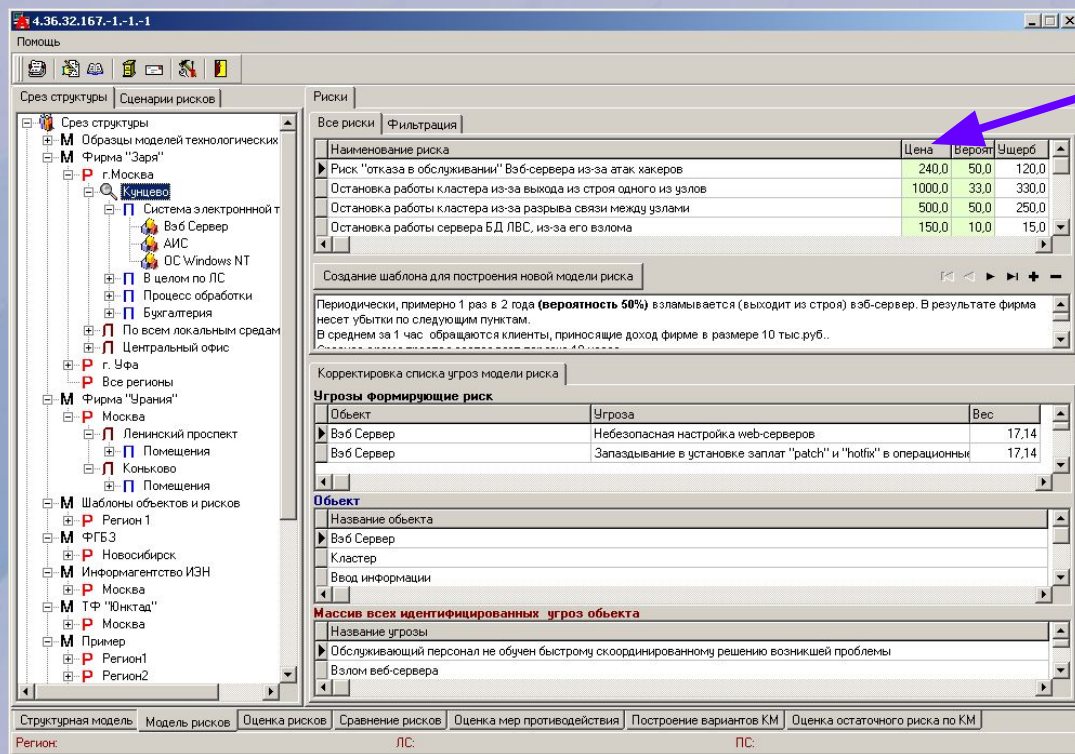
Структурная модель | Модель рисков | Оценка рисков | Сравнение рисков | Оценка мер противодействия | Построение вариантов КМ

Регион: ЛС: ПС:

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
Угроза: Угроза невозможности со стороны руководства обеспечить ИБ АИС		Ожидаемый ущерб: 400,00
		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
Угроза: Отсутствие системы ответственности за безопасность информационных ресурсов		Ожидаемый ущерб: 300,00
		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		Ожидаемый ущерб: 150,00
		Вес: 150,00
Регион: Организация в целом ЛС: Организация в целом ПС: Организация в целом Объект: Организация с АИС		

Оценки цены риска и вероятности события риска



The screenshot shows a software interface for risk assessment. The main window is titled 'Риски' (Risks) and contains a table with the following data:

Наименование риска	Цена	Вероят	Ущерб
Риск "отказа в обслуживании" Вэб-сервера из-за атак хакеров	240,0	50,0	120,0
Остановка работы кластера из-за выхода из строя одного из узлов	1000,0	33,0	330,0
Остановка работы кластера из-за разрыва связи между узлами	500,0	50,0	250,0
Остановка работы сервера БД ЛВС, из-за его взлома	150,0	10,0	15,0

The interface also includes a tree view on the left with categories like 'Срез структуры', 'Сценарии рисков', and 'Риски'. At the bottom, there are tabs for 'Структурная модель', 'Модель рисков', 'Оценка рисков', 'Сравнение рисков', 'Оценка мер противодействия', 'Построение вариантов КМ', and 'Оценка остаточного риска по КМ'.

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 эксперты 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 обоснованиями.

Система поддержки аналитической деятельности в управлении безопасностью автоматизированных информационных систем "РискМенеджер - Анализ"

Срез структуры | Сценарии рисков | Риски

Наименование риска	Цена	Вероят	Ущерб
ОргАИС 1. Потери из-за неспособности руководства организации обеспечить ИБ АИС	400,0	100,0	400,0
ОргАИС 3. Потери из-за отсутствия системы ответственности за безопасность ресурсов АИС	300,0	100,0	300,0
ОргАИС 2. Потери из-за неготовности организации работать во внешних ситуациях	200,0	100,0	200,0
ОргАИС 4. Потери из-за использования в организации нелегального ПО	350,0	10,0	35,0

Создание шаблона для построения новой модели риска

Существует вероятность, в течение ближайших 10 лет у организации могут возникнуть проблемы из-за использования на ряде рабочих мест нелегального ПО. Потери, которая может в результате понести организация оцениваются в 350 тыс. рублей.

MS Sans Serif

Существует вероятность, в течение ближайших 10 лет у организации могут возникнуть проблемы из-за использования на ряде рабочих мест нелегального ПО. Потери, которая может в результате понести организация оцениваются в 350 тыс. рублей.

PK "РискМенеджер" Форма РИСК-21П

Модели рисков

Модель: АО"Дельта"		
Регион: Организация в целом		
ЛС: Организация в целом		
ЛС: Организация в целом		
Риск: ОргАИС 1. Потери из-за неспособности руководства организации обеспечить ИБ АИС		
Цена: 400,00	Вероятность: 100,00	Ожидаемый ущерб: 400,00
Составитель: [имя]		
Угроза: Угроза невозможности со стороны руководства обеспечить ИБ АИС		
Вес: 400,00		
Комментарий к угрозе		

Статистические данные

94% крупных британских корпораций испытали проблемы с информационной безопасностью

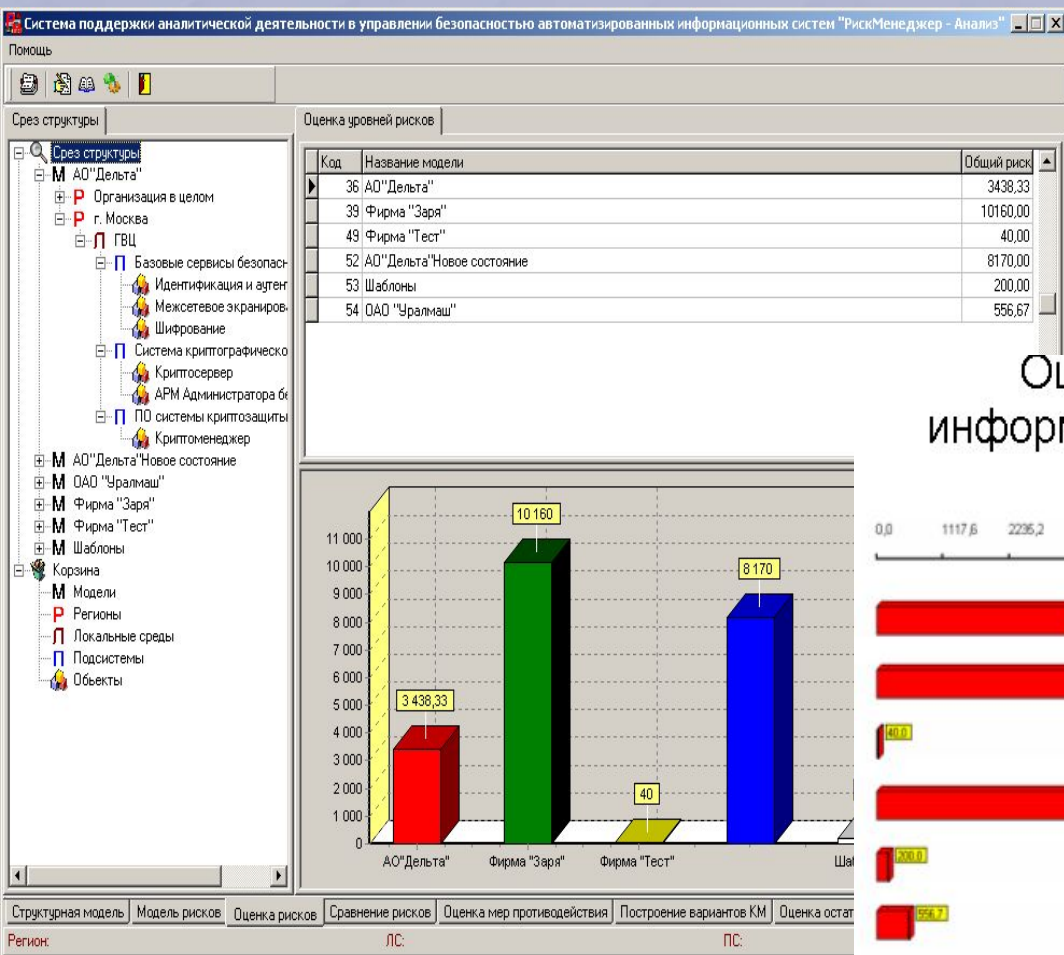
Как показывает исследование, проведенное по заказу правительства Великобритании, за последние 4 года число инцидентов, связанных с информационной безопасностью, в стране утроилось. Причиной этому стали недостаточные меры, предпринимаемые корпорациями, пишет газета [The Inquirer](http://www.theinquirer.net). В ходе исследования была рассмотрена деятельность 1000 британских компаний. 74% из них (94% при этом - крупные корпорации) заявили, что в течение 2003 года хоть раз испытывали проблемы с информационной безопасностью - вирусные атаки, утечку конфиденциальной информации, несанкционированный доступ, мошенничество. Средний убыток, понесенный компаниями в результате подобных проблем составил 110 тыс., причем для крупных компаний сумма убытка была больше - 1120 тыс.

См. также: [Stephen Timmins](#), министр по электоральной политике правительства

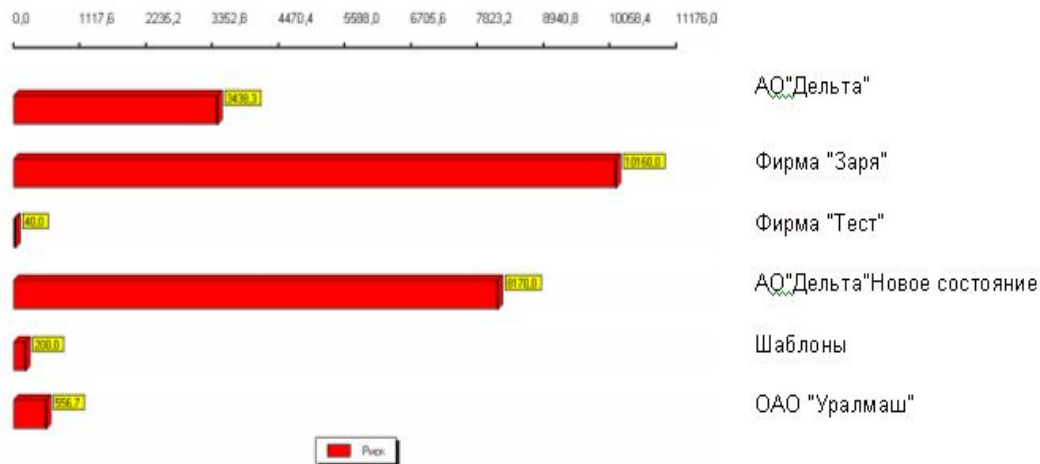
Принципиальные задачи управления критериальными рисками, которые позволяет решать система

«РискДетектор»

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



Оценка возможных рисков нарушения информационной безопасности в оцениваемых системах



Принципиальные задачи управления критериальными рисками, которые позволяет решать система

«РискДетектор»

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

Система поддержки аналитической деятельности в управлении безопасностью автоматизированных информационных систем "РискМенеджер - Анализ"

Помощь

Срез структуры

- Срез структуры
 - М АО "Дельта"
 - Организация в целом
 - Организация в целом
 - Организация с АИС
 - Ключевые серверы обра
 - Информационные ресур
 - СУБД
 - г. Москва
 - ГВЦ
 - Базовые сервисы безопас
 - Идентификация и аутент
 - Межсетевое экранирова
 - Шифрование
 - Система криптографическо
 - Криптосервер
 - АРМ Администратора б
 - ПО системы криптозащиты
 - Криптоменеджер
- М АО "Дельта" Новое состояние
- М ОАО "Уралмаш"
- М Фирма "Заря"
- М Фирма "Тест"
- М Шаблоны
- Корзина
 - М Модели
 - Р Регионы
 - Локальные среды
 - Подсистемы
 - Объекты

Меры противодействия

Событие риска	Цена	Вероятн	О.У.
OrgAIC 1. Потери из-за неспособности руководства организации обеспечить ИБ АИС	400,0	100,0	400,00
OrgAIC 3. Потери из-за отсутствия системы ответственности за безопасность ресурсов АИС	300,0	100,0	300,00
OrgAIC 2. Потери из-за неготовности организации работать во внешних ситуациях	200,0	100,0	200,00
OrgAIC 4. Потери из-за использования в организации нелегального ПО	350,0		
OrgAIC 5. Потери из-за невыполнения сотрудниками организации политики безопасности	1250		

Описание риска

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

Угрозы и меры по риску

ЛС	Подсистема	Объект	Название угрозы
Организация	Организация	Организация	Отсутствие системы ответственности за безопасность информ
Организация	Организация	Организация	Угроза невозможности со стороны руководства обеспечить ИБ

Меры противодействия	Цена риск	Вероятн	Вес угроз	ПСР	Стоимос
M.03.01. Обеспечение ответственности за информационн	15,0	100,0	7,50	285,00	80,00
M.03.02. Классификация информации по уровням секретн	100,0	100,0	50,00	200,00	70,00

Ожидается, что при внедрении меры цена риска снизится в 20 раз.
Стоимость реализации меры оценивается в 80 000 руб.

Структурная модель | Модель рисков | Оценка рисков | Сравнение рисков | Оценка мер противодействия | Построение вариантов КМ | Оценка остаточного р

Регион: ЛС. ПС.

Модели событий рисков

Модель: АО "Дельта"

Риск: OrgAIC 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 указанное событие, 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: M.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: M.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: OrgAIC 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