МОНАХОВ М.Ю., д.т.н.,проф. кафедры ИЗИ

АСТАФЬЕВА Е.С., студентка группы КЗИ-108

ИССЛЕДОВАНИЕ ВХОДНЫХ ДАННЫХ И МЕТОДОВ ИХ ВИЗУАЛЬНОГО ПРЕДСТАВЛЕНИЯ В СИСТЕМЕ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Цель данной работы заключается в исследование и составлении списка первоочередных входных данных, которые необходимы администратору безопасности предприятиям для выработки решений по обеспечению защиты информационной системы. Также исследованы всевозможные комбинации методов наглядного представления этих входных данных, которые представлены в продуктах российских и зарубежных компаний.

Управление информационной безопасностью заключается в планировании, развертывании и поддержании комплекса регламентов и процедур, направленных на минимизацию рисков, устранению и предотвращению угроз нарушения информационной безопасности. Процесс управления с точки зрения действий службы информационной безопасности предприятия может быть условно разбит на два этапа - восприятие входных данных, характеризующих состояние системы на текущий период времени, и формулировка решений на базе использования интеллектуальных средств поддержки. Качество первого этапа определяется качеством предъявляемой информации, а качество (обоснованность) решения определяется возможностями средств интеллектуальной поддержки. Качество предъявляемой информации во многом зависит от того, в каком объеме администратор сможет воспринимать и анализировать данные и насколько понятно и наглядно они будут ему представлены. Собственно, именно в этом случае проблема визуализации стоит очень остро.

Можно выделить основные критерии визуализации входных данных о состоянии информационной безопасности:

- Данные необходимо представлять самыми разными способами в зависимости от их типа и структуры (не ограничиваться использованием таблиц, списков и простых графиков);

- Если это возможно, то большой массив однородных данных представлять в виде одной наглядной статистической картины;
- Использовать яркую палитру цветов при отображении, в особенности при выявлении угроз, атак и т.д., чтобы акцентировать внимание на самом главном;
- Информация должна быть четко структурирована и постоянно обновляться с течением времени.

Информацию, представляемую администратору безопасности для оценки состояния ИБ предприятия и принятия дальнейших решений по ее совершенствованию, тоже можно разделить на типы:

- Условно – постоянная информация (методики оценки и построения системы защиты, необходимые нормативные документы и законодательные акты и тд)
- Информация об общем состоянии сети предприятия и происходящих в ней процессах (карта сети, информация об узлах, каналах связи, сетевом оборудовании, информационных ресурсах, пользователях и их действиях в реальном времени, проходящем трафике и тд)
- Данные о состоянии системы защиты информации предприятия и ее отдельных элементов (угрозы, уязвимости, анализ рисков и тд)

Особое внимание следует уделить визуализации второго и третьего типов информации, так как она по большей части динамическая и очень важно ее правильно проанализировать, чтобы направить защитные меры в правильном направлении.

1. Информация об общем состоянии сети предприятия и происходящих в ней процессах

Построение схемы локальной сети

Визуализация локальной сети предприятия обычно заключается в наглядном расположении всех рабочих станций, серверов, сетевых

периферийных устройств, маршрутизаторов, коммутаторов и каналов на плоскости. Последнее время разработчики используют очень реалистичные изображения элементов сети, что делает ее еще более понятной.

Существуют продукты, которые позволяют пользователю «рисовать» сеть, используя доступные инструменты, которые в большинстве своем идентичные. Помимо самого построения схемы они могут контролировать сеть, в частности, например, ширину полосы пропускания, сетевой трафик, аптайм и прочие параметры роутеров, файрволов, серверов, свитчей, принтеров и других сетевых компонентов. А еще есть программы с более широким функционалом, в которые встроен модуль автоматического построения схемы сети, они сами сканируют сеть, к которой подключен компьютер (например, по диапазону ip-адресов), и выстраивают свою модель, которую администратор может редактировать и дополнять.

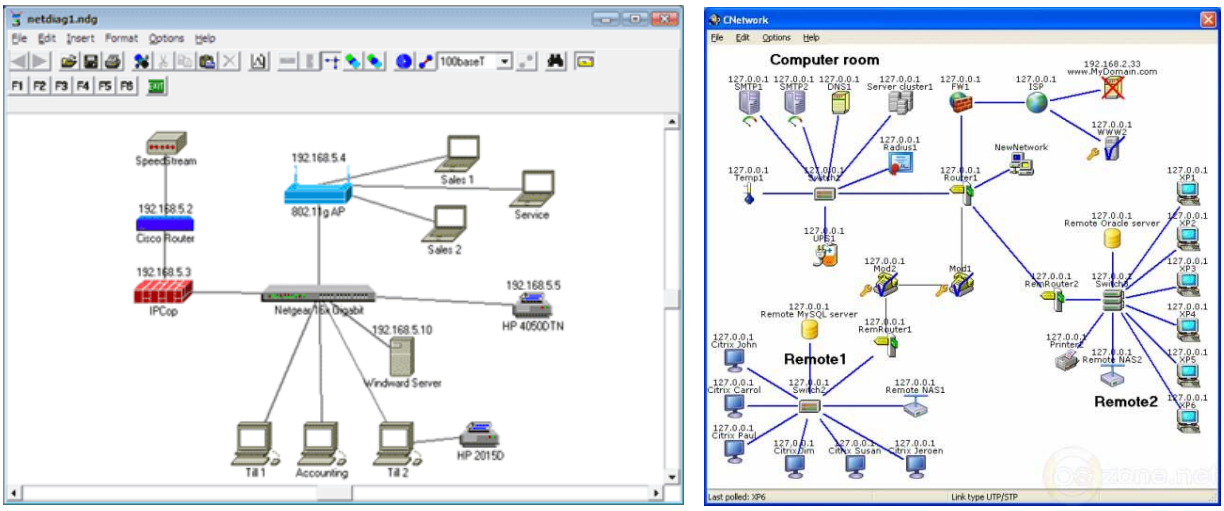


Рисунок 1 - Элементарное изображение сети в NetNotepad и Monitor one FP1.106.391

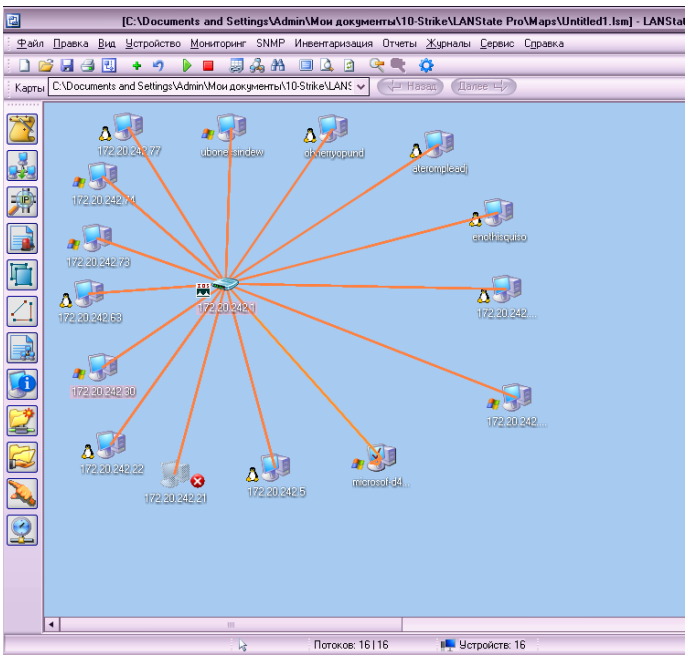


Рисунок 2 – «10 Страйк - Lanstate Pro»- автоматическое создание карт сети

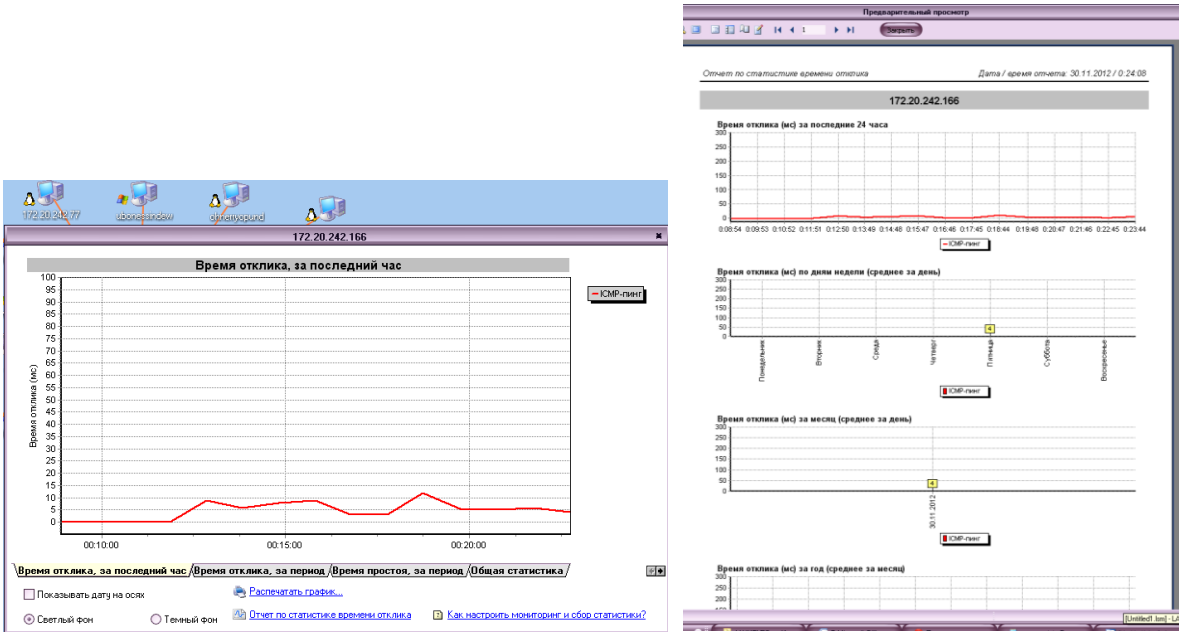


Рисунок 3 - Отображение времени отклика в виде графика в программе «10 Страйк - Lanstate Pro»

Очень важным является возможность редактирования карты и загрузки в файл карты каких- либо графических объектов (например, плана здания на фон) (рис. 4).

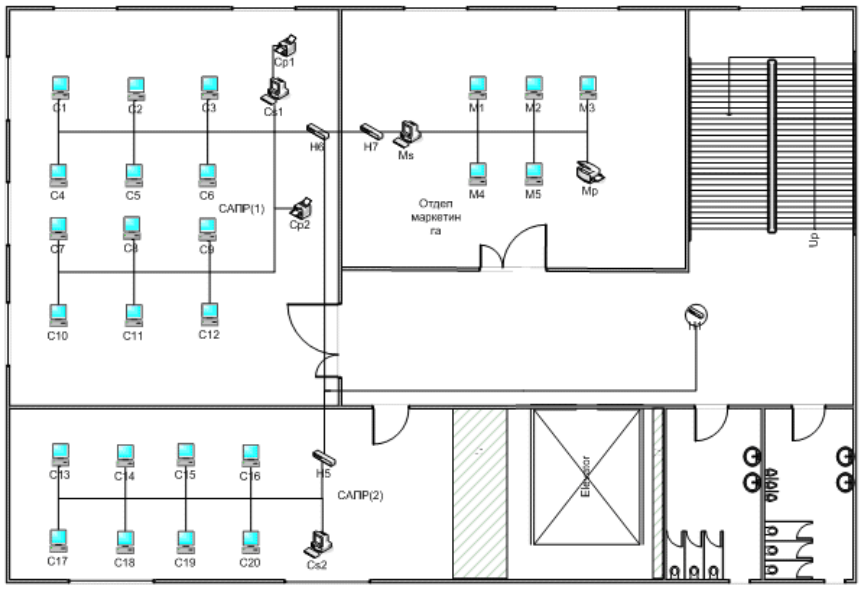


Рисунок 4 – Возможно объединения схемы сети с графическим планом здания

Управление информационными ресурсами и контроль доступа

Большинство продуктов предлагают обеспечить построение гибкой и подробной модели ИС, позволяющей централизованно хранить все защищаемые организацией данные.

Необходимая для отображения информация о состоянии информационных ресурсов:

- Местонахождение и роль ресурса в информационной структуре
- Уровень критичности ресурса с точки зрения ущерба, который может понести предприятие
- Полный перечень пользователей, который имеет доступ к ресурсу с учетом вида и прав доступа
- Средства защиты, прямо или косвенно повышающие защищенность ресурса

Пример визуализации информации о состоянии информационных ресурсов в комплексной системе управления информационной безопасностью и доступа к ним представлены на рисунке 5.

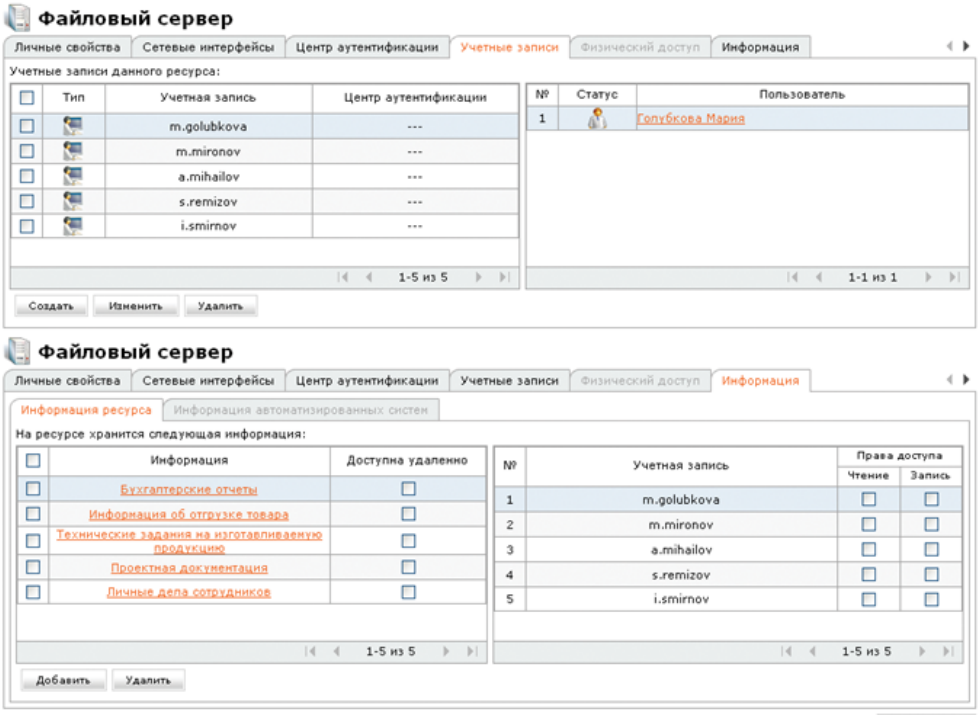


Рисунок 5 - Визуализация менеджера управления ресурсами в Digital Security LifeCycle Management System

В дополнение также используются программы, позволяющие контролировать сетевые общедоступные ресурсы и разрешения на папки, предупреждать каждый раз администратора когда изменен контроль доступа к общим папкам, противоречащий его политике доступа (рис. 6).

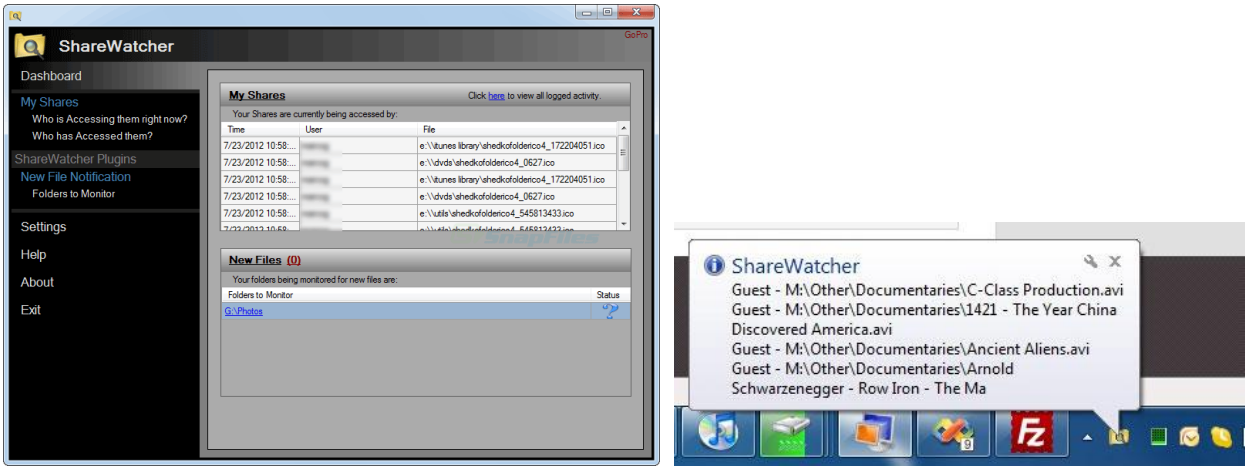


Рисунок 6 – Пример контроля сетевых общедоступных ресурсов в программе ShareWatcher

Как видно из иллюстраций в примерах, визуальное представление этого типа входных данных реализовано по минимуму и в большинстве своем совершенно не удобно для восприятия (в других подобных продуктах

также). Поэтому можно сделать смелый вывод о том, что в данной области есть еще много работы.

Данные о состоянии системы защиты информации предприятия и ее отдельных элементов

Анализ рисков

Анализ рисков представляет собой систематическое использование доступной информации для оценки частоты наступления конкретных событий и масштабов их последствий.

Обычно риски определяются как негативные события, которые могут возникнуть на данном предприятии. Однако анализ рисков дает шанс выявить потенциальные позитивные последствия. Благодаря исследованию всего пространства возможных последствий в каждой конкретной ситуации эффективный анализ рисков позволяет обнаружить проблемы и оценить перспективы.

Анализ рисков может проводиться на качественном или количественном уровне. Качественный анализ рисков, как правило, включает инстинктивную, внутреннюю оценку ситуации. При количественном анализе рискам пытаются присвоить числовые значения либо за счет использования эмпирических данных, либо путем определения количественных характеристик, присущих качественным оценкам.

В России наиболее серьезным и популярным продуктом, предназначенным непосредственно для расчета и анализа рисков информационной безопасности предприятия является программный продукт **ГРИФ**. Как обещают производители, ГРИФ дает полную картину защищенности информационных ресурсов в системе и позволяет выбрать оптимальную стратегию защиты информации компании. В результате работы определенного алгоритма программа представляет следующие данные:

- инвентаризацию ресурсов;
- значения риска для каждого ценного ресурса организации;
- значения риска для ресурсов после задания контрмер (остаточный риск);
- эффективность контрмер.

В приведенных ниже примерах, можно также проследить процесс работы данного продукта, где вся визуализация по сути также ограничивается созданием отчетов в виде графиков и элементарных диаграмм (рис. 6,7,8)

Рисунок 6 – Внесенные пользователям объекты информационной системы

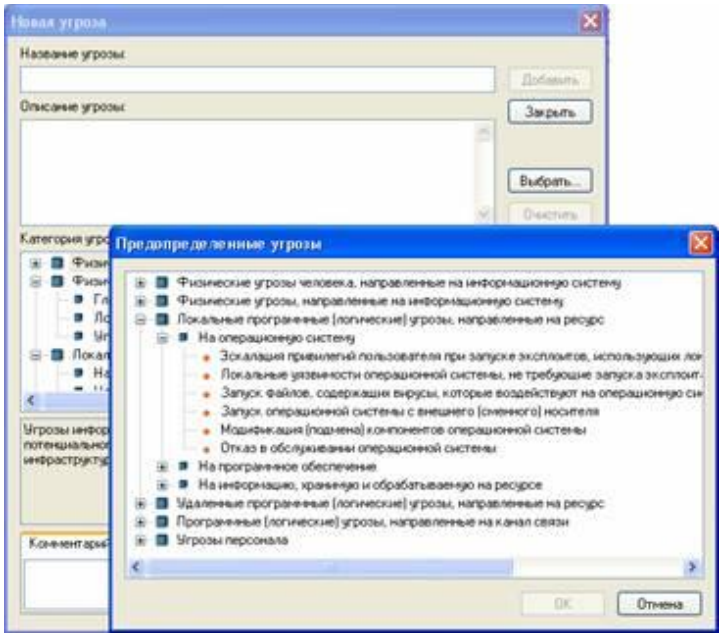
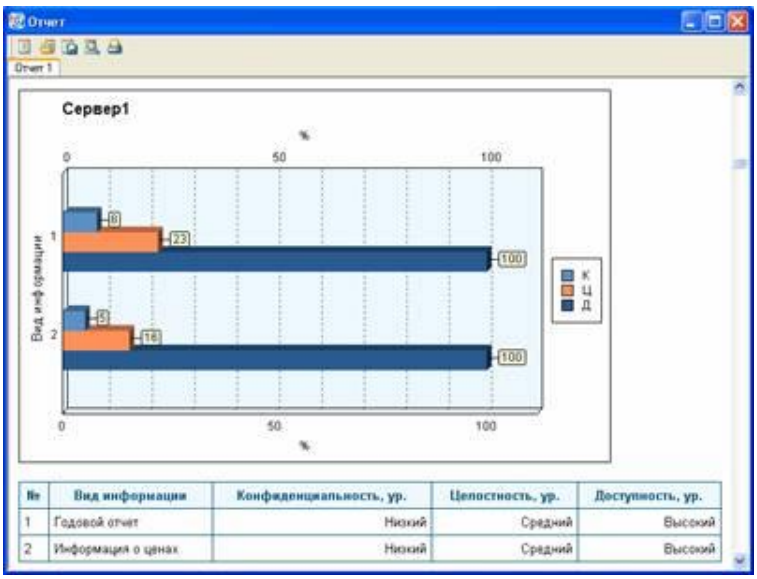


Рисунок 7 – Использование готовых каталогов угроз и уязвимостей



№	Вид информации	Конфиденциальность, ур.	Целостность, ур.	Доступность, ур.
1	Годовой отчет	Низкий	Средний	Высокий
2	Информация о ценах	Низкий	Средний	Высокий

Рисунок 8 – Фрагмент построения модели рисков (диаграмма одного из отчетов)

Однако, на зарубежном рынке существуют более мощные аналоги, которые не предназначены непосредственно для решения вопросов информационной безопасности, а в основном используются для расчета финансовых и экономических рисков, но которые используют те визуальные инструменты, которые так необходимы в области защиты информации. К таким продуктам, в первую очередь относятся, Oracle Crystal Ball и *@Risk* (рис. 9,10)

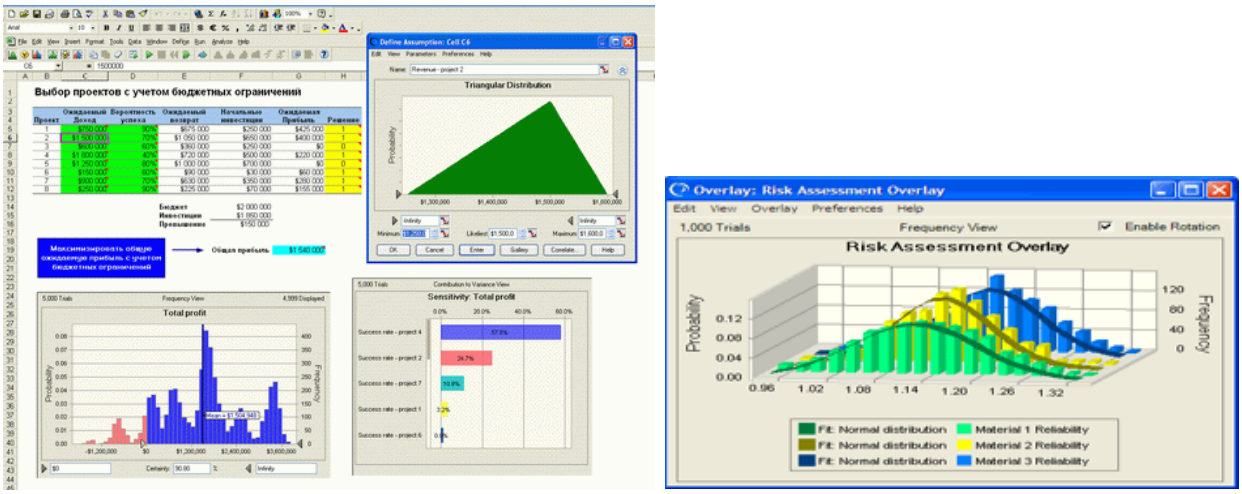


Рисунок 9 – Визуализация процессов в программе Oracle Crystal Ball

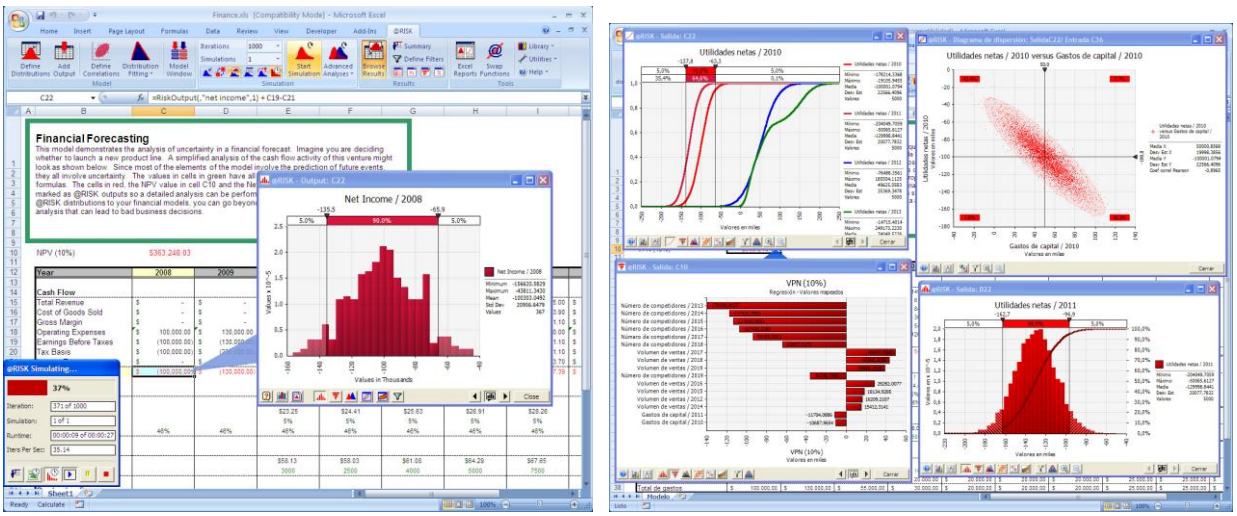


Рисунок 10 - Визуализация процессов в программе *@Risk*

Таким образом, можно сделать вывод, что в области защиты информации на предприятии вопрос представления входных данных для принятия правильных и рациональных решений администратором безопасности раскрыт далеко не полно, а в некоторых случаях практически никак. Следовательно, в этой области есть над чем работать и разрабатывать новые методики и способы представления таких данных в комплексной системе.

Литература и источники

1. Королёва Н.А., Экспертная система поддержки принятия решений по обеспечению информационной безопасности организации,диссертация - Тамбов,2006

2. Управление информационной безопасностью, http://www.arinteg.ru/articles/upravlenie-informatsionnoy-bezopasnostyu-26728.html

3. «Сетевые программы для системных администраторов от "10-Страйк" для мониторинга сети и серверов, инвентаризации сети и компьютеров, учета трафика, поиска файлов в сети», http://www.10-strike.com/rus/

4. DS LifeCycle Management System, http://www.dsec.ru/products/lcms/

5. В.М. Нечунаев. Оценка рисков информационной безопасности корпоративной информационной системы, Ижевский государственный технический университет, каф. «Системы и технологии информационной безопасности», 2009

6. ГРИФ 2006, http://www.dsec.ru/about/articles/grif_ar_methods/

7. @Risk, http://www.palisade.com/risk/ru/

8. Oracle Crystall Ball, http://www.oracle.com/partners/ru/knowledge-zone/applications/crystal-ball-030126-ru.html