Риск анализ это просто

ПОСОБИЕ ДЛЯ СТУДЕНТОВ

Первым делом

Для того, чтобы выполнить работу необходимо установить ПО (Security analysis).

Его необходимо устанавливать в ОС Windows XP x32 (Образ находится в архиве).

Советую запускать из-под виртуальной машины, предлагается VirtualBox (можете использовать vmware или другие аналоги). Любым доступным способом (при помощи общей папки или флешки) скопируйте всё содержимое архива в гостевую ОС, предварительно разархивировав РИСКАНАЛИЗ.zip в основной ОС.

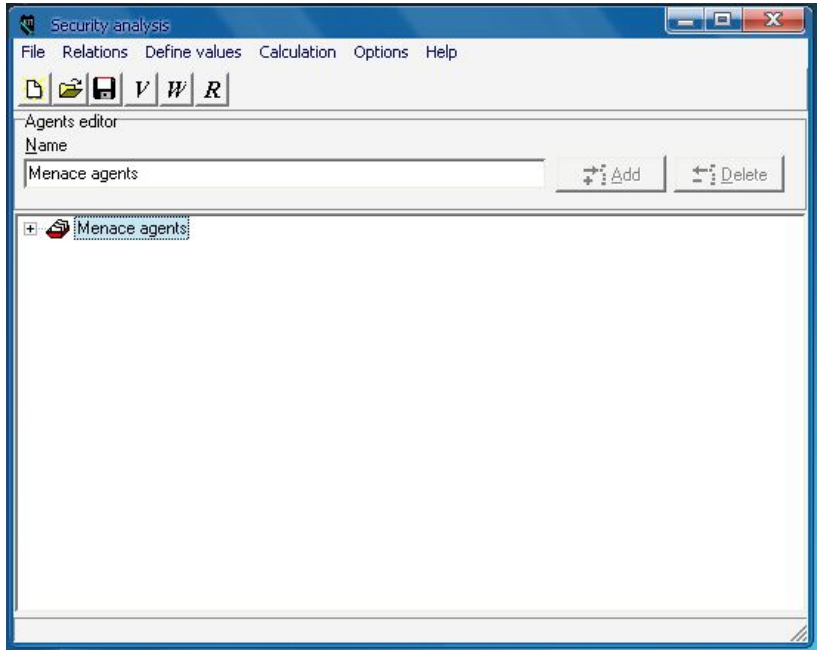
Запустите установочник 7zip, после установки разархивируйте архивы info_sec и infosec01.

Установка Security analysis

В папке info_sec лежит файл SETUP. Запустите его, несколько раз нажмите Next и Finish.

На этом всё.

Первый запуск

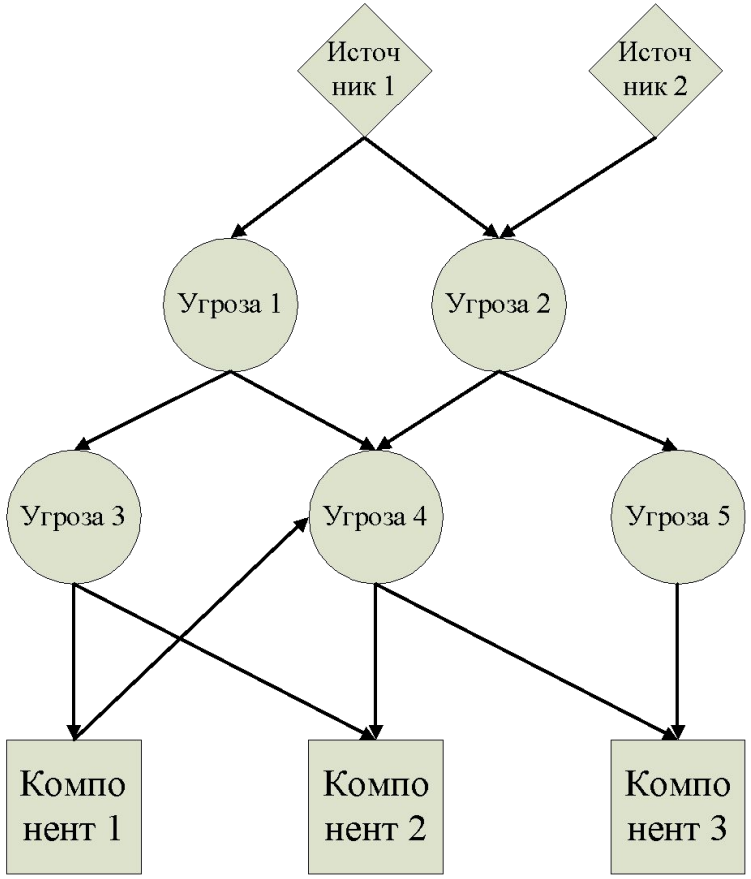


Это стартовое окно программы.
В строке меню File не вызывает вопросов. Там всё как всегда: открыть, сохранить, создать.
Relations – здесь вы определяете отношения элементов в графе (ЗАПОЛНЯТЬ ОБЯЗАТЕЛЬНО!!!).
Define values – для заполнения значений, после правильного заполнения Relations нужные клетки долны подсвечиваться.
Calculation – для пересчета матрицы W, вектора R. Есть два варианта алгоритма, можете посмотреть, что получится при изменении.
Options – опции отображения.
Help – помощь, есть учебник. Так же учебник есть в архиве fv1.0.

Пример

Чтобы не зацикливаться на содержимом, разберем случайную модель, которая представляется следующим графом и матрицей.

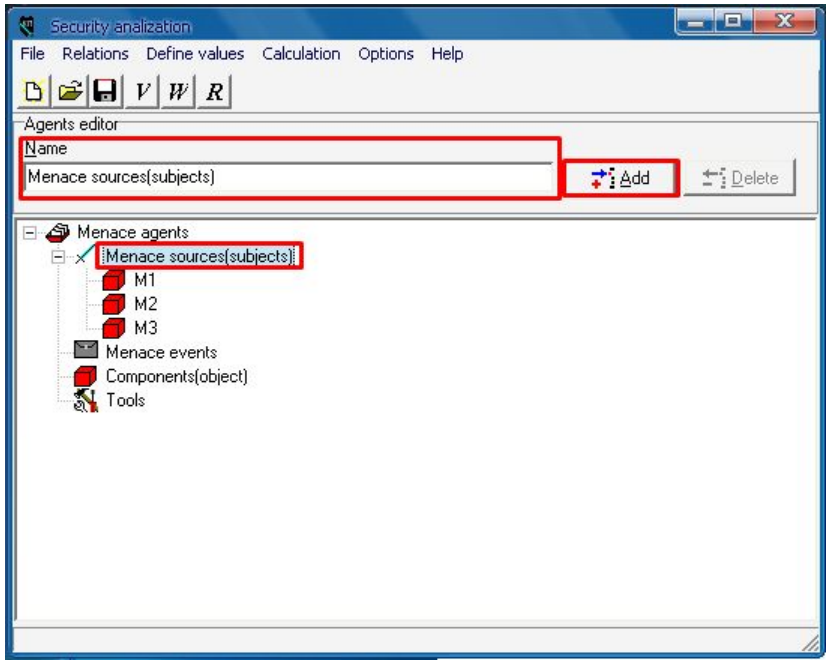
	Источник 1	Источник 2	Угроза 1	Угроза 2	Угроза 3	Угроза 4	Угроза 5	Компонент 1	Компонент 2	Компонент 3
Источник 1	0	0	1	1	0	0	0	0	0	0
Источник 2	0	0	0	1	0	0	0	0	0	0
Угроза 1	0	0	0	0	1	1	0	0	0	0
Угроза 2	0	0	0	0	0	1	1	0	0	0
Угроза 3	0	0	0	0	0	0	0	1	1	0
Угроза 4	0	0	0	0	0	0	0	0	1	1
Угроза 5	0	0	0	0	0	0	0	0	0	1
Компонент 1	0	0	0	0	0	1	0	0	0	0
Компонент 2	0	0	0	0	0	0	0	0	0	0
Компонент 3	0	0	0	0	0	0	0	0	0	0



Создание модели. Источники угроз

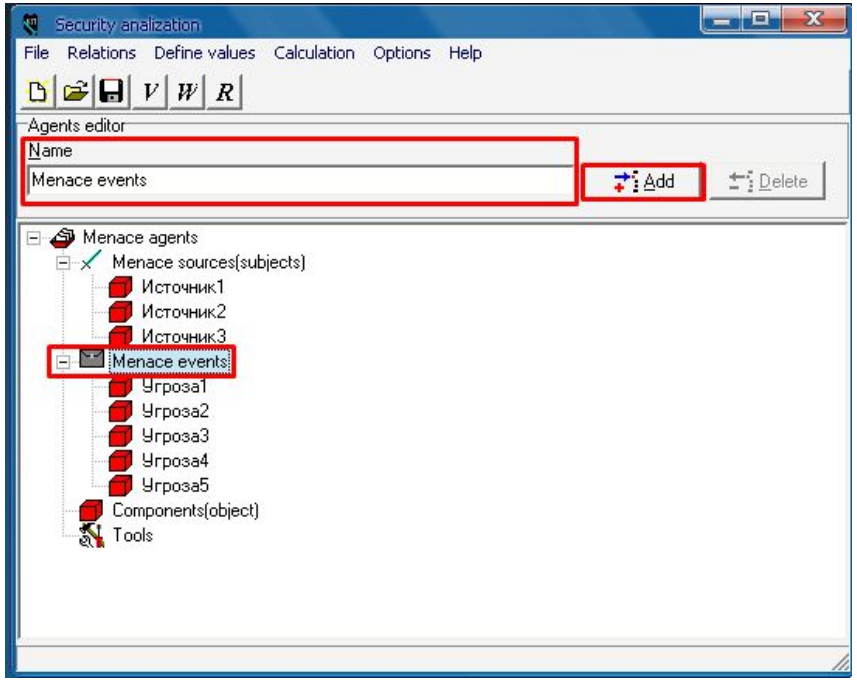
Для того, чтобы добавить источники угроз выберите Menace sources (subjects) и нажмите Add. Обязательно переименуйте каждый новый субъект.

PS. Тут компонентов источников 3, хотя на графе 2. Но исправлять это мне было уже лень, возможно, когда-то потом. Через слайд я это уже исправил (Колесников).



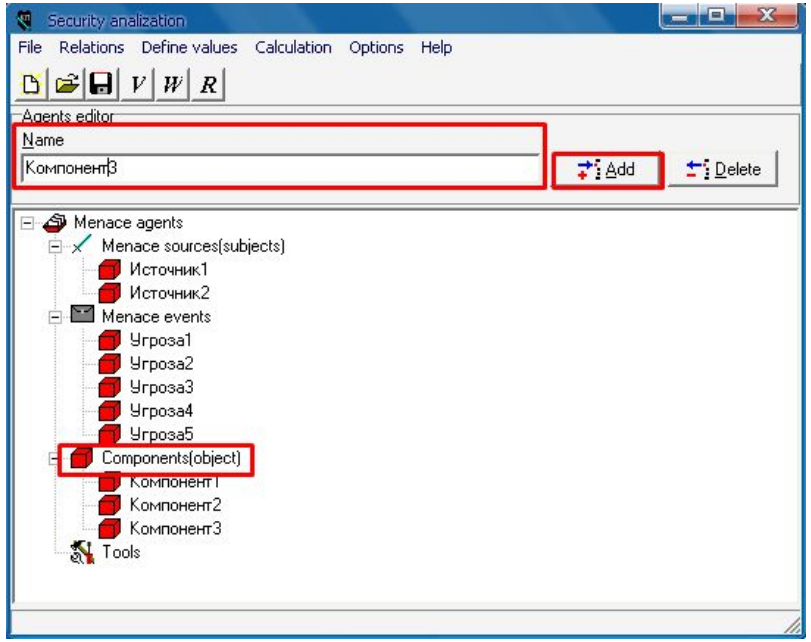
Создание модели. Угрозы

Угрозы в модель добавляются аналогично, только выберите Menace events.



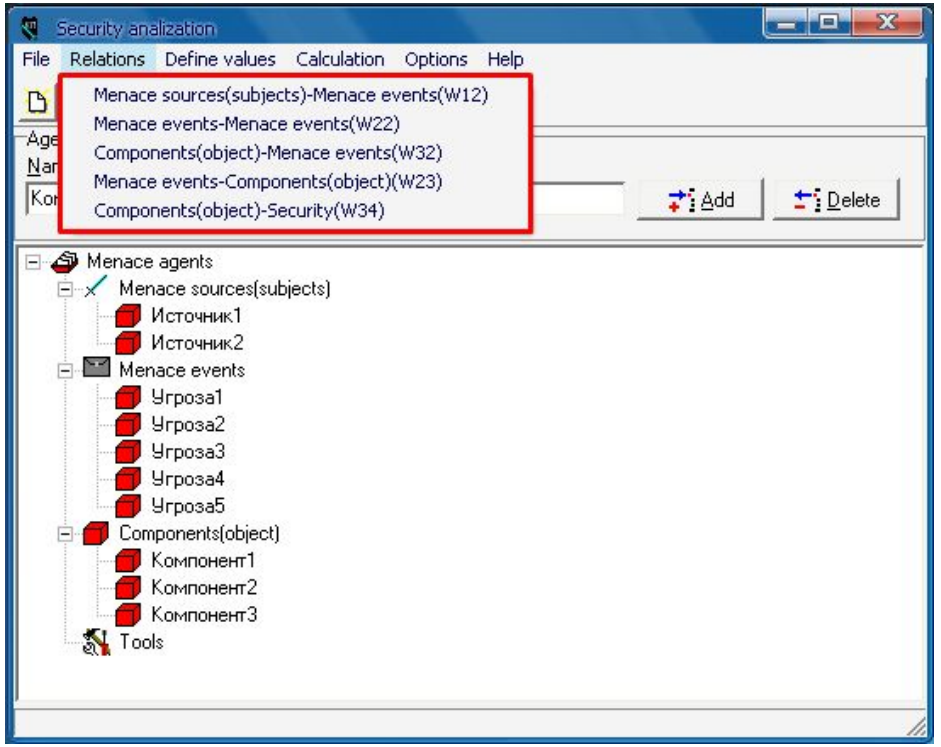
Создание модели. Компоненты

Аналогично поступаем с компонентами.



Связи

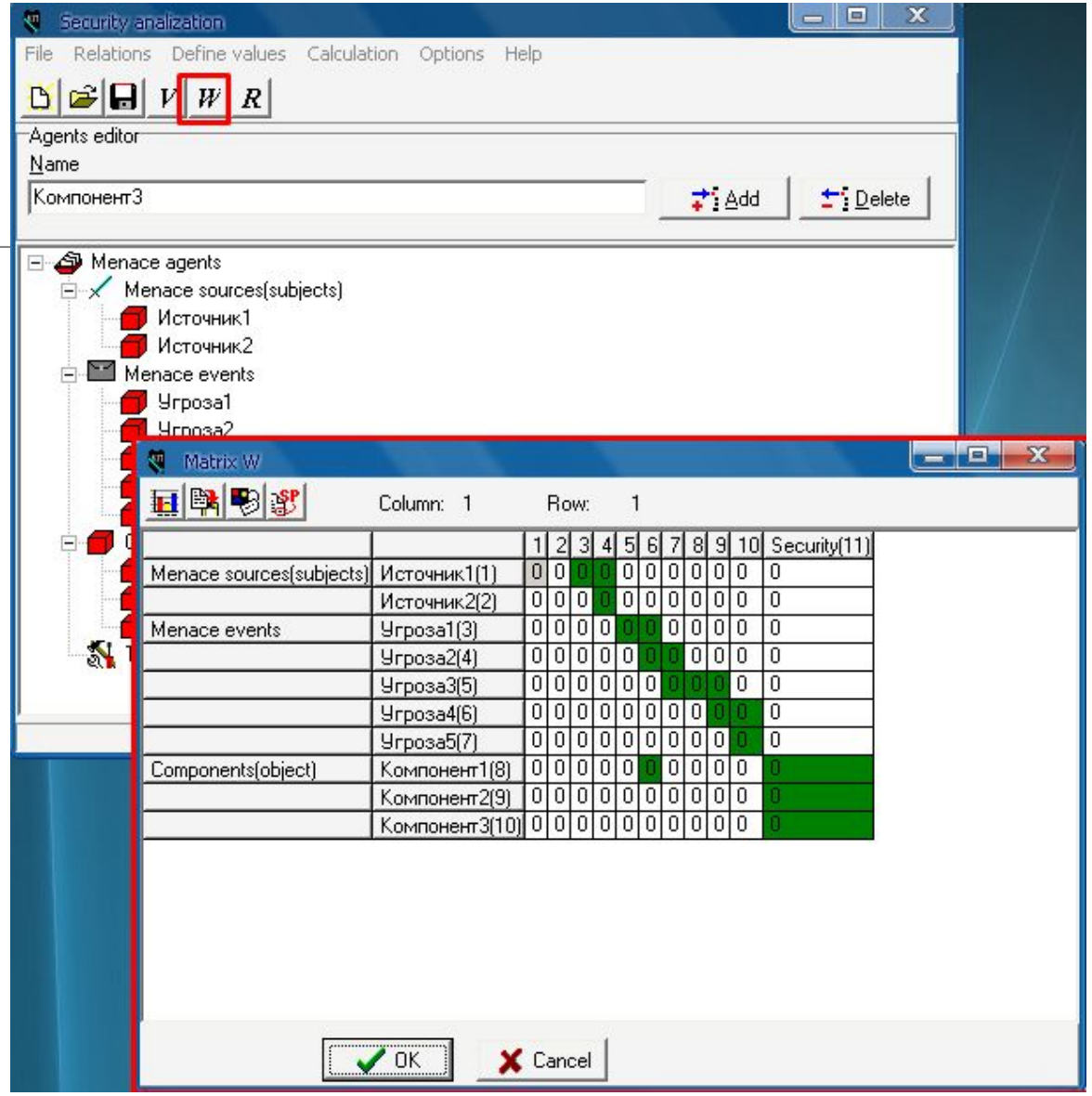
В меню Relations заполняете всё по матрице.
Components – security везде ставите 1.



Итог

Нажав на кноп ку «W», на стартовом окне, вы получите матрицу W, но пока без значений.

Она должна иметь вид, как матрица, определенная вами по графу.



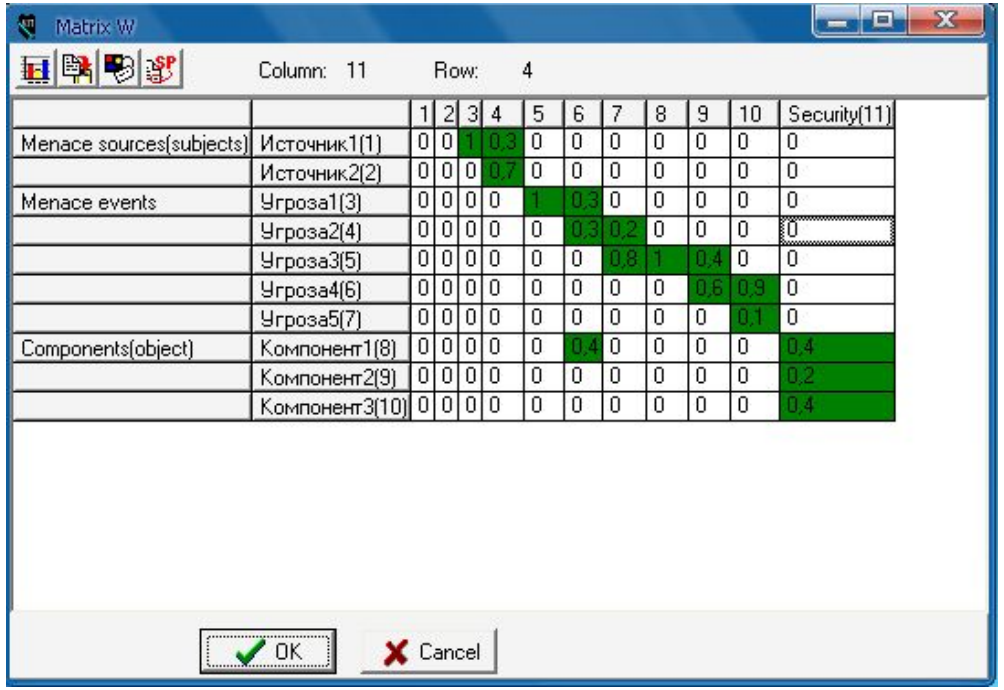
		1	2	3	4	5	6	7	8	9	10	Security(11)
Menace sources(subjects)	Источник1(1)	0	0	0	0	0	0	0	0	0	0	0
	Источник2(2)	0	0	0	0	0	0	0	0	0	0	0
Menace events	Угроза1(3)	0	0	0	0	0	0	0	0	0	0	0
	Угроза2(4)	0	0	0	0	0	0	0	0	0	0	0
	Угроза3(5)	0	0	0	0	0	0	0	0	0	0	0
	Угроза4(6)	0	0	0	0	0	0	0	0	0	0	0
	Угроза5(7)	0	0	0	0	0	0	0	0	0	0	0
Components(object)	Компонент1(8)	0	0	0	0	0	0	0	0	0	0	0
	Компонент2(9)	0	0	0	0	0	0	0	0	0	0	0
	Компонент3(10)	0	0	0	0	0	0	0	0	0	0	0

Заполнение матрицы W

Матрица W заполняется по правилу «в каждом столбце сумма должна быть равна 1.

Физический смысл этого заключен в том с какой вероятностью тот или иной субъект породит угрозу. Чем больше это значение, тем более вероятно, что именно он будет причиной.

Столбец Sesurity определяет критичность (важность) компонента. Чем больше значение, тем более ценен компонент.



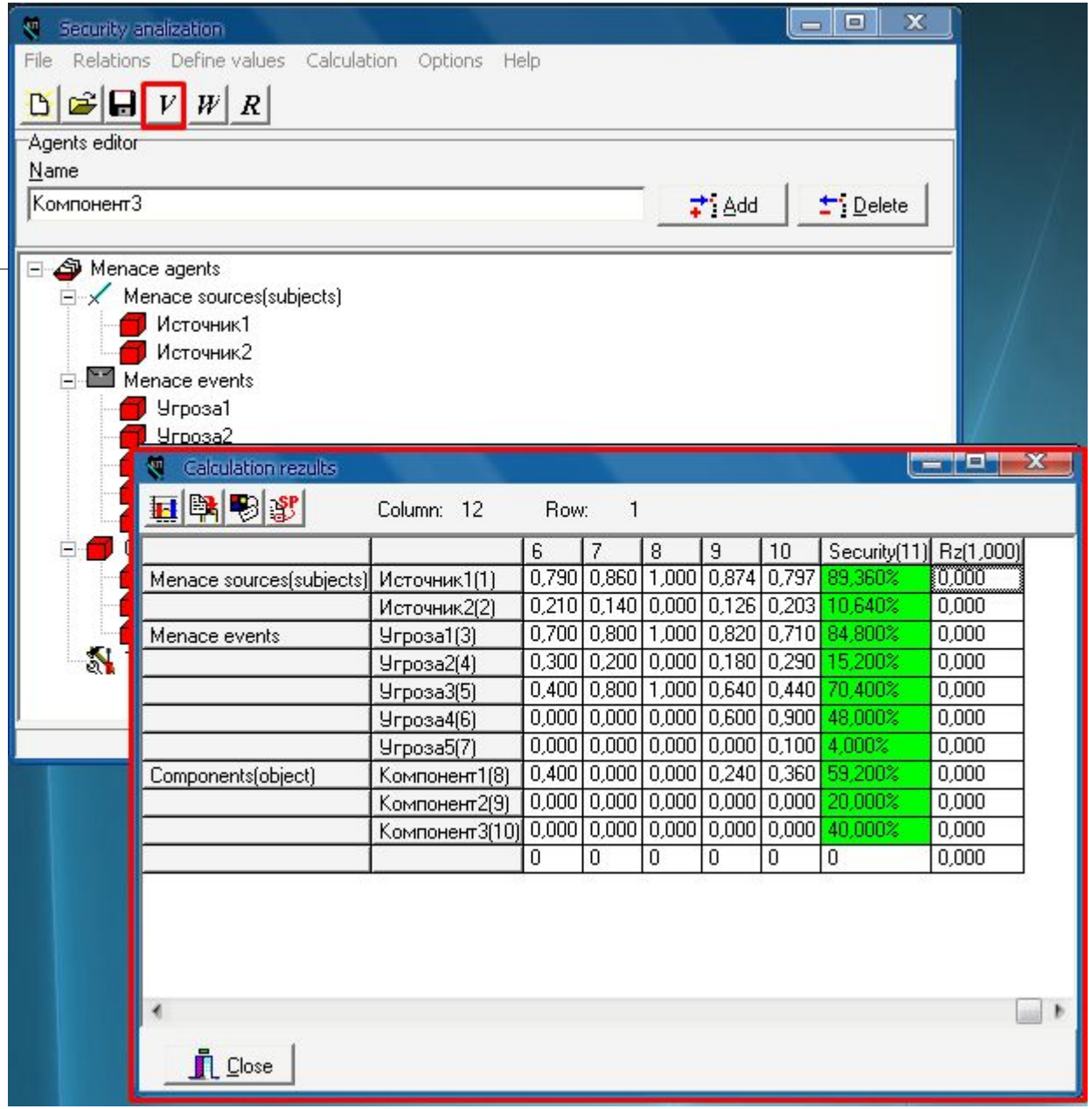
		1	2	3	4	5	6	7	8	9	10	Security(11)
Menace sources(subjects)	Источник1(1)	0	0	1	0,3	0	0	0	0	0	0	0
	Источник2(2)	0	0	0	0,7	0	0	0	0	0	0	0
Menace events	Угроза1(3)	0	0	0	0	1	0,3	0	0	0	0	0
	Угроза2(4)	0	0	0	0	0	0,3	0,2	0	0	0	0
	Угроза3(5)	0	0	0	0	0	0	0,8	1	0,4	0	0
	Угроза4(6)	0	0	0	0	0	0	0	0	0,6	0,9	0
	Угроза5(7)	0	0	0	0	0	0	0	0	0	0,1	0
Components(object)	Компонент1(8)	0	0	0	0	0	0,4	0	0	0	0	0,4
	Компонент2(9)	0	0	0	0	0	0	0	0	0	0	0,2
	Компонент3(10)	0	0	0	0	0	0	0	0	0	0	0,4

Пересчёт

Для пересчета матрицы достаточно нажать на главном окне кнопку «V» и программа сама всё посчитает.

После этого этапа начинается анализ полученных значений столбца Security, определяются самый «опасный» источник, несколько критичных угроз и компонент.

Пока на этом всё (30.03.2018).



		6	7	8	9	10	Security(11)	Rz(1,000)
Menace sources(subjects)	Источник1(1)	0,790	0,860	1,000	0,874	0,797	89,360%	0,000
	Источник2(2)	0,210	0,140	0,000	0,126	0,203	10,640%	0,000
Menace events	Угроза1(3)	0,700	0,800	1,000	0,820	0,710	84,800%	0,000
	Угроза2(4)	0,300	0,200	0,000	0,180	0,290	15,200%	0,000
	Угроза3(5)	0,400	0,800	1,000	0,640	0,440	70,400%	0,000
	Угроза4(6)	0,000	0,000	0,000	0,600	0,900	48,000%	0,000
	Угроза5(7)	0,000	0,000	0,000	0,000	0,100	4,000%	0,000
Components(object)	Компонент1(8)	0,400	0,000	0,000	0,240	0,360	59,200%	0,000
	Компонент2(9)	0,000	0,000	0,000	0,000	0,000	20,000%	0,000
	Компонент3(10)	0,000	0,000	0,000	0,000	0,000	40,000%	0,000
		0	0	0	0	0	0	0,000