Риск анализ это просто - 2

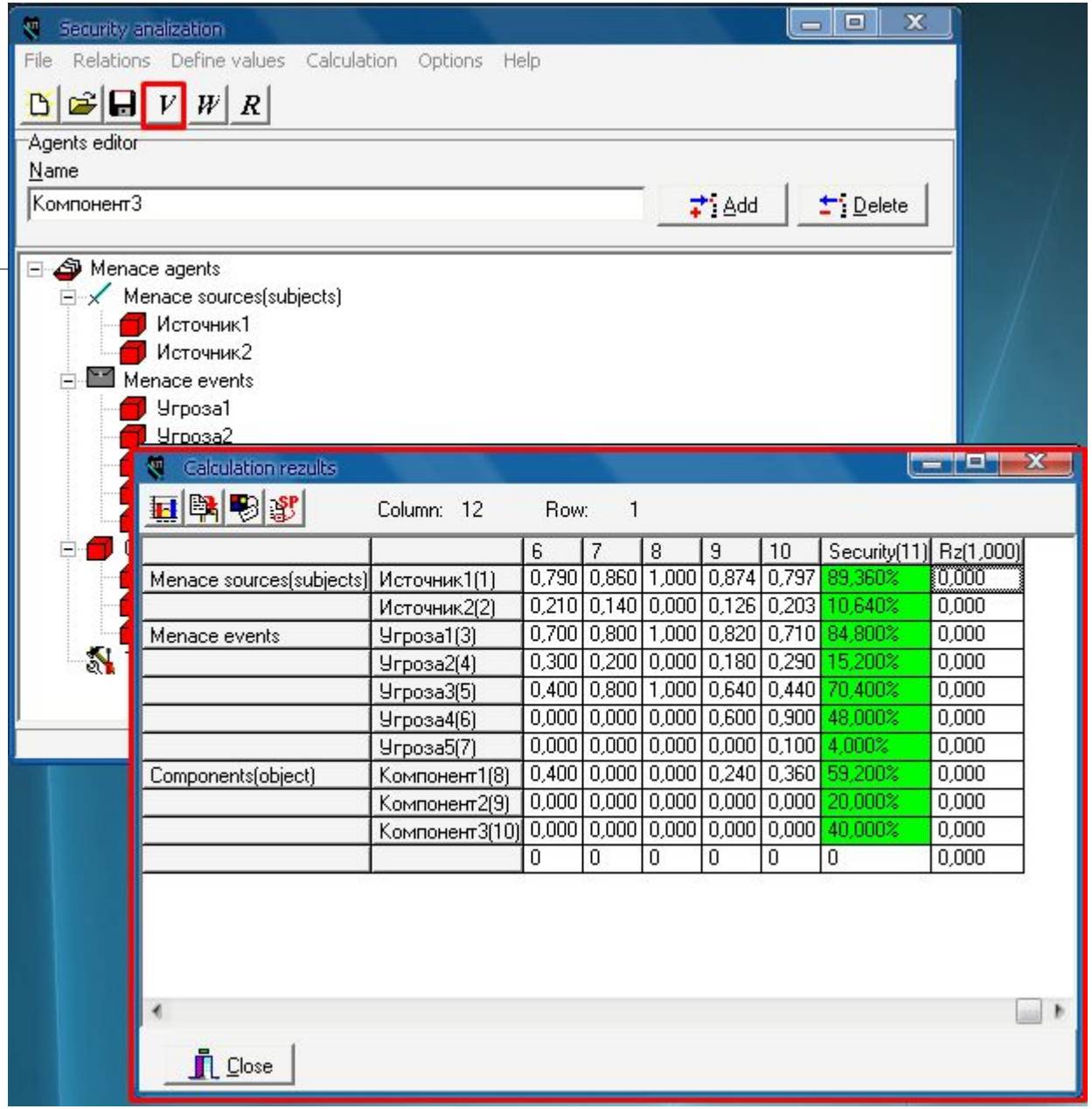
ПОСОБИЕ ДЛЯ СТУДЕНТОВ

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).



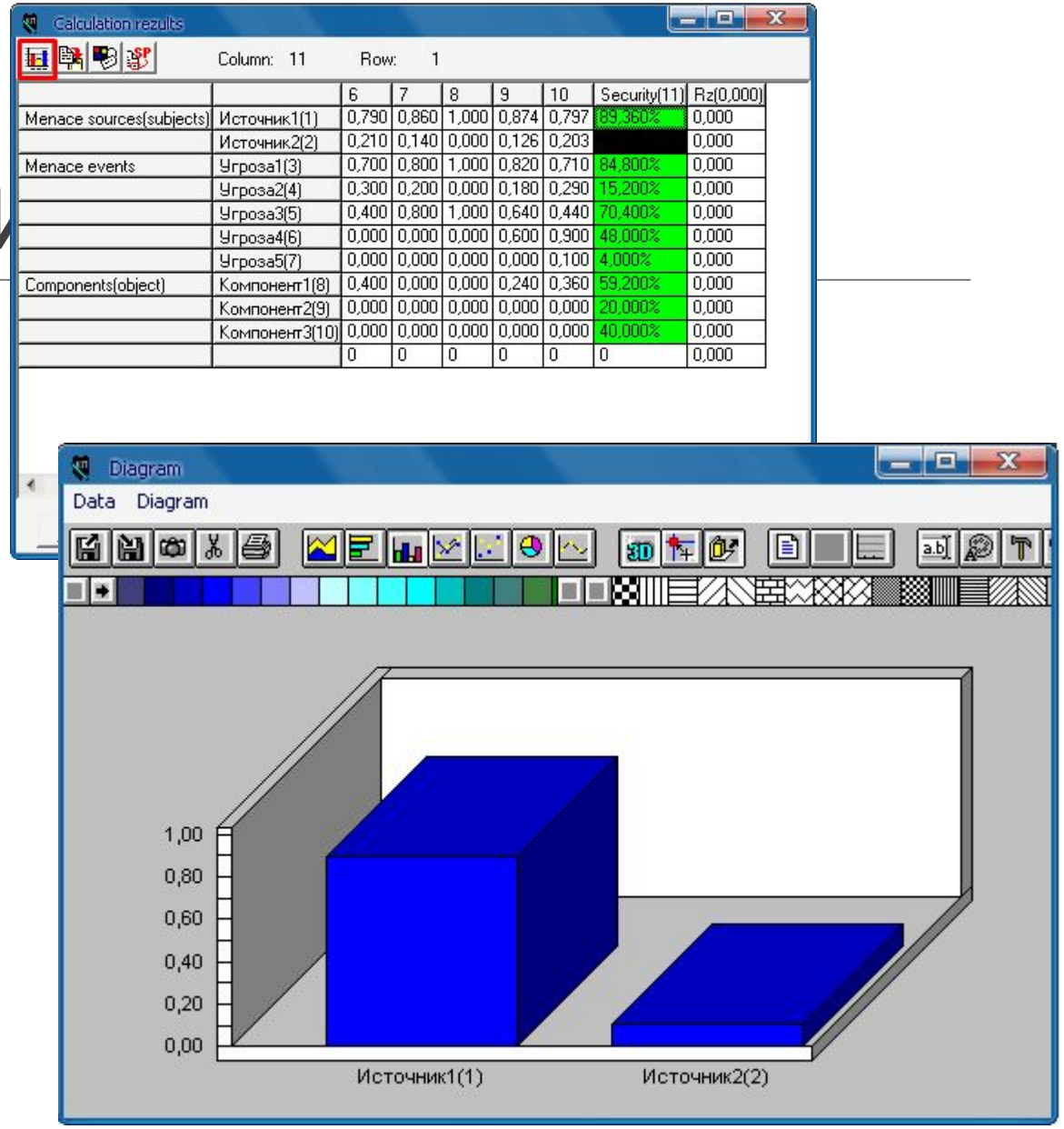
		6	7	8	9	10	Security(11)	Rz(1,000)
Menace sources(subjects)	Источник1(1)	0,790	0,860	1,000	0,874	0,797	89,360%	0,000
	Источник2(2)	0,210	0,140	0,000	0,126	0,203	10,640%	0,000
Menace events	Угроза1(3)	0,700	0,800	1,000	0,820	0,710	84,800%	0,000
	Угроза2(4)	0,300	0,200	0,000	0,180	0,290	15,200%	0,000
	Угроза3(5)	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

Анализ Источники

Первым делом получаем диаграмму по источникам. Для этого выделяем их в столбце Security и нажимаем на кнопку Graph.

Получаем столбчатую диаграмму. Столбцы можно перекрашивать, убирать эффект 3D и т.п.

Конечно, по цифрам и так можно понять, что «Источник 1» несет большую угрозу, чем «Источник 2», но если их много, и надо выбрать несколько, то данный инструмент будет полезным, пользуйтесь.



		6	7	8	9	10	Security(11)	Rz(0,000)
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		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

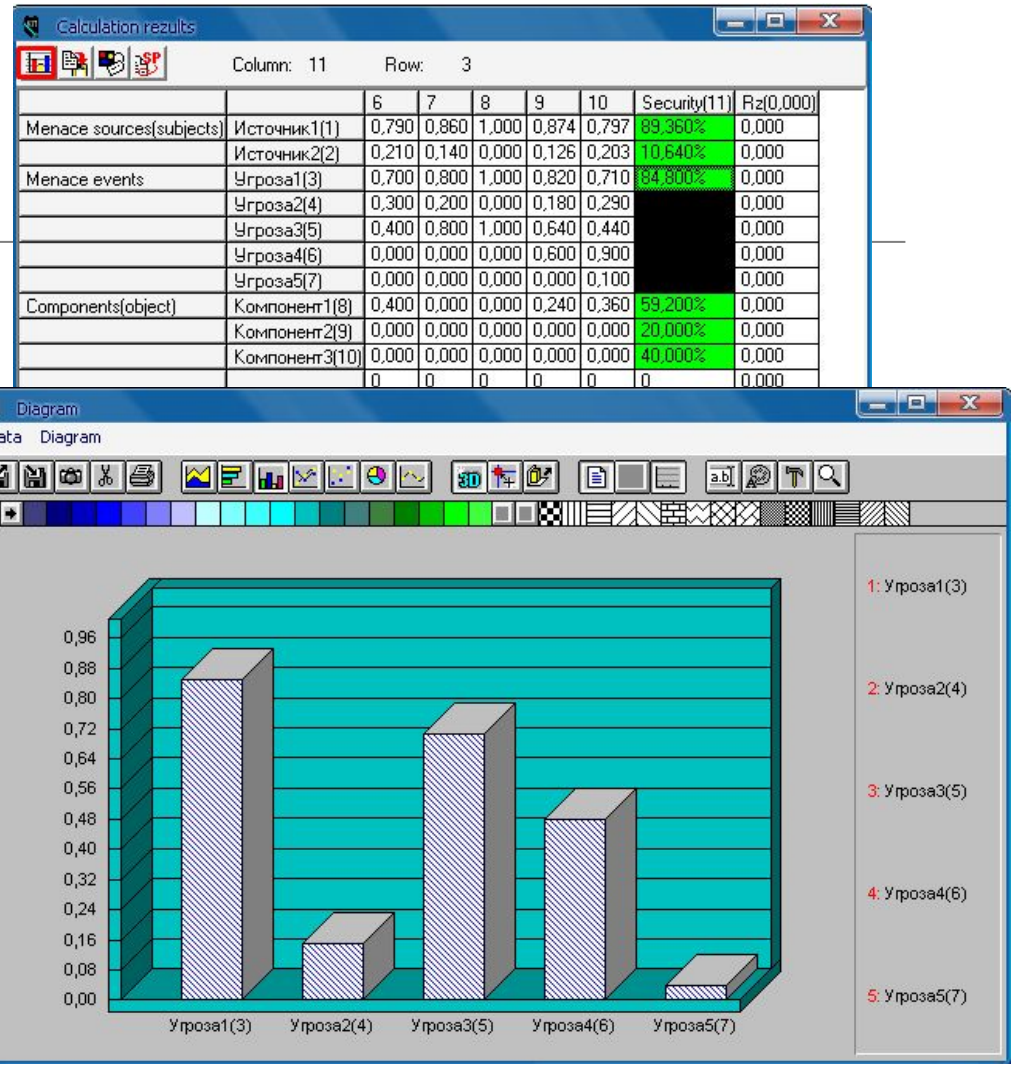
Анализ Угрозы

С угрозами аналогично.

Как пример, можете использовать легенду, она также настраивается, можно менять шрифт, кегель, цвет и т. п.

Собственно среди угроз особенно выделяются 1, 3 и 4.

Значит на них нам и необходимо действовать.



		6	7	8	9	10	Security(11)	Rz(0,000)
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		0,000
	Угроза3(5)	0,400	0,800	1,000	0,640	0,440		0,000
	Угроза4(6)	0,000	0,000	0,000	0,600	0,900		0,000
	Угроза5(7)	0,000	0,000	0,000	0,000	0,100		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

Анализ итог

Есть один ярко выраженный опасный источник и 3 угрозы.

Против них ищем примерно от 7 до 12 средств защиты.

	Источник 1	Источник 2	Угроза 1	Угроза 2	Угроза 3	Угроза 4	Угроза 5	Компонент 1	Компонент 2	Компонент 3	Стоимость
Средство 1	0,1	0,5	0	0	0,2	-0,2	0	0	0	0,1	10
Средство 2	0	0	0,2	0,1	0,2	0	0,2	0	0,1	0	20
Средство 3	0,2	0,2	0	0,2	-0,2	0	-0,3	0,1	0	0	30
Средство 4	0	0,4	0,2	0	0,3	0,1	0	0,1	0	0	15
Средство 5	0	0	0,2	0	0,2	0,2	0	0	0,1	0	25
Средство 6	0,2	0	0,2	0,5	0	0,2	0	0	0	0,1	35
Средство 7	0,4	0,4	0,2	-0,2	-0,1	0	0,2	0	0,1	0	5

Значения в клетках это то, как то или иное средство будет влиять на источник или угрозу. Чем ближе к 1, тем сильнее влияет. Отрицательное значение означает, что средство еще способствует возникновению угрозы. Про стоимость дальше.

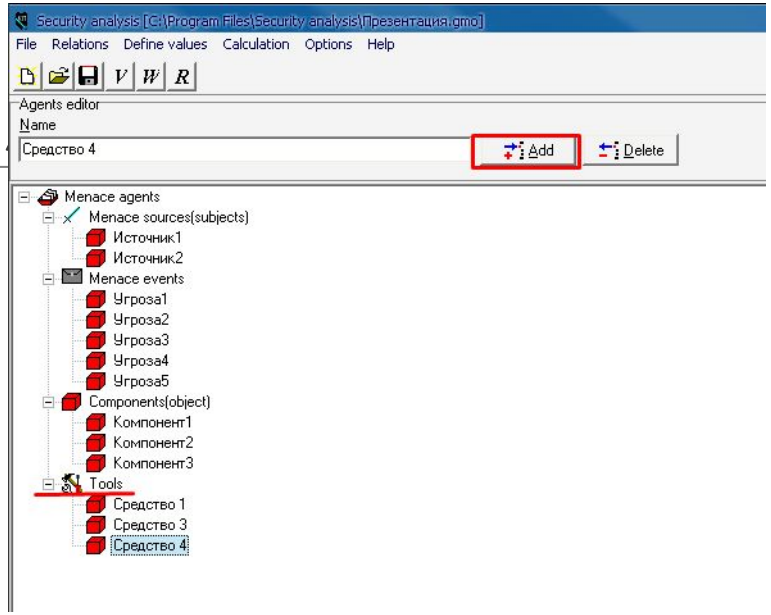
Теперь комбинируем комплексы защиты. Рекомендую выбрать 2-3 комплекса тематических (организационный, правовой, аппаратный, обновления, закупка и т.п.) и один комбинированный. Я выбрал следующие комплексы (1,3,4; 2,5,7; 1,5,6).

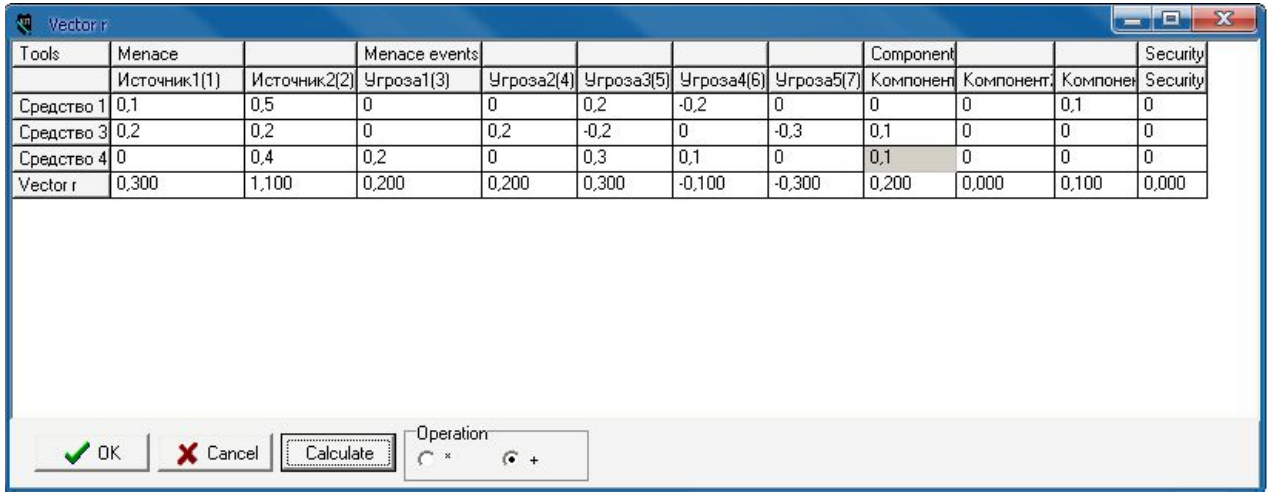
Вектор R. Комплект 1 (1,3

Средства защиты добавляются также, как и источники, угрозы, или компоненты.

Далее нажимаем на кнопку R и выставляем всё согласно таблице.

Обратите внимание на метод Operation. Если у вас средства зависимые, то ставите *, если нет, то +. Но тут стоит честь, что при выборе метода *, отрицательное действие нужно считать иначе, поэтому ставьте + пока что. Нажимаем OK.





Пересчет. Комплекс 1

Выходим в главное окно, нажимаем на V и смотрим в правый верхний угол, там изменилось число Rz. Для комплекса 1 Rz = 0,668. Получив это значение считаем значение эффективности ez.

$e_Z = \frac{R_Z}{c_Z} = \frac{0{,}668}{55} = 0{,}0121$, где c_Z - общая стоимость комплекса, то есть из таблички это 10 + 30 + 15 = 55.

		1	2	3	4	5	6	7	8	9	10	Security(11)	Rz(0,668)
Menace sources(subjects)	Источник1(1)	0,000	0,000	1,000	0,300	1,000	0,790	0,860	1,000	0,874	0,797	89,360%	0,268
	Источник2(2)	0,000	0,000	0,000	0,700	0,000	0,210	0,140	0,000	0,126	0,203	10,640%	0,117
Menace events	Угроза1(3)	0,000	0,000	0,000	0,000	1,000	0,700	0,800	1,000	0,820	0,710	84,800%	0,119
	Угроза2(4)	0,000	0,000	0,000	0,000	0,000	0,300	0,200	0,000	0,180	0,290	15,200%	0,004
	Угроза3(5)	0,000	0,000	0,000	0,000	0,000	0,400	0,800	1,000	0,640	0,440	70,400%	0,118
	Угроза4(6)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,600	0,900	48,000%	-0,016
	Угроза5(7)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,100	4,000%	-0,004
Components(object)	Компонент1(8)	0,000	0,000	0,000	0,000	0,000	0,400	0,000	0,000	0,240	0,360	59,200%	0,046
	Компонент2(9)	0,000	0,000	0,000	0,000	0,000	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	0,000	0,000	0,000	0,000	0,000	40,000%	0,015
		0	0	0	0	0	0	0	0	0	0	0	0,000

Итог исследования

Проводим аналогичную операцию для каждого из комплексов и получаем табличку.

	Комплекс 1	Комплекс 2	Комплекс 3
Rz	0,6680	0,7680	0,7740
cz	55,0000	50,0000	70,0000
ez	0,0121	0,0154	0,0111

Из нее видно, что более эффективный 2 комплекс, лучшую оценку влияния (Rz) имеет третий комплекс, но он самый дорогой. Комплекс 1 показал меньшее значение Rz, но имеет преимущество перед самым дорогим. (Примерно так описываете результат, но конечно подумайте почему так получилось).

Отрицательное влияние средств защиты

Описываете то, что может произойти при внедрении каких-то средств защиты. Например усложнили политику паролей – пользователи перестали их запоминать – начали писать на бумажке – эту бумажку подсмотрел сотрудник другого отдела и передал информацию Вывод: необходимо еще потратить время на обучение сотрудников.

Или перешли на биометрическую пропускную систему – начали собирать больше информации о сотрудниках – охранная организация расторгла контракт и охранник слил базу себе на флэшку. Вывод: надо еще потратить деньги и время, чтобы грамотно настроить доступ к БД системы контроля и управления доступом.

Выводы

На этом всё.

В выводах пишите, что у вас получилось, что вы узнали, каких результатов достигли, кому и в какой сфере деятельности может пригодиться ваша работа.