Выводы

Из апробированных нейронных сетей наиболее перспективными для применения в средствах защиты компьютерных систем являются многослойный перспетрон, сеть Кохонена, сеть PNN, а также рекуррентные сети.

Многослойный перспетрон, сеть Кохонена и сеть PNN целесообразно использовать в управляющих элементах СОА, СОУ, антивирусных системах и в системах защиты от кейллогеров. При этом в качестве анализируемых возможно применение параметров представленных в таблице.

Рекуррентные сети, а также сеть PNN возможно использовать в системах защиты от спама.

Вследствие того что возможности указанных нейронных сетей во многом дополняют друг друга, перспективным путем дальнейших исследований является разработка комбинированной нейронной сети. Ее основными характеристиками должны быть достаточно высокая емкость и точность, а также возможность дообучения в процессе функционирования.

Список литературы

1. *Ежов А.А., Шумский С.А.* Нейрокомпьютинг и его применение в экономике и бизнесе. – М.: МИФИ, 1998. – 224 с.

2. *Круглов В.В., Борисов В.В.* Искусственные нейронные сети. – М.: Горячая линия-Телеком, 2002. – 382 с.

3. *Каллан Р.* Основные концепции нейронных сетей: Пер. с англ. – М.: Вильямс, 2003. – 288 с.

4. *Люгер Ф.* Искусственный интеллект: стратегии и методы решения сложных проблем, 4-е издание.: Пер. с англ. – М.: Вильямс, 2003. – 864 с.

5. *Архипов А., Ишутин А.* Применение моделей обнаружения аномалий для выявления атак // Четверта науково-технічна конференція. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Тези доповідей. – 2006. – с.71-72.

Поступила 01.06.2006

УДК 681.621.396 **Павлов И.Н.**

ПРОЕКТНЫЙ АНАЛИЗ МАКСИМАЛЬНОГО КОЛИЧЕСТВА БАРЬЕРОВ В СОСТАВЕ МЕХАНИЗМА ЗАЩИТЫ ПРИ ОЦЕНКЕ ЖИВУЧЕСТИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Вступление

Специфика проектирования СЗИ на этапе оформления технического задания требует качественной оценки необходимости и достаточности количественных значений барьеров в составе механизма защиты комплексной системы защиты информации (КСЗИ). Другими словами, необходимо определить, насколько увеличение барьеров в составе механизма защиты способно качественно увеличить живучесть самих механизмов защиты, так как нельзя создать действительно живучую КСЗИ, опираясь только на увеличение барьеров в составе механизмов защиты КСЗИ.

2. Основная часть

2.1. Определение показателей живучести механизмов защиты КСЗИ

Как было показано в [1], учитывая общее количество барьеров в МЗ и изменение задач защиты, можно вывести выражение:

$$G_m\left(Z^*\right)=\left(\frac{g_{\text{общ}}-g_{z^*}}{g_{\text{общ}}}\right), \qquad (1)$$

где G_m называется *коэффициентом стойкости* МЗ относительно множества задач z_i^*, т.е. это "доля" барьеров, отказы которых допустимы в КСЗИ без ущерба для её функционирования в зависимости от задач, которые необходимо решить.

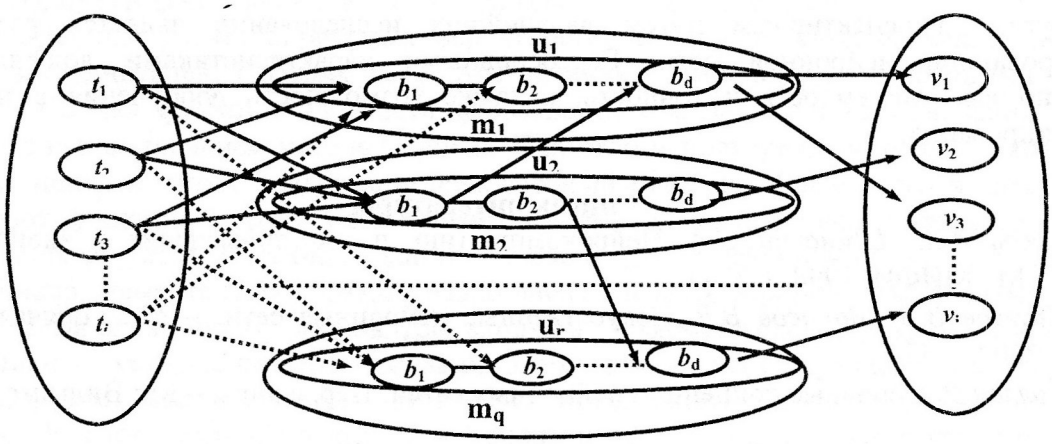

Рис. 1. Место барьеров в системе защиты информации

Из (1) видно, что:

– $0 \le G_m(Z^*) \le 1$;

– $G_m(Z^*) = 0$ тогда и только тогда, когда в системе недопустим отказ ни одного барьера. Причём *КСЗИ может быть достаточно надёжна, но не живуча*, если цель функционирования определена, как выполнимость всех задач из множества Z^*, и не предусмотрена функциональная избыточность и взаимозаменяемость барьеров;

– $G_m(Z^*) = 1$ тогда и только тогда, когда $Z^* = \varnothing$, т.е. КСЗИ "абсолютно" живуча только относительно пустого множества задач.

Введённый коэффициент стойкости существенно зависит от цели функционирования, а значит, от множества задач Z^*. Например, в системе имеется 10 барьеров. Цель функционирования определяется, как выполнимость всех задач из множества Z^*. Предположим, что барьеры однородны. Для решения задач из множества Z^* требуется 7 барьеров. Тогда коэффициент живучести СЗИ относительно множества задач Z^* будет $Srv(Z^*) = 0{,}3$. Если изменить цель функционирования, потребовав, например, выполнения всех задач из множества Z_1^*, для чего необходимо не менее 6 барьеров, то коэффициент живучести системы при этой новой цели функционирования будет $Srv(Z_1^*) = 0{,}4$.

Важным является то, что при деградации системы для повышения её живучести можно осуществить смену цели функционирования.

Например, определим три цели функционирования СЗИ:

1. Решение всех задач из множества Z_1.
2. Решение всех задач из множества Z_2.
3. Решение всех задач из множества Z_3.

Причём для выполнения всех задач из множества Z_1 в системе должно быть:

- не менее 7 исправных барьеров;
- не менее 5 исправных барьеров;

- не менее 2 исправных барьеров.

Тогда коэффициент живучести системы относительно соответствующей цели функционирования равен: $Srv(Z_1) = 0{,}3$; $Srv(Z_1) = 0{,}5$; $Srv(Z_1) = 0{,}8$.

Предположим, что переход к новой цели функционирования осуществляется в том случае, когда выполнимость заданной цели невозможна. Проследим изменение коэффициента живучести при изменении цели функционирования системы. Рассмотрим ту же систему G, состоящую из 10 барьеров. Начальной цели функционирования Z_1 соответствует $Srv(Z_1) = 0{,}3$. Отказ любого 4-го барьера означает нарушение условия выполнимости заданной цели функционирования, т.е. в системе из 7 барьеров отказ означает невозможность выполнения заданной цели – необходимости перехода к новой цели функционирования, например Z_2. Коэффициент живучести $Srv(Z_2) = 0{,}3$ - при переходе к новой цели функционирования системы, условия выполнимости цели функционирования предполагают не более двух отказов барьеров в системе из 7 барьеров. Отказ 6-го барьера (или 2 барьеров в системе из 7 барьеров) означает невыполнимость цели функционирования, определяемую множеством задач Z_2, а значит, необходим переход к новой цели, например Z_3. При этом $Srv(Z_3) = 0{,}6$. Переход к новой цели функционирования не только не ухудшил живучесть системы, а даже улучшил показатель живучести.

Таким образом, при проектировании системы либо в процессе её эксплуатации можно определить иерархию целей функционирования. Переход от одной цели к другой (от цели «верхнего уровня» к цели «низкого уровня») должен осуществляться, когда живучесть (не работоспособность, а живучесть) падает до нуля.

Под функциональным отказом будем понимать неспособность барьеров в системе защиты выполнять какую-либо функцию. Свойство живучести интерпретируется как выполнение заданной цели функционирования, т.е. выполнение заданного числа функций, в условиях возникновения и накопления функциональных отказов [2].

Введём понятие допустимой интенсивности отказов $\lambda' = \sum_{i=1}^{I} \lambda_i$. (показатель надёжности барьера [3]), при которой система способна в полной мере выполнить любую задачу из множества z_i^*. Под интенсивностью отказов системы защиты от НСД следует понимать количество обнаруженных в ней каналов НСД к информации в единицу времени. Численные значения данного параметра могут быть получены на основании статистики угроз НСД, которая приведена в [4].

Тогда под показателем живучести МЗ понимается коэффициент живучести МЗ, учитывающий как коэффициент стойкости МЗ, так и допустимую интенсивность отказов:

$$Srv_m\left(Z^*\right) = \lambda G_m(Z^*). \qquad (2)$$

Анализ живучести МЗ показывает, что при увеличении количества барьеров в составе МЗ увеличиваются верхний и нижний пределы границ живучести МЗ.

Под оценкой живучести КСЗИ понимается коэффициент живучести КСЗИ, который учитывает коэффициенты живучести механизмов защиты, входящих в КСЗИ, и коэффициент перекрытия между этими МЗ:

$$Srv_k(Z^*) = 1 - \left(\prod_{m=1}^{q} Srv_m(Z^*) C_f \right), \qquad (3)$$

где Srv_m – коэффициент живучести механизма защиты при выполнении задачи защиты Z^*; C_f – коэффициент перекрытия между механизмами защиты; q – количество механизмов защиты в составе КСЗИ.

Как показывает анализ живучести КСЗИ, представленный на рис. 2, при увеличении количества МЗ в составе КСЗИ увеличивается количество допустимых отказов – λ', при которых может эффективно работать КСЗИ.

Живучесть КСЗИ, как было проанализировано, в большой мере зависит от количества барьеров в составе МЗ и коэффициента перекрытия между МЗ.

2.2. Анализ максимального количества барьеров в составе механизма защиты КСЗИ

Неоднородность барьеров системы защиты информации значительно усложняет расчёт коэффициента живучести и требует чёткого различия полного и частичного отказов барьеров.

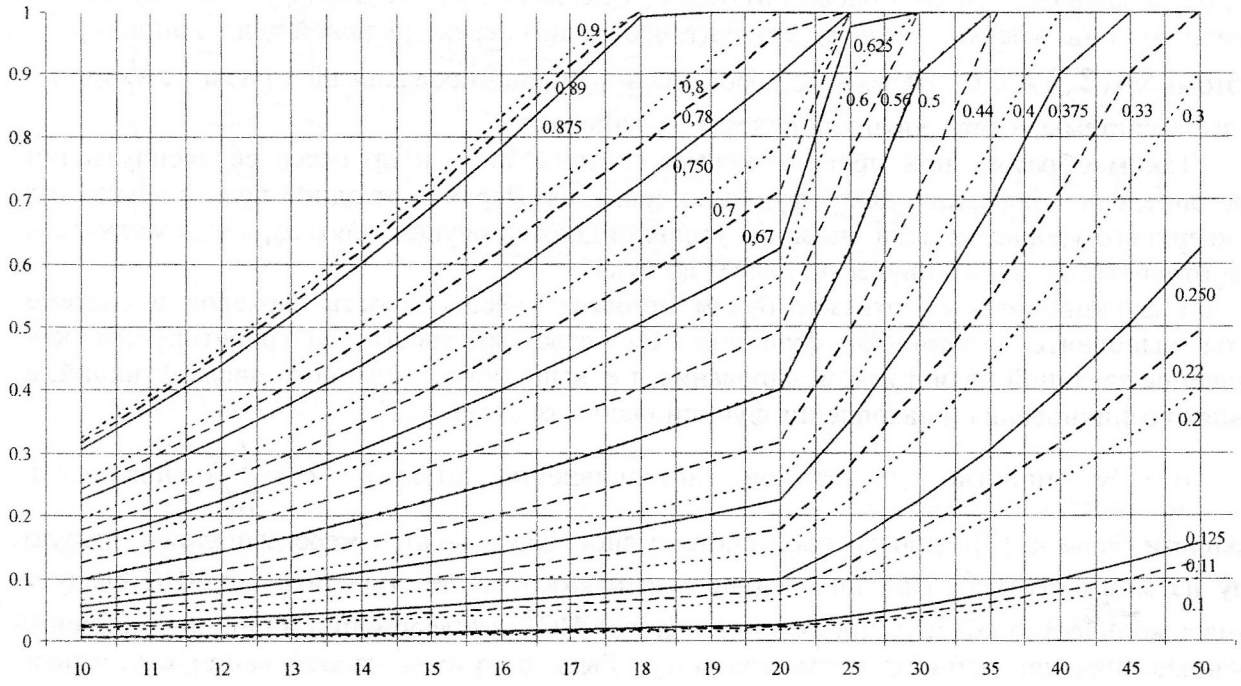

Рис.2. График *Srvk(Z*)* /λ' при *Gm*(1-9(10))=0,2-0,9; *Gm*(1-8(9))=0,22-0,89; *Gm*(1-7(8))=0,250-0,875; *Cf* = 10; *g*max=10 для КСЗИ, состоящей из двух МЗ

Перейдём к задаче построения функциональной структуры системы защиты информации с заданным коэффициентом живучести.

Предположим, что СЗИ G_1, построенная из g барьеров $\{b_1, b_2, ..., b_g\}$, ориентирована на решение задач из множества $Z = \{z_1, z_2, ..., z_k\}$, заданных над множеством элементарных функций $F = \{f_1, f_2, ..., f_m\}$, с коэффициентом перекрытия C_f.

Понятно, что увеличение коэффициента перекрытия не требует увеличения количества барьеров в СЗИ. Зададим коэффициент живучести системы G_1=Srv_1. Для решения задачи приравняем коэффициент живучести системы G_1 к нулю, т.е. Srv_1=0. Нам необходимо повысить живучесть системы, т.е., по существу, построить новую систему G_2 с коэффициентом живучести Srv_2>0.

Предположим, что для повышения живучести допустимо увеличение числа барьеров в СЗИ G_1 до числа N. При этом требуется достичь коэффициента живучести для λ', равного $Srv_2(\lambda') > 0$. В этом случае, исходя из определения коэффициента функциональной живучести (1), следует, что требуется добиться компенсации интенсивности отказов $-\lambda'$,

равной $g_{\max}\lambda'$. Так как предполагается, что возможен отказ любого из барьеров, то требование компенсации отказов означает компенсацию $N\times\lambda'$ отказов для любой элементарной функции из множества $F=\{f_1,f_2,...,f_m\}$. Таким образом, нам необходимо обеспечить компенсацию $Zg_{\max}\lambda'$ функциональных отказов.

Для этого необходимо $\dfrac{Zg_{\max}\lambda'}{C_f}$ барьеров.

Итак, новая СЗИ G_2 будет иметь g'_{max} барьеров, причём

$$g_{\max}=g+\frac{Zg'_{\max}\lambda'}{C_f}, \tag{4}$$

где g- число барьеров в системе G_1, откуда следует, что

$$g'_{\max}C_f=m\times g'_{\max}\lambda'+gC_f,$$
$$g'_{\max}(C_f-Z\lambda')=C_fg,$$
$$g'_{\max}=\frac{C_fg}{C_f-Z\lambda'}.$$

Но так как $g'_{\max}$ – число целое (число барьеров), то

$$g'_{\max}=\left[\frac{g}{1-\dfrac{Z\lambda'}{C_f}}\right]. \tag{5}$$

Имея g'_{max} барьеров, мы достигаем в системе G_2 коэффициента живучести, равного заданной величине. На рис.3–6 показано изменение значений максимального количества барьеров в МЗ при увеличении барьеров для повышения живучести КСЗИ. В результате можно сделать вывод, что если увеличивать количество барьеров в МЗ, при увеличении допустимой интенсивности отказов барьеров, в составе МЗ, наступает период насыщения, после которого кривая резко опускается на отрицательные значения и в дальнейшем стремится к нулю. Если же увеличивать количество коэффициентов перекрытия барьеров, то можно увеличить допустимое количество отказов в МЗ.

При объединении всех графиков и «обрезании» отрицательной составляющей графиков (т.к. они не берутся в расчёт) получим следующие зависимости, показанные на рис. 7:

из (5) следует, что при $\lambda=0\Rightarrow N=g$, что соответствует исходным предположениям, т.к.

$$g_{\max}>0,g>0,Z>0,\lambda'>0,C_f>0,$$
$$\text{то}\quad 1-\frac{Z\lambda'}{C_f}>0\Rightarrow\frac{Z\lambda'}{C_f}<1\quad\text{или}\quad\lambda'<\frac{C_f}{Z}; \tag{6}$$

из неравенства (6) следует, что верхний предел функциональной живучести СЗИ определяется двумя характеристиками системы: коэффициентом перекрытия системы – C_f и количеством элементарных функций – m.

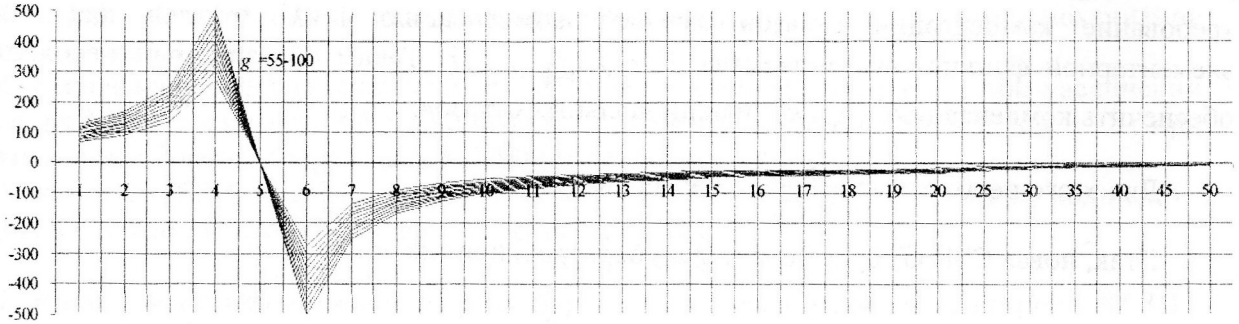

Рис. 3. График значений *g*max / λ' при *Z=10; *Cf* =1; *g* =55-100**

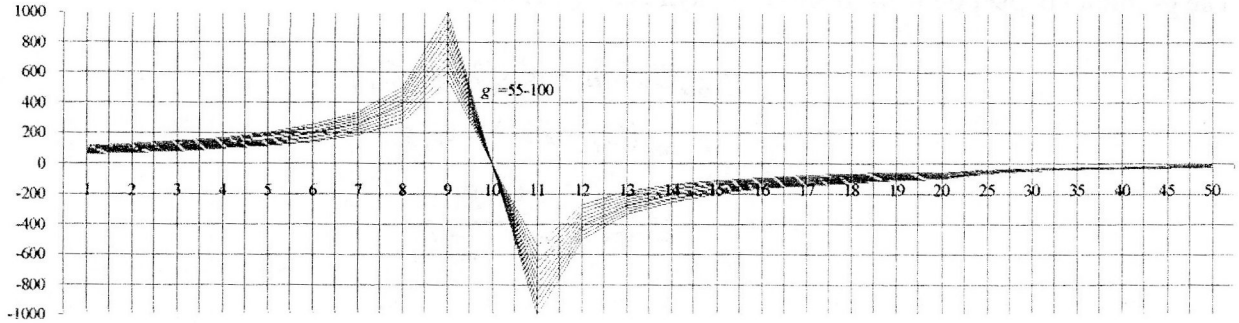

Рис. 4. График значений *g*max / λ' при *Z=10; *Cf* =2; *g* =55-100**

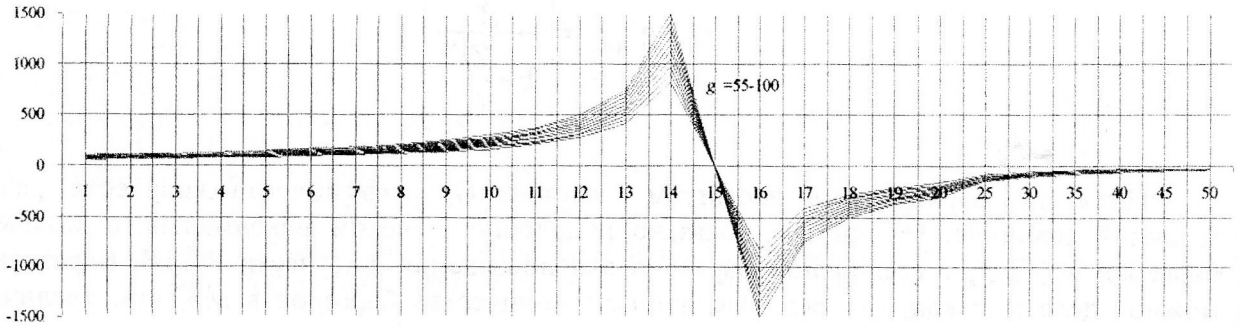

Рис. 5. График значений *g*max / λ' при *Z=10; *Cf* =3; *g* =55-100**

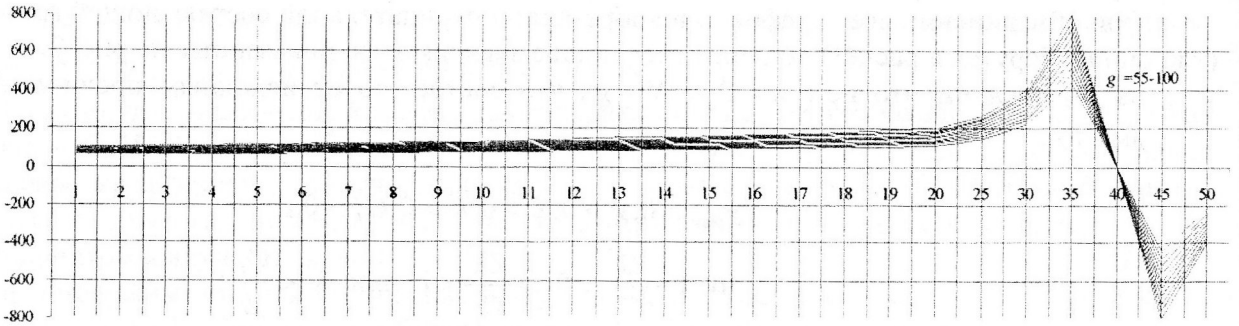

Рис. 6. График значений *g*max / λ' при *Z=10; *Cf* =8; *g* =55-100**

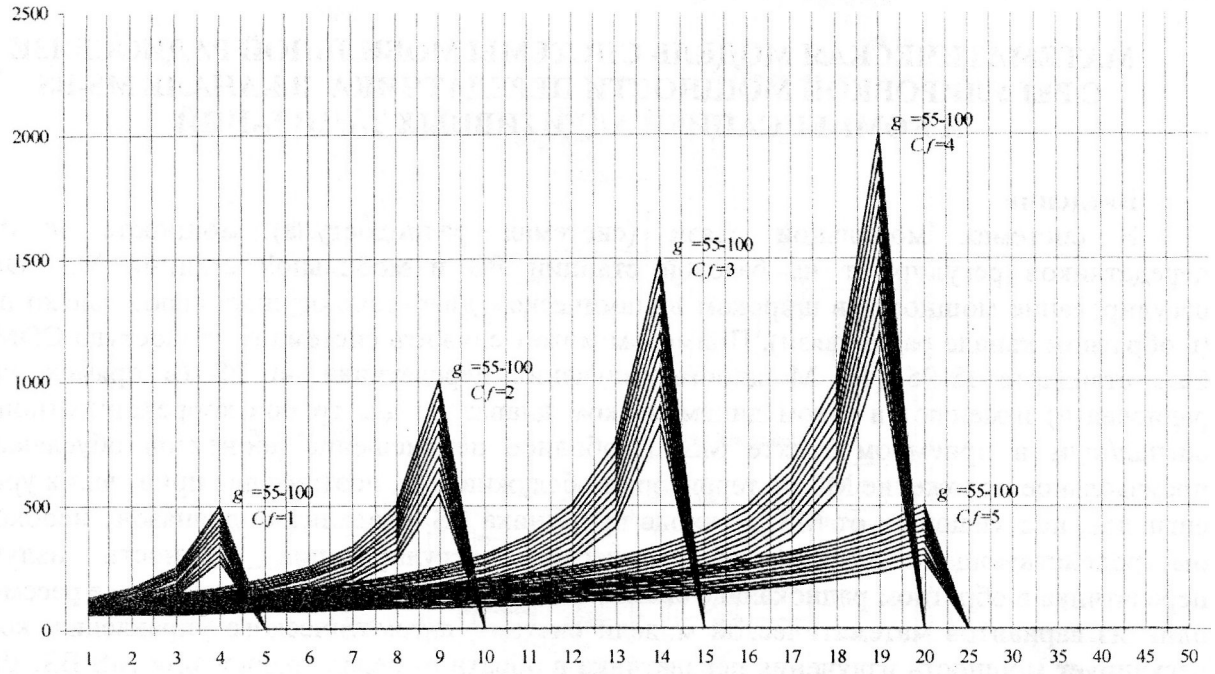

Рис. 7. Графики значений gmax / λ' при Z*=10; Cf =1-5; g =55-100

Таким образом, относительно любого множества задач, заданного над множеством элементарных функций – F, живучесть не может превысить C_f/Z. Более того, для того чтобы построить СЗИ с коэффициентом живучести, равным C_f/Z, необходимо взять бесконечное количество барьеров.

Оценка (6) не зависит от количества барьеров в СЗИ.

Верхняя оценка коэффициента живучести пропорциональна коэффициенту перекрытия и обратно пропорциональна числу элементарных функций (Z – характеризует множество задач, т.е. цель функционирования).

3. Выводы

Определив *коэффициент живучести как «часть» (долю) барьеров, отказы которых допустимы в СЗИ без ущерба для её функционирования*, было определено, что никакое количественное наращивание барьеров (т.е. дополнительное резервирование) не позволит достичь коэффициента живучести, большего, чем $\frac{C_f}{m}$. Повысить живучесть СЗИ можно путём повышения коэффициента перекрытия, что связано, прежде всего, с улучшением связности барьеров.

Список литературы

1. *Павлов И.Н.* Методика оценки количественных показателей живучести систем защиты информации // Збірник "Захист інформації". – К.: 2005. – № 4. – С. 5 – 14.

2. *Mead R.* Requirements Engineering for Survivable Systems // Puttsburgh. 2003.

3. *Горицкий В.М., Павлов И.Н.* Оценка вероятности безотказной работы комплексной системы защиты информации // Збірник "Зв'язок". – К.: 2005. – № 5. – С. 50 – 56.

4. *Ефимов А.И., Пальчун Б.П., Ухлинов Л.М.* Методика построения тестов проверки технологической безопасности инструментальных средств автоматизации программирования на основе их функциональных диаграмм // Вопросы защиты информации. – М.: 1995. – №3(30). – С.52 – 54.

Поступила 23.01.2006