УДК 681.324:004.621 **Орленко В.С., Тискина Е.О. Хорошко В.А.**

КРИТЕРИИ ДЛЯ ОЦЕНКИ ЖИВУЧЕСТИ ЦЕНТРАЛИЗОВАННЫХ И ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Введение

Применение и широкое внедрение средств вычислительной техники (микропроцессоров, микро-ЭВМ и одноплатных ЭВМ) в системы технической защиты информации позволяют децентрализовать функции управления и регулирования, которые до сих пор осуществляются центральной ЭВМ или центральным процессором. Кроме того одноплатные ЭВМ или микро-ЭВМ дают возможность возлагать на них разные системные функции, которые раньше выполнялись несколькими дискретными управляющими автоматами [1].

Путем децентрализации можно снизить опасность выхода из строя всей системы, так как в этом случае большая часть решающе-управляющей структуры остаётся работоспособной.

В технике управления процессами защиты теперь можно заменить независимые локальные исполнительные элементы на единое программируемое управление на современной элементной базе. Поэтому сейчас на первый план выходят вопросы живучести и надежности в целом системы и вероятности тотального отказа её, так как при выходе из строя центрального управляющего элемента (центральной ЭВМ) выполнение своих функций всей системой подвергается опасности.

Цель работы

Целью данной статьи является выявление и выработка критериев оценки для сравнения живучести централизованных и децентрализованных систем защиты информации (СЗИ). При этом, исходным пунктом рассуждения является вопрос, какие условия должны выполняться для централизованной СЗИ, чтобы относительно выбранных критериев достигалась равная с существующими системами из различных дискретных групп живучести.

Основная часть

Сравним децентрализованную структуру рис.1 и централизованную рис.2.

На рис.1 изображена система, состоящая из *n* независимых функциональных частей (подсистем), например из системы противодействия несанкционированному получению акустической информации; подавление побочных электромагнитных излучений и т.д.

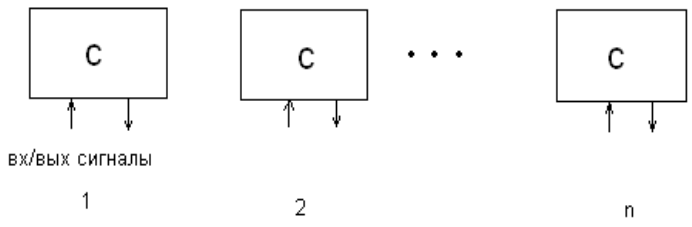

Рис.1 Децентрализованная структура с n подсистемами функционирования С

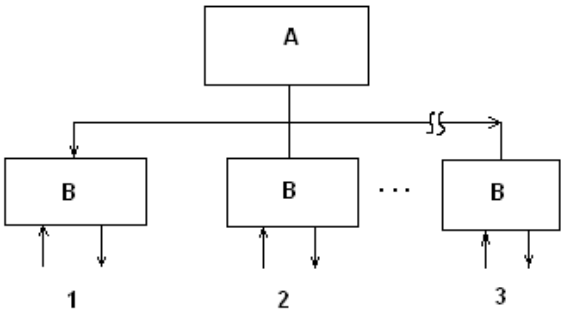

Рис.2 Централизованная структура с центральной системой А и периферийными подсистемами В

Полная несвязность данной системы представляет противоречащую практике изалязацию, которая должна упростить последующие рассуждения. В дальнейшем будем предполагать, что все n подсистем обладают приблизительно равными величинами живучести или надежности . Живучесть(надежность) характеризуется частотой отказов λ_c и частотой восстановления μ_c , которую можно определить из среднего времени ремонта t_r как:

$$\mu = \frac{1}{t_r} \tag{1}$$

На рис.2 показана централизованная структура причем в блоке А концентрируются элементы, вызывающие отказ всей структуры. Если схема на рис.2 использует микропроцессорную систему с шинной структурой, то блок А в основном состоит из процессора, памяти, памяти данных и памяти программ, шинных усилителей-формирователей, дешифраторов и блока питания.

Элементы подсистемы В представляют собой различные подсистемы защиты, которые обеспечивают защиту информации на объекте. Это аналогично структуре на рис.1 подсистемы с известными и равными друг другу числом входов и выходов, величины живучести (надежности) которые можно обозначить через $\lambda_в$ и $\mu_в$.

Зная величины λ и μ , можно для каждой функциональной структуры рис.1 и рис.2 рассчитать надежность V:

$$V = \frac{1}{1 + \lambda / \mu} \tag{2}$$

Это выражение представляет собой «непрерывную надежность» и указывает с какой вероятностью находится система в любой момент времени в работоспособном состоянии. В последующем выборе структуры необходимо анализировать величину живучести (надежности), полученную из данного выражения для централизованной и децентрализованной структур.

1. Среднее время между отказами (MTB F).

Если предположить, что для системы на рис.1 и рис.2 отказа подсистемы достаточно для непрерывного функционирования всей системы, то относительно рассмотренной живучести (надежности) систему можно представлять как логическую последовательность единичных подсистем. Общая частота отказов системы определяется суммой частот отказов отдельных компонентов [1,2], причем общая частота отказов является обратной величиной к ожидаемому усредненному времени между отказами MTBF .

В последующем индексом λ будем обозначать величины децентрализованной системы, а индексом Z – величины централизованной системы. Следовательно, получим:

$$MTBF_D = \frac{1}{n \cdot \lambda_c} \tag{3}$$

$$MTBF_Z = \frac{1}{\lambda_A + n \cdot \lambda_B} \tag{4}$$

Из этого очевидно централизованная и децентрализованная системы обладают равными временными интервалами между отказами, тогда имеет место отношение :

$$\lambda_A + n \cdot \lambda_B = n \cdot \lambda_C , \tag{5}$$

т.е., для случая неизбыточных систем "множество" единичных подсистем при равной технологии эквивалентно.

2. Живучесть (надежность) (V).

Если величину V можно отнести к выходу каждого элемента, то через выражение (2) можно прийти к понятию живучесть (надежность) [2].

Системная живучесть для децентрализованных и централизованных систем вытекает из живучести отдельных подсистем:

$$V_D = V_C^n , \tag{6}$$

$$V_Z = V_A \cdot V_B^n , \tag{7}$$

Величины V_D и V_Z представляют собой вероятности, с которыми все подсистемы общей системы в любой момент времени являются работоспособными. Равные величины живучести достигаются при выполнении соотношения:

$$V_A \cdot V_B^n = V_C^n , \tag{8}$$

Благодаря высокой степени интеграции современной элементной базы системы, она обладает лучшими MTBF и величиной живучести по сравнению с системой, смонтированной на дискретных элементах [3].

До настоящего времени для определения системной живучести (надежности) иерархическая организация системы не принималась во внимание. Однако во многих практических случаях из-за различного воздействия на процесс важно, на каком уровне иерархии находится подсистема. Например, для системы рис.2 отказ блока А делает невозможным дальнейшее протекание процесса, в то время как отказ одного элемента В вполне может допустить дальнейшую ограниченную работу.

Для дальнейшего рассмотрения необходимо предположить, что процесс управления можно разделить на ряд относительных но равных независимых комплексов управления, которые, смотря по обстоятельствам, могут управлять группами сигналов. При децентрализованной структуре (рис.1) каждый комплекс образуется подсистемой С, в то время как в централизованной системе (рис.2) комплексы управления образуются из восстановленных подсистем В и подсистемы А. В дальнейшем рассматриваем вопрос о возможности комплексного отказа (все комплексы управляются с ошибками) и о сравнительных возможностях управления при ожидаемом количестве ошибочно управляемых комплексов для той и другой структуры.

3. Вероятность комплексного (тотального) выхода из строя (P_n).

Ошибочное управление всех n управляющих комплексов является комплексным выходом из строя. Если можно ввести понятие ненадежности

$$U = 1 - V, \tag{9},$$

то вероятность комплексного (тотального) выхода из строя P_n при децентрализованной системе получается как продукт всех n ненадежностей U_C :

$$p_{nD} = U_C^n , \tag{10}$$

Для централизованной структуры комплексный отказ появляется при выходе из строя подсистемы А или при случайном отказе всех подсистем уровня В, или при наличии обоих этих событий. Для определения вероятности комплексного отказа важным является

предположение о независимости подсистем В, т.е. отказ подсистемы В не оказывает влияния на функционирование остальных подсистем. Отсюда вероятность комплексного (тотального) отказа можно записать [2]:

$$P_{nz}=V_A \cdot V_B^{\,n} + U_A \qquad (11)$$

для $V_A \approx 1$ получим

$$P_{nz} \approx U_B^{\,n} + U_A \qquad (12)$$

тогда при ровных вероятностях комплексного отказа ($P_{nd} = P_{nz}$) из условия

$$U_A + U_B^{\,n} \approx U_c^{\,n} \qquad (13)$$

следует

$$U_A < U_c^{\,n} \qquad (14)$$

т.е. ненадёжность централизованной подсистемы А должна быть в случае $P_{nd} = P_{nz}$ меньше, чем ненадёжность децентрализованной подсистемы в целом, что в практике достигается без избыточности уже для малых значений n.

4. Среднее количество ошибочно управляемых комплексов

Число ошибочно управляемых комплексов i (i=0, 1, 2, …, n) в случае децентрализации является идентичным с числом отказавших подсистем С. Т.е. величина вероятности отказа P_{id} управляющих комплексов определяется согласно формулы

$$P_{id} = \binom{n}{i} V_c^{\,n-i} (1- V_c)^{\,i}; \; i=0, 1, 2, \ldots, n. \qquad (15)$$

Это биноминальное распределение представлено на рис.3 для $V_c = 0{,}8$ и $n = 3$.

Из рис.3 видно, что для i>1 вероятность P_{id} сильно убывает. Средняя (ожидаемая) величина этого биноминального распределения рассчитывается по формуле

$$\overline{n_d} = n(1- V_c) \qquad (16)$$

и является для децентрализованной структуры средним количеством ошибочно управляемых комплексов.

При рассмотрении централизованных систем для i<n необходимо считать, что центральная подсистема А не отказывает, в противном случае все n управляющих комплексов будут выдавать неправильные выходные сигналы. Вероятность отказа i комплексов

$$P_{iz} = V_A \binom{n}{i} V_B^{\,n-i} (1- V_B)^{i}; \; i=0, 1, 2, \ldots, n. \qquad (17)$$

Случай i=n уже определяется как комплексный (тотальный) отказ.

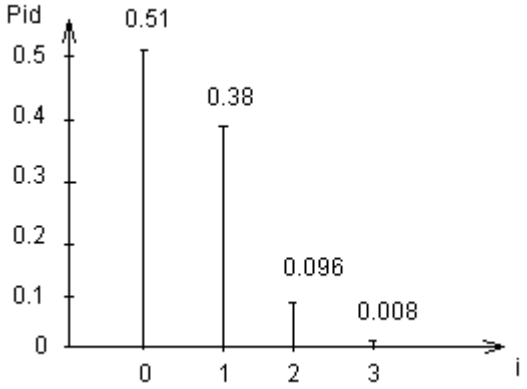

Рис.3 Величина вероятности P_{id} для ошибочного управления bi комплексах при децентрализованной структуре с надёжностью $V_c = 0{,}8$ и $n = 3$ комплексами.

Рис.4 представляет вероятность P_{iz} появления i ошибочно управляющих комплексов при величинах $V_A = V_B = 0{,}8$ и $n = 3$.

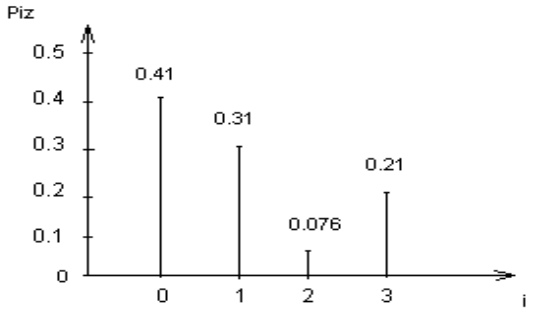

Рис.4 Величина вероятности P_{iz} для ошибочного управления bi комплексах при централизованной структуре с надёжностью V_A=0,8, V_B =0,8 и n =3 комплексами.

Из рис.4 видно, что вероятность P_{iz} для i<n легко сопоставима с вероятностью P_{id} благодаря предположению об неисправности подсистемы А, в то время как величина вероятности комплексного (тотального) отказа P_{nz} практически представляет собой ненадёжность блока А и коренным образом отличается от P_{nd}.

Средняя величина числа неправильно управляющих комплексов централизованной структуры определяется как

$$n_z = \sum_{i=1}^{n} i\cdot\overline{P_{iz}} = (1- V_A V_B) = U_A{}^n(1-V_B)+n(1- V_A) \qquad (18)$$

При сравнении этого выражения с формулой (16), становится ясным, что обе управляющие структуры являются эквивалентными относительно средней величины числа ошибочно управляющих комплексов при выполнении соотношения

$$V_A \times V_B = V_C \qquad (19)$$

Это соотношение получается из уравнений (13) и (14) при ровных вероятностях комплексного (тотального) отказа [3].

5. Средние потери $\overline{(v)}$

Определение средних потерь вытекает из условий практики, так как вероятность P_i может значительно отличаться от распределения на рис.3 и рис.4, с увеличением i увеличивается отличие. С целью устранения этого несоответствия каждой величине P_i(i=1, 2, …, n) придаётся весовой коэффициент ν (i) и средние потери определяется как

$$\overline{v} = \sum_{i=1}^{n} v(i)P_i \qquad (20)$$

Коэффициент ν(i) учитывает увеличение материальных убытков с ростом числа ошибочно управляющих комплексов. Считаем этот процесс линейным

$$\nu(i)=c\cdot i \qquad (21)$$

и учитываем его в формулах (16) и (18). Усреднение функции даёт возможность практичности правильно производить оценку ошибок определенного количества.

Выводы

Подбор приведённых величин, характеризующих живучесть (надёжность) является зависимым от каждого конкретного случая применения системы. Если систему необходимо рассмотреть в целом, и отказ элемента системы или подсистемы может возникнуть в любом месте, то предпочтение следует отдавать параметрам MTBF и V. Если есть возможность разбить систему на функционально независимые подсистемы с группами сигналов, то либо

рассматриваются данные о комплексном (тотальном) отказе, либо средняя величина характеристики отказов, либо обе величины вместе.

Предпочтительные результаты даёт переход к системам с центральным вычислительно-управляющим блоком на децентрализованных подсистемах. Здесь рассматривается специфические проблемы живучести (надёжности) и частоты ошибок при передаче информации в пространственных структурах с распределёнными сетями.

Список литературы

1. *Козлова К.В.* – Кількісна оцінка захисту радіоелектронних об'єктів / Козлова К.В., Хорошко В.О. // Захист інформації. – № 1, 2007. – с. 30-38.

2. *Гурина С.А.* – Живучесть систем защиты в условиях внешних воздействий / Гурина С.А., Егоров Ф.И., Хорошко В.А. // Захист інформації. – № 2, 2008. – с. 69-78.

3. *Тискина Е.О.* Выбор критерия для оптимизации технической системы защиты информации / Тискина Е.О., Хорошко В.А. // Системи обробки інформації, вип.. 7 (79), 2009. – с. 90-93.

Поступила 23.03.2010

УДК 004.73

Дудикевич В.Б., Гарасим Ю.Р.

МЕТОД ЗАГАЛЬНОГО РЕЗЕРВУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Система захисту інформації в ЗКМЗ повинна мати властивість живучості. Це зумовлене тим, що припинення функціонування СЗІ ЗКМЗ внаслідок дії ДФ (як внутрішніх, так і зовнішніх) призводить до великих економічних втрат або катастрофічних наслідків через реалізацію загроз конфіденційності, доступності та цілісності інформації, яка в них функціонує.

Живучість (survivability) системи захисту інформації в ЗКМЗ передбачає її здатність зберігати та виконувати встановлений обсяг власних цільових функцій у відповідному середовищі з врахуванням різних зовнішніх та внутрішніх ДФ, що можуть призводити до відмов її функціональних елементів за рахунок відповідної зміни структури і поведінки системи, зберігаючи мінімально допустимий рівень якості функціонування відповідно до встановлених рівнів деградації із подальшим відновленням початкового ефективного функціонування протягом встановленого часу.

Мета і задачі дослідження

Метою роботи є дослідження доцільності використання методу постійного загального резервування системи захисту інформації ЗКМЗ при різних варіантах набору кількості функціональних елементів системи та кількості систем резервування із врахуванням вартості запровадження відповідного рішення. Для досягнення поставленої мети в роботі вирішуються наступні завдання: 1) класифікація можливих методів резервування СЗІ ЗКМЗ; 2) визначення параметрів живучості СЗІ ЗКМЗ; 3) дослідження математичної моделі оцінки живучості СЗІ ЗКМЗ; 4) визначення методів та засобів забезпечення живучості СЗІ ЗКМЗ при її загальному резервуванні.

Об'єктом дослідження є система захисту інформації в захищених корпоративних мережах зв'язку, що складається з великої кількості гетерогенних обчислювальних вузлів, сенсорів та каналів передавання даних і встановленого проміжного програмного забезпечення захисту інформації.