УДК 004.42:004.056

Л. К. Птицына, А. В. Птицын

ПРЕОДОЛЕНИЕ НЕОПРЕДЕЛЕННОСТИ ОТНОСИТЕЛЬНО ДИНАМИЧЕСКИХ ПРОФИЛЕЙ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Выделяются типовые приемы комплексирования программно-аппаратных средств в комплексных системах защиты информации, формируется математический базис для определения их динамических характеристик.

Ключевые слова: комплексные системы защиты информации, принципы параллельности, профили, динамические характеристики, точность оценивания, функция распределения.

Применение принципа мультиплексирования при организации комплексных систем защиты информации предоставляет широкие возможности совершенствования архитектуры с целью повышения эффективности их функционирования. Преимущества мультиплексирования могут раскрыться в наибольшей степени, если параллельная работа программных и аппаратных средств обеспечения информационной безопасности организуется не только при обнаружении возможных угроз, но и при проведении необходимых мероприятий по защите информации. Планирование эффекта от подобных действий становится возможным в случае преодоления неопределенности относительно динамических профилей комплексных систем защиты информации в условиях параллельной работы средств. В связи с этим появляется объективная необходимость определения динамических характеристик систем защиты информации при комплексировании программно-аппаратных средств. Распространенные в настоящее время приемы преодоления указанной неопределенности сводятся к оцениванию динамических характеристик в процессе функционирования комплексных систем защиты информации, когда изменения в их конфигурации ограничены возможностями выбранной архитектуры. В то же время, неопределенность игнорируется при выборе их архитектуры. Для устранения подобной проблемной ситуации предлагается формальный подход к определению динамических характеристик комплексных систем защиты информации, который опирается на математический аппарат анализа распределенных процессов в части моделирования механизмов их синхронизации [1].

Ориентируясь на практическую значимость, в качестве динамических характеристик выбираются средние времена защиты информации.

Возможные способы комплексирования отдельных средств обеспечения защищенности данных основываются на различных сочетаниях типовых вариантов их согласованного функционирования:

– параллельное функционирование аппаратных средств;

– параллельное функционирование программных средств;

– параллельное функционирование программных и аппаратных средств.

Применительно к перечисленным типовым вариантам осуществляется определение выбранных показателей качества защиты информации.

Среди известных принципов объединения результатов параллельного функционирования отдельных средств широко распространены принципы И-параллельности и ИЛИ-параллельности, выбор каждого из которых обусловливается спецификой функционального назначения комплексируемых средств. По этой причине при определении среднего времени защиты информации учитывается характер процедур объединения частных результатов, описываемый с помощью логических функций «И» ($\wedge$), «ИЛИ» ($\vee$).

Выполним определение искомых показателей на случай параллельного функционирования аппаратных средств. Пусть каждое *n*-е аппаратное средство обеспечивает такое выполнение возлагаемых задач, при котором среднее время защиты информации характеризуется величиной $T_{n,P}$. Принимая гипотезу об экспоненциальном распределении времени защиты, находим вероятность того, что все необходимые мероприятия будут реализованы в промежутке времени $(0, t_k)$:

$$W_n(t_k) = 1 - e^{-t_k / T_{n,P}}. \qquad (1)$$

После нахождения функции распределения времени окончания *N* параллельно выполняемых функциональных процессов в условиях применения принципа И-параллельности, получим следующее соотношение для среднего времени защиты информации T_P:

$$T_P \approx \Delta t \sum_{k=1}^{K} k \left[\prod_{n=1}^{N} W_n(t_k) - \prod_{n=1}^{N} W_n(t_{k-1}) \right], \qquad (2)$$

$$\Delta t = t_k - t_{k-1}, \qquad k = 1, 2, ..., K,$$

где Δt – интервал обновления результатов работы аппаратных средств защиты информации.

В соотношении (2) переменная *K* представляет наименьшее значение, удовлетворяющее неравенству

$$1 - \sum_{k=1}^{K} \left[\prod_{n=1}^{N} W_n(t_k) - \prod_{n=1}^{N} W_n(t_{k-1}) \right] \le \varepsilon, \qquad (3)$$

где *N* – число параллельно работающих аппаратных средств.

В соотношении (3) величина ε представляет собой вероятность события, при котором время защиты информации превышает граничное значение, равное $K\Delta t$.

Через функцию распределения времени окончания N параллельно выполняемых функциональных процессов в условиях применения принципа ИЛИ-параллельности находим среднее время защиты информации для второго типового случая:

$$T_P \approx \Delta t \sum_{k=1}^{K} k \left[\prod_{n=1}^{N} \left(1 - W_n(t_{k-1})\right) - \prod_{n=1}^{N} \left(1 - W_n(t_k)\right) \right], \quad (4)$$

где K – наименьшее целое значение, удовлетворяющее неравенству

$$1 - \sum_{k=1}^{K} \left[\prod_{n=1}^{N} \left(1 - W_n(t_{k-1})\right) - \prod_{n=1}^{N} \left(1 - W_n(t_k)\right) \right] \le \varepsilon. \quad (5)$$

Проанализируем случай параллельного действия программных средств защиты информации. В соответствии с характерными особенностями функционирования программных средств, раскрытыми в [2], n-й подпроцесс защиты информации, включающий M этапов, описывается полумарковской моделью, позволяющей получить выражение для определения среднего времени защиты информации:

$$T_{n,P} = \frac{\left[\prod_{m=1}^{M-1} (1 - \mathrm{P}_{n,m}) \right] \sum_{m=1}^{M} t_{n,m}}{1 - \prod_{m=1}^{M} (1 - \mathrm{P}_{n,m})} + \frac{t_{n,1} \left[1 - \prod_{m=1}^{M-1} (1 - \mathrm{P}_{n,m}) \right] + \sum_{m=2}^{M-1} \left\{ t_{n,m} \left[\prod_{j=1}^{m-1} (1 - \mathrm{P}_{n,j}) \left(1 - \prod_{K=m}^{M-1} (1 - \mathrm{P}_{n,\kappa}) \right) \right] \right\}}{1 - \prod_{m=1}^{M} (1 - \mathrm{P}_{n,m})} + \frac{\sum_{m=1}^{M} \mathrm{P}_{n,m} t_{\acute{K},n,m} \prod_{k=1}^{m-1} (1 - \mathrm{P}_{n,k})}{1 - \prod_{m=1}^{M} (1 - \mathrm{P}_{n,m})}. \quad (6)$$

В указанной модели случайные длительности отдельных этапов контроля информационных процессов при функционировании n-го программного средства защиты представляются математическими ожиданиями $t_{n,m}$, $m = \overline{1,M}$. Причем на каждом из этапов предусматривается возможное обнаружение появляющейся угрозы с вероятностью $P_{n,m}$, $m = \overline{1,M}$.

После подстановки соотношения (6) в формулу (1) математическое ожидание времени защиты информации в комплексной системе определяется по формулам (2), (3) в условиях И-параллельности и по формулам (4), (5) в случае ИЛИ-параллельности.

Рассмотрим порядок определения динамических характеристик систем защиты информации при параллельной работе программно-аппаратных средств. По найденным функциям распределения $W_n(t_k)$, $n = 1, 2, ..., N$ на основании соотношений (2), (3) образуется следующее представление искомой оценки при реализации принципа И-параллельности:

$$T_P \approx \Delta t \sum_{k=1}^{K} k \left[\left(\prod_{n=1}^{N_S} W_n(t_k) \right) \left(\prod_{n=1}^{N_H} W_n(t_k) \right) - \left(\prod_{n=1}^{N_S} W_n(t_{k-1}) \right) \left(\prod_{n=1}^{N_H} W_n(t_{k-1}) \right) \right], \quad (7)$$

$$1 - \sum_{k=1}^{K} \left[\left(\prod_{n=1}^{N_S} W_n(t_k) \right) \left(\prod_{n=1}^{N_H} W_n(t_k) \right) - \left(\prod_{n=1}^{N_S} W_n(t_{k-1}) \right) \left(\prod_{n=1}^{N_H} W_n(t_{k-1}) \right) \right] \le \varepsilon, \quad (8)$$

где N_S – число программных средств; N_H – число аппаратных средств; $N = N_S + N_H$ – общее число комплексируемых средств; $W_n(t_k)$, $n = 1, 2, ..., N_S$ – функции распределения, характеризующие качество защиты информации с применением программных средств; $W_n(t_k)$, $n = 1, 2, ..., N_H$ – функции распределения, представляющие качество защиты информации при использовании аппаратных средств.

Неравенство (8) предназначается для выбора значения K по заданному уровню ε.

В соответствии с формулами (4), (5) среднее время защиты информации в случае параллельного функционирования программных и аппаратных средств, результаты работы которых объединяются с применением логической функции «ИЛИ», выражается следующим образом:

$$T_0 \approx \Delta t \sum_{k=1}^{K} k \left[\left(\prod_{n=1}^{N_S} \left(1 - W_n(t_{k-1})\right) \right) \left(\prod_{n=1}^{N_H} \left(1 - W_n(t_{k-1})\right) \right) - \left(\prod_{n=1}^{N_S} \left(1 - W_n(t_k)\right) \right) \left(\prod_{n=1}^{N_H} \left(1 - W_n(t_k)\right) \right) \right], \quad (9)$$

$$1 - \sum_{k=1}^{K} \left[\left(\prod_{n=1}^{N_S} \left(1 - W_n(t_{k-1})\right) \right) \left(\prod_{n=1}^{N_H} \left(1 - W_n(t_{k-1})\right) \right) - \left(\prod_{n=1}^{N_S} \left(1 - W_n(t_k)\right) \right) \left(\prod_{n=1}^{N_H} \left(1 - W_n(t_k)\right) \right) \right] \le \varepsilon. \quad (10)$$

Верхняя граница для переменной k представляет собой наименьшее значение K, которое удовлетворяет неравенству (10). В данном случае задаваемая величина ε является вероятностью того, что время защиты информации при комплексировании программно-аппаратных средств по принципу ИЛИ-параллельности превышает верхнюю границу $K\Delta t$.

Благодаря использованию неравенств (3), (5), (8), (10) обеспечивается возможность регулирования степени приближения оценок (2), (4), (7), (9) к реальным значениям математических ожиданий времен защиты информации.

Выражения (1)–(10) образуют базис соотношений для получения приближенной количественной оценки показателей качества систем защиты информации при комплексировании программно-аппаратных средств по принципу И- и ИЛИ-параллельности с регулируемой степенью приближения.

Таким образом, формализация процесса преодоления неопределенности относительно динамических профилей комплексных систем защиты информации, основанная на системе выведенных аналитических соотношений, обеспечивает планирование их качества при выборе архитектуры.

Библиографические ссылки

1. Птицына Л. К., Соколова Н. В. Программное обеспечение компьютерных сетей. Моделирование механизмов синхронизации параллельных вычислительных процессов в системах мониторинга и управления : учеб. пособие. СПб. : Изд-во Политехн. ун-та, 2010.

2. Птицына Л. К., Птицын А. В. Архитектура ЭВМ и систем. Модели и методы анализа динамических характеристик программных систем защиты информации : учеб. пособие. СПб. : Изд-во Политехн. ун-та, 2007.

L. K. Ptitsyna, A. V. Ptitsyn

OVERCOMING OF UNCERTAINTY OF DYNAMIC PROFILES OF COMPLEX SYSTEMS OF PROTECTION OF THE INFORMATION

Typical modes of hardware-software means complexing in complex systems of protection of the information are allocated, the mathematical basis for definition of their dynamic characteristics is formed.

Keywords: complex systems of protection of the information, parallelism principles, profiles, dynamic characteristics, accuracy of estimation, distribution function.

УДК 681.3.004.8

В. А. Филимонов

УЧЕБНО-ИССЛЕДОВАТЕЛЬСКИЙ СИТУАЦИОННЫЙ ЦЕНТР – ПОЛИГОН ДЛЯ КОМАНДЫ СИСТЕМНЫХ АНАЛИТИКОВ

Рассматриваются учебно-исследовательские ситуационные центры как инфраструктура для реализации процессов коллективного исследования, проектирования и обучения. Предложены варианты построения прототипов, схема «4 уровня» для рассмотрения объектов. Описана технология подготовки сервисных команд для ситуационных центров. Приведен обзор некоторых проектов, реализованных в Омске в 2005–2010 гг.

Ключевые слова: ситуационный центр, сервисная команда, рефлексивный анализ.

Рассматриваемой проблемой является отсутствие теории подготовки команд системных аналитиков и соответствующих систем подготовки таких команд. Объектом исследований являются системы коллективной деятельности: исследовательской, проектной и учебной.

Комплекс задач и подходы к решению. Указанный выше коллектив будем далее называть проектной группой. Нами сформулирован следующий комплекс задач [1]. Проектная группа решает *задачу 1*: создает проект, которым, в частности, может быть представление (теория, модель и т. п.) о некотором объекте исследования. Предполагая, что работу проектной группы обеспечивают технические средства и сервисная команда, приходим к *задаче 2*: создание (виртуальной) технологии оптимальной поддержки всего жизненного цикла постановки и решения задачи 1. Далее возникает *задача 3* – создание инфраструктуры (машины, комплекса), в которой формируются технологии, указанные в задаче 2. Создание технологии требует постановки *задачи 4* – подготовки специалистов по решению перечисленных задач (как учить) и *задачи 5* – создания собственной технологии для решения задачи 4 (как учить учителей).

В качестве инфраструктуры нами используются учебно-исследовательские ситуационные центры (СЦ). Сам термин «ситуационный центр» уже является достаточно распространенным. В частности, в поисковых машинах на соответствующий запрос выдается от 60 000 до 600 000 ссылок. Мы будем понимать СЦ как пространство, предназначенное для динамического коллективного формирования образа ситуации, объекта, процесса, обеспеченное ключевыми, т. е. критическими относительно решаемой задачи, ресурсами [2]. Основные отличия учебного аспекта СЦ от исследовательского заключаются в следующем:

– преимущественное внимание уделяется изучению методов, а не рассмотрению информации, относящейся к определенной задаче;