УДК 004.056

ОБ ОДНОМ ПОДХОДЕ ОЦЕНКИ НАДЕЖНОСТИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Алиева Фарида

Институт Систем Управления Национальной Академии Наук Азербайджана

Аннотация

Данная статья посвящена вопросам, оценки надежности системы обеспечения безопасности в компьютерных системах. В статье рассмотрен и изложен один подход оценки надежности системы безопасности. Данный подход основан на определении уровня контролируемости выполнения программ и обрабатываемых ими данных.

Abstract

This article is devoted to the issues of evaluating the reliability of the security system in computer systems. The article considers and describes one approach to assessing the reliability of the security system. This approach is based on determining the level of control over the execution of programs and the data processed by them.

Введение

В качестве системы обеспечения безопасности (СОБ) для компьютерных сетей будем рассматривать программно-технический комплекс защиты информационных ресурсов и инфраструктур, в рамках которых эти ресурсы существуют, обрабатываются и передаются. СОБ состоит из множества отдельно разработанных, но совместно используемых методов и средств обеспечения безопасности [1-3].

СОБ, как и другие компоненты компьютерных систем и сетей является объектом атак. Поэтому необходимо также защищать ее безопасность, что требует держать под контролем работу СОБ.

Исходя из вышесказанного, данная статья посвящена вопросам оценки надежности программного обеспечения, в том числе, системы обеспечения безопасности компьютерных систем и сетей.

Понятие контролируемости вычислительного процесса

Учитывая, что надежность СОБ характеризуется ее способностью осуществлять контроль за защищаемыми программно-техническими средствами, вычислительными процессами и данными. В этом смысле оценка надежности СОБ напрямую связана с решением задачи обеспечения контроля одного вычислительного процесса, программно-технического ресурса или человека со стороны другого [4,5].

Понятие контроля вычислительного процесса (ВП) можно сформулировать путем описания в виде следующей структуры символьных записей:

<ВП > (исходные данные)=<поименованные результаты работы ВП >

В качестве вычислительного процесса рассмотрим некоторую программу, защищаемую программно-техническими модулями СОБ. Пусть B – имя защищаемой программы, A – имя контролирующей программы (модуля СОБ), $F(t)$ - результат работы программы A на момент времени t.

Положим, что программа A контролирует работу программы B, и она в состоянии получить доступ к промежуточным и конечным результатам программы B.

Согласно предложенной структуре записи получим следующее выражение:

$$B = F(t) \qquad (1)$$

Результатами работы программы B является следующее:

- $F(t_1)$ ="text.doc" – файл, документ, созданный на MS WORD с именем "text.doc";
- $F(t_2)$ ="password" – символьный пароль, вводимый пользователем с клавиатуры в момент времени t_2.

Факт контроля работы программы B со стороны программы A может быть записан следующим образом:

$$B^A = F(t) \tag{2}$$

Если программа A контролирует работу программы B, то отсюда следует, что результатом обработки для программы A являются исходные, промежуточные и результирующие данные программы *B*, а также сама программа B, то есть

$$B^A = F(t) \Rightarrow A(B, F(t)) = F_1(t) \tag{3}$$

где $F_1(t)$ – возможный результат преобразования данных F программой A.

Факт НСД может быть записан в виде (3), где B - программа, которая осуществляет обработку исходных данных и получение результата $F(t)$, для $t > 0$, A - программа, которая в случае появления данных F осуществляется НСД, то есть получает несанкционированную копию $F_1(t)$.

В случае, если работу программы контролирует СОБ, главной задачей которой является обеспечение информационной безопасности, процесс программного взаимодействия может быть записан в виде:

$$B^{A<\text{СОБ}>} = F(t) \Rightarrow A^{<\text{СОБ}>}(B, F(t)) = F_1(t) \Rightarrow <\text{СОБ}>(F_1(t)) = F_2(t) \tag{4}$$

Под степенью контроля будем понимать число процессов, контролирующих исходный процесс, который можно записать в следующем виде

$$B^{A^{A^{\cdots A^A}}} \quad \text{или} \quad B^{Ak}.$$

Если одну и ту же программу контролируют две разные программы и порядок контроля нам не известен, то будем записывать в виде $B^{A,C}$. Если в B^{Ak} параметр k стремится к бесконечности, то будем считать, что программа A осуществляет полный или тотальный контроль, за работой программы B.

Контроль вычислительного процесса может быть осуществлен различными способами, и степень контроля k ничего не говорит о том, какие и сколько команд исполняемого модуля контролируются. СОБ, получив управление, может проанализировать от одной до всех команд исполняемого кода по любому адресу оперативной памяти.

Оценка качества контроля и надежности СОБ

Поэтому необходимо ввести еще одну характеристику - качества контроля. Под качеством контроля будем понимать отношение веса контролируемых команд к общему весу команд в теле контролируемого модуля:

$$w = \frac{W(A(B))}{W(B)}, \tag{5}$$

где $W(B)$ - вес всех команд в модуле B; $W(A(B))$ - вес контролируемых команд в программе B программой A. Вес блока команд характеризует возможности данного блока команд, связанные с воздействием на внешнюю программно-аппаратную среду данной программы.

Значение параметра качество контроля отражает вероятность того, что контролирующая программа отследит факты НСД (попытки проникновения или несанкционированного копирования).

Учитывая вышесказанную, определим вероятность выявления СОБ факта НСД учетом следующих исходных данных: k - степень контроля со стороны СОБ, w - качество контроля СОБ, l - степень контроля со стороны НСД. По следующей формуле можно определить контроль, осуществляющий СОБ:

$$P_l = \frac{k}{k+1} \tag{6}$$

Вероятность выявления СОБ факта НСД с учетом (6) составит

$$P(СОБ) = \frac{k \times w}{k+1} \tag{7}$$

Понятно, что увеличение степени и качества контроля существенно замедляет работу контролируемой программы. Поэтому главная задача разработчика СОБ заключается в нахождении для любого факта НСД таких, минимальных k и w, при которых можно было бы с определенной вероятностью Р гарантировать безопасность программы $B(1)$, то есть

$$B^{X,Zk} \overset{k+1}{\Longrightarrow} 0$$

В данном выражении $k+1$ - обозначает, что речь идет о результатах, которые могут быть получены после работы $k+1$ контролирующей программы.

Заключение

Таким образом, работа посвящена вопросам, оценки надежности системы обеспечения безопасности в компьютерных системах. В работе рассмотрен и изложен один подход оценки надежности системы безопасности. Данный подход основан на определении уровня контролируемости выполнения программ и обрабатываемых ими данных. А именно только в случае известности уровня контролируемости работы можно сказать о надежности программного обеспечения, в том числе СОБ. Можно предположить, что чем выше вероятность выявления СОБ факта НСД, тем она является более надежной.

Список использованных источников

1. Гроувер Д. Защита программного обеспечения. – М.: Радио и связь, 1992. -286 с.
2. Шураков В.В. Надежность программного обеспечения систем обработки данных. М.: Статистика. 1981. - 216 с.
3. Липаев В.В. Надёжность программных средств. М.: СИНТЕГ, 1998. - 232 с.
4. Романюк С. Г. Оценка надежности программного обеспечения. // Открытые системы. СУБД. 1994. № 04. https://www.osp.ru/os/1994/04/178540/
5. Степович-Цветкова Г.С. Оценка надежности программного обеспечения посредством применения функционального подхода. Инженерный вестник Дона, №3, 2015.