УДК 51.004

К ВОПРОСУ ОБ ИНФОРМАЦИОННОЙ СТРУКТУРЕ ПРОЦЕССА РАСПРЕДЕЛЕНИЯ ВРЕМЕННОГО РЕСУРСА МЕЖДУ РАЗНОТИПНЫМИ СРЕДСТВАМИ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

[1]Кочедыков С.С., [1]Кравченко А.С., [2]Родин С.В., [2]Перминов Г.В., [1]Душкин А.В.

[1]ФКОУ ВПО «Воронежский институт ФСИН России», Воронеж, e-mail: a_dushkin@mail.ru;

[2]ФГОУ ВПО «Воронежский институт МВД России», Воронеж, e-mail: irosvment@mail.ru

Так как существует некоторое многообразие источников угроз несанкционированного доступа к информации, обрабатываемой в информационно-телекоммуникационных системах различного назначения, а также некоторое многообразие средств защиты информации, обусловленных использованием принципиально различных механизмов защиты информации, это приводит к несогласованному, а в некоторых случаях неэффективному использованию таких средств защиты. С целью устранения такого рода противоречий предлагается подход, обеспечивающий совместное использование разных по типу средств защиты информации за счет решения задачи оптимального распределения временного ресурса, отвлекаемого от вычислительного ресурса информационно-телекоммуникационной системы. В качестве оценки средств защиты информации от несанкционированного доступа используется вероятностный подход. Наиболее удобной формой получения этих вероятностей является имитационное моделирование процессов обработки информации в информационно-телекоммуникационной системе с учетом значимости (важности) задач защиты информации, определяемой с использованием методов экспертной оценки.

Ключевые слова: информационно-телекоммуникационная система, защита информации, несанкционированный доступ, математическая модель, процесс

TO THE QUESTION OF INFORMATION OF THE STRUCTURE TIME ALLOCATION OF RESOURCES BETWEEN DIFFERENT TYPES OF MEANS OF PROTECTION AGAINST UNAUTHORIZED ACCESS

[1]Kochedykov S.S., [1]Kravchenko A.S., [2]Rodin S.V., [2]Perminov G.V., [1]Dushkin A.V.

[1]Voronezh Institute of the Federal penitentiary service of Russia, Voronezh, e-mail: a_dushkin@mail.ru;

[2]Voronezh Institute of the Ministry of internal Affairs of Russia, Voronezh, e-mail: irosvment@mail.ru

Considering that there are a variety of sources of threats unauthorized access to information processed in information and telecommunication systems for various applications, and the availability to some variety of means of information protection, due to the use of fundamentally different mechanisms of information protection, leads to inconsistent, and in some cases inefficient use of such remedies. To resolve such contradictions, we propose an approach for joint use of different means of information protection at the expense of solving the problem of optimum allocation of time resources, we distract from the computing resource of information and telecommunication systems. As assessment of information protection from unauthorized access uses a probabilistic approach. The most convenient form of obtaining these probabilities is a simulation of the processes of information processing in information and telecommunications system in view of the importance of the task of protection of the information defined using the methods of expert evaluation.

Keywords: information-telecommunications system, protect information, unauthorized access, mathematical model, process

Анализ результатов информатизации всех сфер общественной жизни свидетельствуют о подавляющем количестве средств обработки информации и средств ее обмена в информационно-телекоммуникационных системах (ИТКС). Вместе с тем увеличение объемов обрабатываемой в ИТКС информации приводит к возрастанию угроз их информационной безопасности, в том числе и угроз несанкционированного доступа (НСД), что, в свою очередь, приводит к необходимости обеспечения защиты процессов, связанных с обработкой информации. Выработка мер защиты информации, адекватных угрозам обрабатываемой информации в ИТКС, привела к разработке соответствующих средств защиты информации (СЗИ), в том числе от НСД. Вместе с тем многообразие источников угроз НСД к информации в ИТКС и разнотипность СЗИ, обусловленная использованием принципиально различных механизмов защиты информации, приводят к несогласованному, а в некоторых случаях неэффективному использованию СЗИ.

С целью устранения такого рода противоречий предлагается методический подход, обеспечивающий совместное использование разнотипных СЗИ за счет решения ряда частных оптимизационных задач, связанных с минимизацией отвлечения вычислительного ресурса ИТКС путем его распределения между разнотипными СЗИ исходя из их потенциальных возможностей по реализации задач защиты информации.

С целью решения задачи математического моделирования противодействия НСД к ИТКС разнотипными СЗИ, в условиях минимизации отвлечения вычислительного ресурса этих систем, как задачи оптимального распределения ресурса по способам организации защиты информации от НСД необходимо определить целевую функцию и функцию ограничения. В основу алгоритма определения ограничений положена гипотеза о том, что возможности средств защиты информации того или иного типа определяются исходя из частоты их использования и значимости.

Это приводит к необходимости оценки соответствующих возможностей средств защиты информации того или иного типа. В качестве такой оценки предлагается использовать частотную характеристику процесса защиты информации от НСД в ИТКС при ее обработке. В дальнейшем в качестве такой характеристики условимся использовать вектор $\vec{W}$ вероятностей выполнения задач защиты информации от НСД средствами защиты информации придаваемого и встраиваемого типа, формально представляемый в виде

$$\vec{W} = (w_1, w_2),$$

где w_1 – вероятность выполнения задач защиты информации от НСД средствами защиты информации придаваемого типа, а w_2 – вероятность выполнения задач защиты информации от НСД средствами защиты информации встраиваемого типа.

С учетом того, что данные вероятности описывают полную группу событий будет справедливым условие

$$w_1 + w_2 = 1.$$

Наиболее удобной формой получения этих вероятностей является имитационное моделирование процессов обработки информации в ИТКС в условиях противодействия угрозам НСД. Соответствующая схема моделирования должна имитировать:

1) многоэтапный процесс обработки информации в ИТКС;

2) воздействие угроз на процесс обработки информации в виде попыток прямого манипулирования информацией злоумышленником, либо манипулирования с использованием вредоносных программ;

3) противодействие угрозам средствами защиты информации придаваемого и встраиваемого типа. Подобная схема моделирования предполагает имитацию рассмотренных выше процессов на заданном интервале моделирования. В результате формируется множество $Q^{(y)} = \left\{ q_s^{(y)},\ s = 1,2,\ldots,S \right\}$ инициированных воздействий угроз НСД.

Обозначив через $Q'^{(y)}$ подмножество элементов $Q^{(y)}$, обслуживание которых производилось средствами защиты информации придаваемого типа, а через $Q''^{(y)}$ – подмножество элементов $Q^{(y)}$, обслуживание которых производилось средствами защиты информации встраиваемого типа, частотную характеристику процесса защиты информации в ИТКС при ее обработке запишем в виде:

$$w_1 = \frac{\left|Q'^{(y)}\right|}{\left|Q'^{(y)}\right| + \left|Q''^{(y)}\right|};$$

$$w_2 = \frac{\left|Q''^{(y)}\right|}{\left|Q'^{(y)}\right| + \left|Q''^{(y)}\right|}.$$

С учетом изложенного требуемая вероятность реализации задач защиты информации СЗИ придаваемого типа определяется в соответствии с выражением

$$E_{(\text{тр})}^{(\text{пр})} = w_1 \cdot \xi_1,$$

где ξ_1 – важность (значимость) задач защиты информации СЗИ придаваемого типа, определяемая методом непосредственной оценки.

Требуемая вероятность реализации задач защиты информации СЗИ встраиваемого типа определяется в соответствии с выражением

$$E_{(\text{тр})}^{(\text{вс})} = w_2 \cdot \xi_2,$$

где ξ_2 – важность задач защиты информации СЗИ встраиваемого типа.

Обобщенная требуемая вероятность противодействия угрозам НСД к информации в ИТКС определяется в соответствии с выражением

$$E_{(\text{зи})}^{(\text{тр})} = E_{(\text{тр})}^{(\text{пр})} \cdot E_{(\text{тр})}^{(\text{вс})}.$$

Схема организации защиты СЗИ придаваемого типа может быть реализована путем решения одной или нескольких задач защиты информации обеспечивающих механизм данного типа защиты. При этом совокупность элементарных событий по решению этих задач является независимой. Это дает основание полагать, что обобщенный показатель эффективности противодействия НСД к ИТКС средствами придаваемого типа определяется в соответствии с выражением

$$E_{(\text{зи})}^{(\text{пр})} = 1 - (1 - E_1)^{\lambda_1} (1 - E_2)^{\lambda_2} \ldots (1 - E_i)^{\lambda_i} = 1 - \prod_{i=1}^{I} (1 - E_i)^{\lambda_i}, \quad (1)$$

где E_i – эффективность i-й задачи защиты, согласно выражению $\tau_{(зи)}^{(вс)} \le \tau_{(мз)}^{(вс)}$; $\tau_{(зи)}^{(вс)}$ – фактическое время выполнения задач СЗИ; $\tau_{(мз)}^{(вс)}$ – максимальное время действия СЗИ, время действия активного периода вредоносного программного воздействия; λ_i – индикатор отвлечения вычислительного ресурса за счет использования i-й задачи защиты средствами СЗИ.

В случае СЗИ встраиваемого типа механизм организации защиты может быть реализован путем решения одной или нескольких последовательностей задач защиты информации. Совокупность элементарных событий по реализации таких последовательностей является независимой. В этом случае эффективность противодействия НСД к ИТКС при решении j-й последовательности задач защиты информации средствами данного типа определяется в соответствии с выражением

$$E_j^{(вс)} = P\left(\tau_{j,1}\cdot\mu_{j,1} + \tau_{j,2}\cdot\mu_{j,2} + \cdots + \tau_{j,N}\cdot\mu_{j,N} \le \tau_{(мз)}^{(вс)}\right), \quad (2)$$

где $\tau_{j,n}$ – время выполнения n-й задачи в j-й последовательности; $\mu_{j,n}$ – индикатор отвлечения вычислительного ресурса за счет использования n-й задачи в j-й последовательности, определяемый по формуле

$$\mu_{j,n} = \begin{cases} 1, & \text{если } n\text{-я задача используется в } j\text{-й последовательности;} \\ 0, & \text{в противном случае.} \end{cases}$$

Тогда обобщенный показатель эффективности противодействия НСД к ИТКС средствами данного типа определяется в соответствии с выражением

$$E_{(зи)}^{(вс)} = 1 - \prod_{j=1}^{J}\left(1 - E_j^{(вс)}\right).$$

С учетом изложенного обобщенный показатель эффективности противодействия угрозам НСД к ИТКС разнотипными СЗИ определяется согласно выражению

$$E_{(зи)} = 1 - \left(1 - E_{(зи)}^{(пр)}\right)^{\lambda_i}\left(1 - E_{(зи)}^{(вс)}\right). \quad (3)$$

Рассмотренные ограничения используются в дальнейшем при решении оптимизационной задачи по минимизации отвлечения вычислительного ресурса ИТКС в условиях противодействия угрозам НСД разнотипными СЗИ.

В основу алгоритма определения минимального уровня отвлечения вычислительного ресурса ИТКС положены требования наличия резерва вычислительного ресурса ИТКС, унифицированности параметра представления вычислительного ресурса ИТКС и согласованности целей при решении задач обработки информации и ее защиты. С целью определения минимального уровня отвлечения вычислительного ресурса ИТКС проведем анализ классических и эвристических подходов решения аналогичных задач.

Наиболее приемлемым в этом плане является класс задач математического программирования, позволяющий проводить оптимизацию решений, для которых характерны следующие условия: показатель эффективности представляет собой функцию от элементов решения; ограничительные условия, налагаемые на возможные решения, имеют вид равенств или неравенств. Рассмотрим в этом контексте оптимизационную задачу.

Будем считать, что *имеется* пять задач $z_i^{(пр)}$, $i = 1, 2, ..., 5$ защиты информации, решаемых придаваемыми средствами защиты информации, и пять задач $z_j^{(вс)}$, $i = 1, 2, ..., 5$ защиты информации, решаемых встраиваемыми средствами: $z_1^{(пр)}$ – разграничение доступа к вычислительным ресурсам и устройствам ИТКС; $z_2^{(пр)}$ – разграничение полномочий пользователей; $z_3^{(пр)}$ – преобразование данных; $z_4^{(пр)}$ – контроль последствий влияния угроз НСД к информации в ИТКС; $z_5^{(пр)}$ – поддержание целостности вычислительной среды; $z_1^{(вс)}$ – контроль процесса обработки информации на предмет его подверженности угрозам НСД; $z_2^{(вс)}$ – выявление угроз НСД; $z_3^{(вс)}$ – подавление угроз НСД; $z_4^{(вс)}$ – идентификация последствий воздействия угроз НСД к информации в ИТКС; $z_5^{(вс)}$ – оперативное восстановление информационных процессов, подвергнутых воздействию угроз НСД.

Требуется таким образом распределить вычислительный ресурс ИТКС между задачами защиты информации, выполняемыми разнотипными средствами, чтобы достичь его минимального отвлечения, обеспечив требуемый уровень ее защиты $E_{(зи)}^{(тр)}$.

Согласно приведенной выше структурной схеме механизм организации защиты СЗИ придаваемого типа изобразим на рис. 1.

Для этого обозначим через λ_i, $i = 1, 2, ..., 5$ коэффициенты отвлечения вычислительного ресурса ИТКС средствами защиты информации придаваемого типа при решении ими соответствующих задач защиты информации. В этом случае имеет место выражение

$$\lambda_i = \begin{cases} 1, & \text{если } i\text{-я задача защиты информации используется,} \\ 0, & \text{в противном случае.} \end{cases}$$

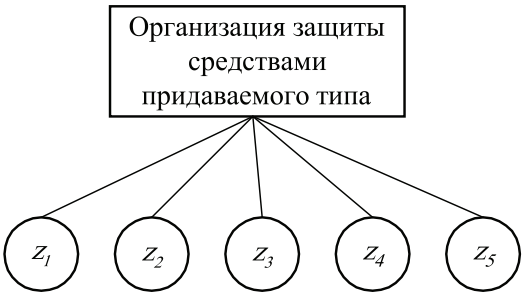

Рис. 1. Структурная схема механизма организации защиты СЗИ придаваемого типа

Соответствующий i-й задаче защиты информации объем вычислительного ресурса обозначим через x_i, $i = 1, 2, ..., 5$. В свою очередь механизм организации защиты СЗИ встраиваемого типа формально можно представить следующим образом (рис. 2).

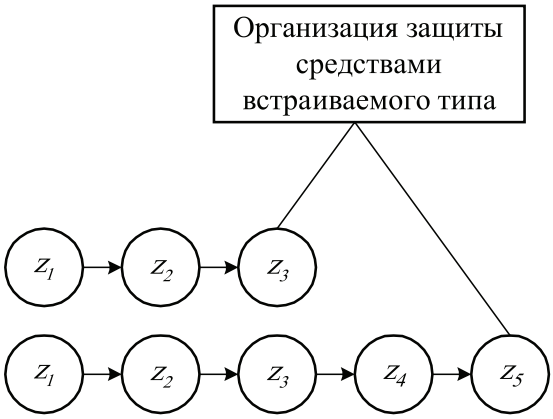

Рис. 2. Структурная схема механизма организации защиты СЗИ встраиваемого типа

Обозначим через $\mu_j^{(1)}$, где $j = 1, 2, 3$ – коэффициент отвлечения вычислительного ресурса ИТКС, средствами встраиваемого типа при решении ими задач обнаружения угроз НСД к ИТКС, а через $\mu_l^{(2)}$, $l = 1, 2, ..., 5$ – коэффициент отвлечения вычислительного ресурса ИТКС, средствами встраиваемого типа при решении ими задач полного цикла противодействия НСД к ИТКС. При этом $\mu_j^{(1)}\left(\mu_l^{(2)}\right)$ соответствует числу реализаций данной последовательности задач.

Обозначим через y_j, $j = 1, 2, 3$ объем вычислительного ресурса, отвлекаемый для реализации j-й задачи защиты, а через y_l, $l = 1, 2, ..., 5$ – объем вычислительного ресурса, отвлекаемый для реализации l-й задачи защиты.

Объем отвлекаемого при этом вычислительного ресурса составит

$$\tau_{(p)} = \sum_{i=1}^{5} \lambda_i \cdot x_i + \mu_j^{(1)} \sum_{j=1}^{3} y_j + \mu_l^{(2)} \sum_{l=1}^{5} y_l. \quad (4)$$

В свою очередь уровень эффективности противодействия НСД к ИТКС, обеспечиваемый при реализации задач СЗИ обоих типов, не должен быть меньше $E_{(зи)}^{(тр)}$, откуда получаем условие-неравенство

$$E_{(зи)} \geq E_{(зи)}^{(тр)}, \quad (5)$$

в котором $E_{(зи)}$ определяется согласно (3).

Входящие в выражения (1) и (2) коэффициенты λ_i, $\mu_j^{(1)}$ и $\mu_l^{(2)}$ характеризуют степень влияния вычислительного ресурса, отвлекаемого при решении соответствующих задач защиты информации на эффективность противодействия угрозам НСД. Эти условия представляют собой ограничения, накладываемые на решение оптимизационной задачи. Таким образом, решаемая задача имеет следующую формулировку: выбрать такие неотрицательные значения переменных λ_i, $i = 1, 2, ..., 5$, $\mu_j^{(1)}$, $j = 1, 2, 3$ и $\mu_l^{(2)}$, $l = 1, 2, ..., 5$, удовлетворяющие неравенству (5), при которых функция этих переменных в формуле (4) обращалась бы в минимум. Поставленная задача представляет собой задачу математического программирования и решается известными методами.

Таким образом, в работе показан вариант совместного использования разных по типу средств защиты информации за счет решения задачи оптимального распределения временного ресурса, отвлекаемого от вычислительного ресурса информационно-телекоммуникационной системы. В основе алгоритма определения ограничений лежит гипотеза об определении возможностей средств защиты информации исходя из частоты их использования и значимости. Оценка эффективности применения средств защиты информации от несанкционированного доступа основана на вероятностном подходе с использованием методов имитационного моделирования процессов обработки информации с учетом значимости (важности) задач защиты.

Список литературы

1. Вентцель Е.С. Исследование операций. – М.: Советское радио, 1972. – 552 с.

2. Душкин А.В. Распознавание угроз несанкционированного воздействия на защищенные информационные телекоммуникационные системы: методы и математические модели: монография. – Воронеж: ВВВАИУ, 2008. 256 с.

3. Душкин А.В., Новосельцев В.И., Сумин В.И. Математические модели и информационные процессы управления сложным объектом: монография. – Воронеж: Научная книга, 2014. 125 с.

4. Иглхарт Д.Л., Шедлер Д.С. Регенеративное моделирование сетей массового обслуживания: пер. с англ. – М.: Радио и связь, 1984. – 136 с.

5. Кочедыков С.С. Математическая модель противодействия НСД к ИТКС разнотипными СЗИ в условиях минимизации отвлечения вычислительного ресурса: дис. … канд. техн. наук. – Воронеж, 2002.

6. Кочедыков С.С. Методический подход к решению задачи оптимального распределения временного резерва в интересах обеспечения информационной безопасности разнородными системами защиты информации. Информация и безопасность. – 2001. – № 1. – С. 60–63.

7. Кочедыков С.С. и др. Об одном способе решения задачи оптимального распределения временного резерва в информационно-телекоммуникационных системах в интересах обеспечения информационной безопасности. Информация и безопасность. – 2000. – № 1. – С. 40–44.

8. Кофман Б. Методы и модели исследования операций: пер. с франц. – М.: Мир, 1966. – 523 с.

9. Литван Б.Г. Экспертная информация. Методы получения и анализа. – М.: Радио и связь, 1982. – 181 с.

10. Хедли Дж. Нелинейное динамическое программирование: пер. с англ. – М.: Мир, 1967. 506 с.

References

1. Ventcel E.S. Issledovanie operacij. M.: Sovetskoe radio, 1972. 552 p.

2. Dushkin A.V. Raspoznavanie ugroz nesankcionirovannogo vozdejstvija na zashhishhennye informacionnye telekommunikacionnye sistemy: metody i matematicheskie modeli: monografija. Voronezh: VVVAIU, 2008. 256 p.

3. Dushkin A.V., Novoselcev V.I., Sumin V.I. Matematicheskie modeli i informacionnye processy upravlenija slozhnym obektom: monografija. Voronezh: Nauchnaja kniga, 2014. 125 p.

4. Iglhart D.L., Shedler D.S. Regenerativnoe modelirovanie setej massovogo obsluzhivanija: per. s angl. M.: Radio i svjaz, 1984. 136 p.

5. Kochedykov S.S. Matematicheskaja model protivodejstvija NSD k ITKS raznotipnymi SZI v uslovijah minimizacii otvlechenija vychislitelnogo resursa: dis. … kand. tehn. nauk. Voronezh, 2002.

6. Kochedykov S.S. Metodicheskij podhod k resheniju zadachi optimalnogo raspredelenija vremennogo rezerva v interesah obespechenija informacionnoj bezopasnosti raznorodnymi sistemami zashhity informacii. Informacija i bezopasnost. 2001. no. 1. pp. 60–63.

7. Kochedykov S.S. i dr. Ob odnom sposobe reshenija zadachi optimalnogo raspredelenija vremennogo rezerva v informacionno-telekommunikacionnyh sistemah v interesah obespechenija informacionnoj bezopasnosti. Informacija i bezopasnost. 2000. no. 1. pp. 40–44.

8. Kofman B. Metody i modeli issledovanija operacij: per. s franc. M.: Mir, 1966. 523 p.

9. Litvan B.G. Jekspertnaja informacija. Metody poluchenija i analiza. M.: Radio i svjaz, 1982. 181 p.

10. Hedli Dzh. Nelinejnoe dinamicheskoe programmirovanie: per. s angl. M.: Mir, 1967. 506 p.

Рецензенты:

Сумин В.И., д.т.н., профессор кафедры управления и информационно-технического обеспечения, ФКОУ ВПО «Воронежский институт ФСИН России», г. Воронеж;

Дубровин А.С., д.т.н., доцент, профессор кафедры управления и информационно-технического обеспечения, ФКОУ ВПО «Воронежский институт ФСИН России», г. Воронеж.