УДК 681.3.004

**Н.Н. Браиловский, А.В. Хорошко,
В.А. Хорошко, Д.В.Чирков**

МОДЕЛЬ ПРОЦЕССА ЗАЩИТЫ ИНФОРМАЦИИ

Разработана модель процесса защиты информации, которая позволяет оценить эффективность системы технической защиты

Защита информации – это регулярное использование методов и средств, принятие мер и осуществление мероприятий с целью системного обеспечения требуемого уровня защищенности объекта. Оценка эффективности систем защиты информации (СЗИ) возможна на основании анализа обобщенной модели взаимодействия СЗИ и окружающей среды. Причем обобщенная модель должна отображать процесс защиты информации как процесс взаимодействия дестабилизирующих факторов и средств защиты.

В настоящее время широко используется вероятностная модель (рис.1), в соответствии с которой обработка информации на объекте Oi осуществляется в условиях воздействия на информацию угроз {Yi}. Для противодействия угрозам информации могут использоваться средства защиты {Cη}, оказывающие нейтрализующее воздействие на дестабилизирующие факторы.

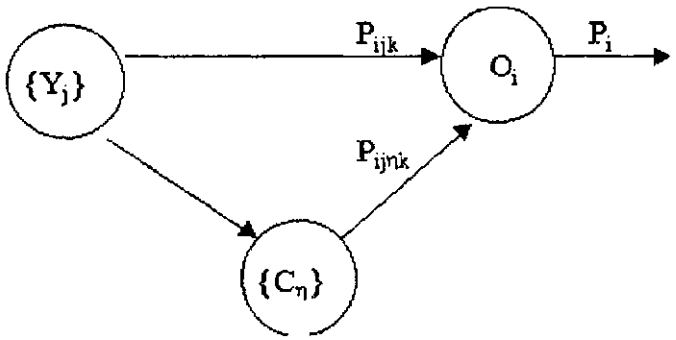

Рис. 1. Обобщенная модель процесса защиты информации

В соответствии с работой [1] в общем случае Pijk - вероятность негативного воздействия j-го фактора на i-й объект в k-м состоянии, а Pijk - вероятность нейтрализации, воздействия j-й угрозы на i-й объект в k-м состоянии с применением η -го средства защиты. При этом характер и уровень воздействия одних факторов не зависит от характера и уровня воздействия других. Однако могут быть и взаимозависимые факторы. Средства защиты с точки зрения эффективности защиты также могут быть как независимыми, так и взаимозависимыми:

С учетом изложенного выше можно записать:

$$P_i = 1 - \prod_{\forall k} (1 - P_{ik})\alpha_k ,$$

где α_k – доля k-го режима работы СЗИ в анализируемый период времени. Наиболее объективным будет представление αk в виде интервала времени пребывания СЗИ в k-м состоянии (Δtk) в общей продолжительности оцениваемого интервала времени ΔT, т.е.

$$\alpha_k = \frac{\Delta t_k}{\Delta T} .$$

Следовательно, вероятность надежной защиты информации в группе объектов определяется зависимостью [1]:

$$P = \prod_{\forall i} P_i .$$

Необходимо при этом учесть фактор времени. Действительно, показатели защищенности, выраженные приведенными выше зависимостями, будут справедливы лишь для какого-то отрезка времени δt. Если же этот интервал времени ΔT, на котором оценивается защищенность информации, существенно больше δt, то

$$P(\Delta T) = \prod_{z=1}^{\bar{z}} P_z(\delta t),$$

где $\bar{z} = \left[\frac{\Delta T}{\delta t}\right]$ – целое; $P_z(\delta t)$ – показатель защищенности информации на z-м интервале длиною δt.

Рассмотренная модель привлекательна своей простотой, так как для определения показателей защищенности информации достаточно знать вероятностные характеристики дестабилизирующего воздействия на информацию и эффективность функционирования средств защиты, что на практике весьма затруднительно. Это связано с тем, что пользователь не знает, когда и какими средствами злоумышленник попытается несанкционированно получить информацию. Помимо отмеченного недостатка, в этой модели также отсутствуют учет возможного ущерба от воздействия различных факторов на функционирование СЗИ и эффективность самой СЗИ. Поэтому данной моделью и моделями, подобными ей, следует пользоваться лишь для общих оценок при определении степени того внимания, которое должно быть уделено проблеме защиты.

Авторы считают, что целесообразнее использовать модель, в которой отображается взаимодействие СЗИ с источником информационных ресурсов (ИИР) и пользователем информацией (ПИ). Причем,в этой модели учитывается воздействие внешней среды, которое бывает как естественное, так и искусственное (действия злоумышленников). Этот анализ производим с учетом свойств систем и используемых данных [2]. Поскольку частными показателями эффективности функционирования СЗИ могут быть отдельные ее "свойства" или их совокупность, которые описываются уравнением:

$$a_I^{\chi} = \sum_{\substack{\chi \in k \\ \varphi \in \Psi}} a_N^{\Psi} W_{IN}^{\chi\varphi} + \sum_{\chi \in k} a_{I0}^{\chi 0} + \sum_{\substack{I \neq J \\ \chi \in k}} a_j W_{JI}^{\chi k},$$

где I, j – точки входа и выхода системы χ (I ≠ j), то правая часть в порядке следования представляет собой произведение обобщенных множеств переменных произвольной χ - системы на операторы {W}, характеризующие способы реализации этих свойств, транслируемые соответственно N-точками выхода φ -системы, внешней среды (0) и Ψ-точками внутренних переменных К-системы.

Для оценки показателя эффективности преобразуем обобщенную гипотетическую модель взаимосвязи СЗИ, ИИР и ПИ в соответствии с рис.2.

Проанализируем взаимосвязь между СЗИ, (ИИР) и (ПИ), составим семейство уравнений, описывающих взаимосвязь свойств систем ПИ, ИИР и СЗИ:

$$a_i^1 = \sum_{n=1-4}^{i=1,2} a_n^2 W_{in}^{12} + \sum_{i=1,2} a_{i0}^1 W_{i0}^{10} + \sum a_q^3 W_{iq}^{13} + \sum_{i \neq j=1-3} a_j^1 \left(W_{ji}^{11}\right)^{-1},$$

$$a_m^2 = \sum_{m=1-4} a_{m0}^2 W_{m0}^{20} + \sum_{m=1-4} a_2^3 W_{m2}^{23} + \sum_{m \neq n=1-4} a_n^2 W_{nm}^{22} + \sum_{m=1-4} a_1^3 W_{m1}^{23}, \qquad (1)$$

$$a_p^3 = \sum_{P=1-3} a_3^1 W_{P3}^{31} + \sum a_{P0}^3 W_{P0}^{30} + \sum a_q^3 (W_{qp}^{33})^{-1} + \sum_{m=1,2,4}^{P=3} a_n^2 W_{pn}^{32},$$

$$a_3^1 = a_3^3 W_{33}^{13}; \qquad a_3^3 = \sum_{m=1,2,4} a_m^2 W_{3m}^{32}.$$

Анализ выходных переменных систем согласно рис. 2 при помощи формулы (1) дает возможность определить частные показатели эффективности функционирования СЗИ при выполнении самостоятельных (W_{pq}^{33}) или межсистемных (W_{32}^{13}, W_{33}^{31} и др.) функций по связи с внешней средой.

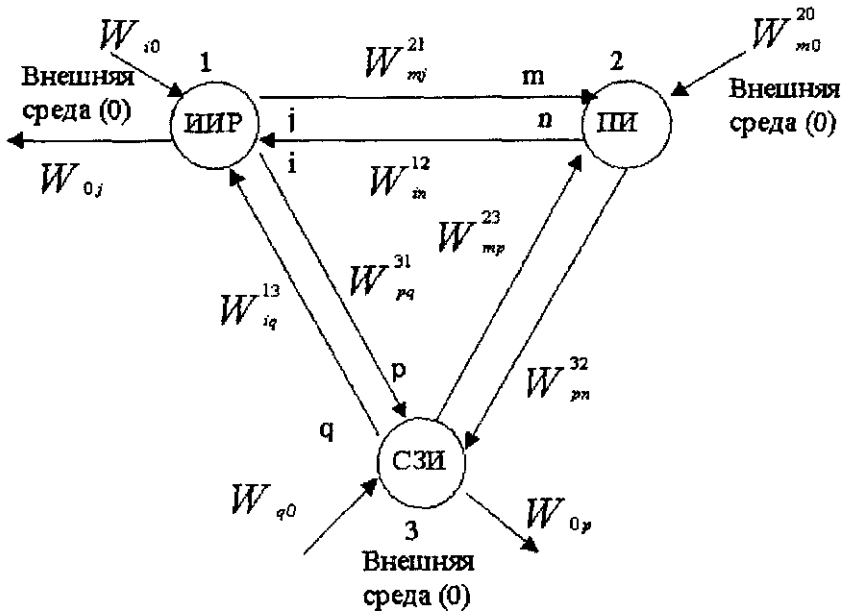

Рис.2. Модель взаимосвязи СЗИ с ИИР и ПИ

В конечном итоге эффективность функционирования СЗИ будет определяться возможностями (W), т.е.

Эсзи = f[am, an, Win, Wmj, Wqn, Wmq, ….].

Выражение для обобщенной эффективности СЗИ для рассматриваемого уровня взаимодействия систем (рис.2) примет вид:

$$Э_{сзи}^{(1)} = \sum_{s \neq r} K_{sr} K(W_{sr}) / \sum K_{sr},$$

где s = r = i, j, m, n, p, q, 0; Ksr - коэффициенты, определяющие потребность в реализации отдельных задач СЗИ (Ksr=1), их значимость. Отсутствие такой потребности характеризуется величиной Ksr =0.

Приведенные выражения позволяют более точно оценить эффективности СЗИ, чем вероятностные показатели, которые рекомендуются авторами работ по защите информации [2,3], а использование системы (1) с достаточно высокой точностью описывать процесс защиты информации на различных объектах. Модель, реализованная на базе этих выражений, позволяет устранить недостатки, которые присущи вероятностным моделям.

Список литературы

1. *Герасименко В.А., Малюк А.А.* Основы защиты информации. -М.:, Моск. Гос.ИФИ, 1997. -538 с.

2. *Фисенко В.М., Хорошко В.А.* Анализ эффективности средств защиты информации. // Защита информации: Сб.науч.тр.-К.: КМУГА,1996.- С. 11-13.

3. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных В. 2-х кн. –М.: Энергоатомиздат,1994.

Стаття надійшла до редакції 12 квітня 1999 року.

Микола Миколайович Браіловський (1972) закінчив Українську державну академію зв'язку в 1994 році. Інженер кафедри автоматизації прийому та обробки інформації. Спеціалізується в галузі технічного захисту інформації.

Mykola M. Brailovskyi (b. 1972) graduated from Ukrainian State Communication Academy (1994). Engineer of Automatic Reception and Processing of Information Department. Specializes in technical protection of information.

Олексій Володимирович Хорошко (1973) закінчив Київський міжнародний університет цивільної авіації у 1996 році. Аспірант кафедри технічної електродинаміки. Спеціалізується у галузі технічного захисту інформації.

Olexyi V. Khoroshko (b. 1973) graduated from Kyiv International University of Civil Aviation (1996). Aspirant of Technical electrodynamics Department. Specializes in technical protection of information

Володимир Олексійович Хорошко (1945) закінчив Київський інститут інженерів цивільної авіації у 1968 році. Доктор технічних наук професор кафедри автоматизації прийому та обробки інформації. Автор більш як 150 наукових праць. Галузь наукових досліджень – обчислювальні комплекси, системи та мережі; захист інформації.

Volodymir O. Khoroshko (b. 1945) graduated from Kyiv Institute of Civil Aviation Engineers (1968). DSc (Eng), professor of Automatic Reception and Processing of Information Department. Author of more than 150 publications. Specializes in the fields of culculation complexes, systems and networks, protection of information.

Дмитро Володимирович Чирков (1940) закінчив Київський інститут інженерів цивільної авіації у 1964 році. Кандидат технічних наук доцент кафедри автоматизації прийому та обробки інформації. Автор більш як 100 наукових праць. Галузь наукових досліджень – обробка інформаційних сигналів; захист інформації.

Dmitro V. Tchirkov (b. 1940) graduated from Kyiv Institute of Civil Aviation Engineers (1964). PhD (Eng), ass. professor of Automatic Reception and Processing of Information Department. Author of more than 100 publications. Specializes in the fields of processing of information signals and protection of information.