УДК 004.056.5

ГРАФОВАЯ МОДЕЛЬ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С ВЗАИМОВЛИЯЮЩИМИ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ И СРЕДСТВАМИ ВОЗДЕЙСТВИЯ

Мирошина И.Е.

ФГБОУ ВПО «Воронежский государственный педагогический университет», Воронеж, e-mail: mirosh.irina2014@yandex.ru

В работе рассмотрена возможность формализации процесса динамической безопасности информации в неоднородных вычислительных сетях на основе графового их представления и критерия устойчивости взаимовлияющих процессов. Рассмотрены следующие составляющие модели фрагмента сети: модель множества распределения защищаемой информации, модель множества средств воздействия, модель множества комплексов средств защиты, модель связи множества распределения защищаемой информации и множества комплексов средств защиты, модель связи множества распределения защищаемой информации и множества средств воздействия, модель связи множества средств воздействия и множества комплексов средств защиты информации.

Ключевые слова: безопасность информации, средства защиты, средства воздействия

GRAPH MODEL OF COMPUTER NETWORK WITH INTERDEPENDENT MEANS OF INFORMATION PROTECTION AND MEANS OF INFLUENCE

Miroshina I.E.

Voronezh State Pedagogical University, Voronezh, e-mail: mirosh.irina2014@yandex.ru

The paper considers the possibility of formalization of the process of dynamic information security in heterogeneous computer networks on the basis of the graph of their submission, and sustainability criteria interdependent processes. Includes the following components of the model of a fragment of the network: a model of multiple distribution of protected information, the model of many means of influence, model many complexes of means of protection, the connection model of multiple distribution of sensitive information and many complexes of means of protection, the connection model of multiple distribution of sensitive information and many means of influence, the connection model of many means of influence and many complexes of means of information protection.

Keywords: security of information, means of influence, means of protection

В работах [1, 2] рассмотрены некоторые методологические основы защиты информации в кибернетическом пространстве. Однако условия непрерывной эволюции средств защиты и средств воздействия на них в разнородных вычислительных сетях приводят к необходимости построения адекватной модели и формализации процесса динамической безопасности информации.

Целями исследования являются возможности графового представления вычислительных сетей с распределенными в них конфиденциальной информации и взаимовлияющими средствами ее защиты и средствами неправомерных действий для формализации процесса динамической безопасности на основе выбранного критерия устойчивости.

Возможны два режима работы системы защиты информации (СЗИ):

• недоступность защищаемой информации для системы «неправомерных действий» (СНД);

• либо ее доступность для СНД.

Основной (целевой) функцией СЗИ является обеспечение безопасности защищаемой информации. Под устойчивостью взаимовлияющих процессов будем понимать свойство системы защиты информации в вычислительных сетях с разнородной структурой, определяющее способность СЗИ к длительному поддержанию ее основной функции в заданных границах вне зависимости от изменения внешних воздействий со стороны СНД. Следовательно, эффективность функционирования СЗИ при выбранной политике безопасности зависит от адекватности реализации основной (целевой) функции системы защиты информации.

В соответствии с [3] для выбранной политики безопасности структурную модель PISP (Information Security Policy) вычислительной сети с системой защиты информации и системой неправомерных действий определим в виде кортежа моделей следующим образом:

$$M_{ISP} = <M_{PI}, M_{SIA}, M_{MPI}, M_{PI\_MPI}, M_{PI\_SIA}, M_{MPI\_SIA}>,$$

где M_{PI} – модель множества распределения защищаемой информации (*Protected Information*); M_{SIA} – модель множества средств воздействий (СВ) при выбранной политике безопасности на СЗИ с целью незаконного (несанкционированного) досту-

па к защищаемой информации (*System of Illegal Activities*); M_{MPI} – модель множества комплексов средств защиты информации (КСЗИ) в СЗИ при выбранной политике безопасности информации (*Means of Protecting Information*); M_{PI_MPI} – модель связи множества распределения защищаемой информации и множества КСЗИ; M_{PI_SIA} – модель связи множества распределения защищаемой информации и множества СВ; M_{MPI_SIA} – модель связи множества СВ и множества КСЗИ.

Модель M_{ISP} в целом и все элементы кортежа модели будем рассматривать на определенном фрагменте вычислительной сети с распределенной в ней информацией. На этом же фрагменте вычислительной сети будем рассматривать и взаимодействие между распределением средств защиты и средств воздействия.

Модель множества распределения защищаемой информации (M_{PI}) представим в виде пустого графа:

$$G_{PI}=(V(I), \varnothing),$$

где $V(I)=\{V_j(I_i)\}$ – множество объектов вычислительной сети (j-х вершин) с множеством i-х типов защищаемой информации из домена $I_i=\{I_{ik}\}$, где k определяет уровень защищаемой информации (под уровнем защищаемой информации будем понимать такой ее атрибут как несекретность, конфиденциальность, совершенная секретность, для служебного пользования, особая важность и т.д.).

Структуру объектов фрагмента вычислительной сети зададим в виде графа:

$$G_{Vj}=(V_j, E_{Vj}),$$

где V_j – множество объектов вычислительной сети, содержащих информацию с определенными свойствами I_{ik}, а E_{Vj} – множество связей между объектами вычислительной сети.

Модель множества средств воздействий M_{SIA} описывается пустым графом в виде:

$$G_{SIA}=(A(I), \varnothing),$$

где $A(I) = \{A_n(I_i)\}$ – множество средств воздействий (*actions*) n-м правонарушителем на i-й тип информации.

На основе нуль-графа G_{SIA} создается нуль-граф $G_{Ij}=(\{I_i\},\varnothing)$, объединение вершин которого формирует входной объект $I=\cup I_i$, для СНД. Основываясь на изложенном, модель связи множества распределения защищаемой информации и множества СВ, устанавливающая отношения между этими множествами, является биграфом M_{PI_SIA}: $G_I = (A_I, E_I)$, $A_I=\{I_i\}\cup I$.

Модель M_{MPI} множества комплексов средств защиты информации (КСЗИ) в системе защиты информации (СЗИ) при выбранной политике безопасности описывается пустым графом в виде:

$$G_{MPI}=(KSZ(I),\varnothing),$$

где $KSZ(I) =\{KSZ_m(I_i)\}$ – множество комплексов средств защиты информации *m-ой* СЗИ, обеспечивающей безопасность i-го типа информации.

Система защиты информации включает следующие основные компоненты:

$$СЗИ = \{КСЗИ_{MP}, КСЗИ_{SW}, КСЗИ_{PM}, КСЗИ_{PI}\},$$

где $КСЗИ_{MP}$ – конкретное средство защиты (*mean of protection*); $КСЗИ_{SW}$ – его программное обеспечение (*software*); $КСЗИ_{PM}$ – используемый метод защиты (*protection method*); $КСЗИ_{PI}$ – защищаемая информация (*protected information*).

Соответственно $KSZ_m(I_i)=\{KSZ_{lm}(I_i)\}$, где l определяет конкретную компоненту системы защиты.

Модель M_{PI_MPI} связи множества распределения защищаемой информации и множества КСЗИ описывается биграфом в виде:

$$G_{KSZ} = (V_{KSZ}, E_{KSZ}),\ V_{KSZ}=PI\cup \{PI_i\}.$$

В этой модели защищаемая информация *PI* (*protected information*) разбивается на элементы PI_i., которые не позволяют системе неправомерных действий за счет распределенных средств защиты V_{KSZ} осуществить противоправные действия.

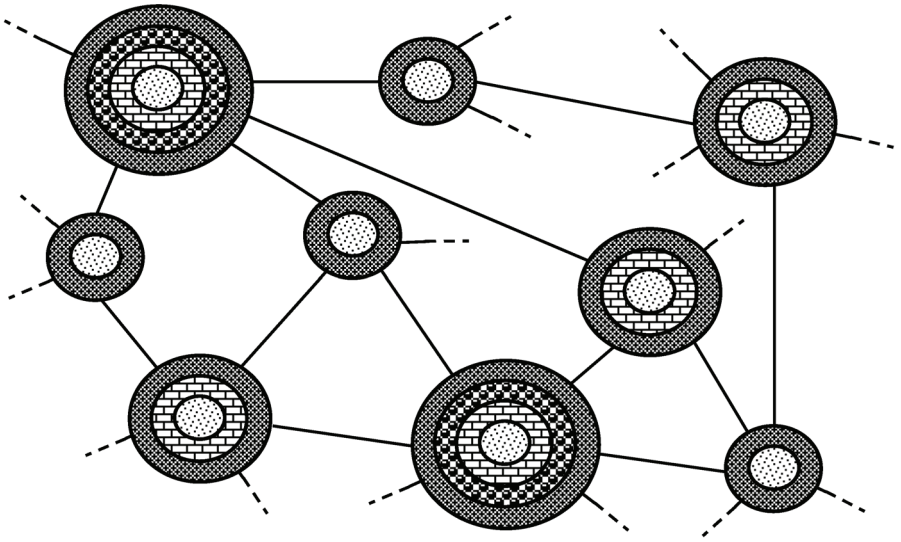
Модель M_{MPI_SIA} связи множества СВ и множества КСЗИ является моделью функции обеспечения безопасности информации в вычислительных сетях (целевой функции), которую можно представить в виде:

$$(R{:}I\times X\rightarrow PI),$$

где R – множество глобальных реакций системы на входное воздействие I на защищаемую информацию при состоянии системы X, а PI – выходное состояние защищаемой информации [4].

Как и в [5], структурно эта модель представима в виде орграфа $G_{IDI} =(V_{IPI}, E_{IPI})$ у которого $V_{IPI} =I\cup X\cup PI$ – множество вершин и E_{IPI} – множество дуг. В графе G_{IPI} вершины PI достижимы из вершин I только через вершины множества состояний X, а множество дуг E_{IDI} определяет множество стратегий доступа к информации при взаимооднозначном соотношении $E_{IPI} \Leftrightarrow R$. На основании сравнения множества I и PI можно делать вывод об устойчивости или неустойчивости состояний вычислительной сети с КСЗИ к внешним воздействиям.

Обобщая модели составляющих, представим структурную модель фрагмента вычислительной сети с системой защиты информации при выбранной политике безопасности и системой неправомерных действий, осуществляющей несанкционированный доступ к защищаемой информации с конкретным набором свойств (M_{ISP}) как на рисунке.



Фрагмент вычислительной сети с объектами V и распределенной в них информацией I, средствами воздействия A и средствами защиты KSZ:

– множество j-х объектов вычислительной сети с множеством i-х типов защищаемой информации I: $V(I)=\{V_j(I_i)\}$;

– множество I защищаемой информации i-го типа с k-м атрибутом: $I_i=\{I_{ik}\}$;

– множество средств воздействия n-м правонарушителем на i-й тип защищаемой информации I: $A(I) = \{A_n(I_i)\}$;

– множество конкретных l-х компонент защиты в m-м КСЗИ, обеспечивающей безопасность i-го типа информации I: $KSZ_m(I_i) = \{KSZ_{lm}(I_i)\}$.

Информация, циркулирующая при выбранной политике безопасности в вычислительных сетях с взаимодействующими системами защиты информации и «неправомерных действий», подвергается различным модификациям (например – старение и обновление, рассеяние и концентрация). Такой же модификации подвергаются и сами средства защиты информации и воздействия на КСЗИ. Поэтому можно сделать вывод, что функционирование процессов происходящих в модели M_{ISP} зависит от функционирования процессов происходящих в моделях M_{PP}, M_{SIA}, M_{MPI}.

Таким образом, предложенная графовая модель вычислительной сети с распределенной в ней информацией, а также средствами защиты и средствами воздействия, может служить основой для оценки динамической устойчивости или неустойчивости состояний вычислительной сети с КСЗИ к внешним воздействиям, а значит и эффективности КСЗИ при выбранной политике безопасности.

Список литературы

1. Джахуа Д.К., Чулюков В.А. Управление в информационно-кибернетическом пространстве // Сборник научных трудов SWorld. Вып. 3. Том 5. – Одесса: КУПРИЕНКО СВ, 2013. – С. 14-16.

2. Грищенко К.П., Чулюков В.А. Контроль программного обеспечения на остутствие недекларированных возможностей с помощью аппарата сетей Петри // Сборник научных трудов SWorld. Вып. 3. Том 5. – Одесса: КУПРИЕНКО СВ, 2013. – С. 16-18.

3. Сысоев Д.В. Автоматизированные технологии функционирования информационной системы в структурно-параметрическом представлении взаимодействия с внешней средой: диссертация на соискание ученой степени кандидата технических наук. – Воронеж, 2001. – 146 с.

4. Месарович М. Общая теория систем: математические основы / М. Месарович, Я. Токахара. – М.: Мир, 1978. – 311 с.

5. Шиляк Д.Д. Децентрализованное управление сложными системами. – М.: Мир, 1994. – 576 с.