УДК 663.1:004.056

И.Г. Дровникова[1], Е.А. Рогозин[2], А.В. Хвостов[3], А.А. Змеев[4]
([1]Воронежский институт МВД России, [2]Воронежский институт МВД России,
[3]Воронежский Государственный Технический Университет,
[4]Военная академия ВКО им. Г.К. Жукова; e-mail: idrovnikova@mail.ru)

АНАЛИЗ АРХИТЕКТУРЫ И КЛАСТЕРИЗАЦИЯ СТРУКТУРЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ПРИ ОБОСНОВАНИИ ТРЕБОВАНИЙ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Предложена методика кластеризации информационной структуры защищённых автоматизированных систем, позволяющая существенно снизить размерность решаемой задачи обоснования требований к информационной безопасности. Методика предназначена для обоснования количественных требований к системам защиты информации на основе оптимизации их структуры.

Ключевые слова: защита информации, информационная безопасность, матрица связности графа, элементы сильной связности.

I.G. Drovnikova, E.A. Rogozin, A.V. Hvostov, A.A. Zmeev

ANALYSIS OF ARCHITECTURE AND CLUSTERING STRUCTURE OF AUTOMATIC SYSTEMS AT THE SUBSTANTIATION OF THE REQUIREMENTS TO INFORMATION SECURITY

The method of clustering the information structure of protected automated systems which allows significantly reduce the size of the problem of substantiation the requirements which is being solved is offered. The method is intended to substantiate quantitative requirements for the systems information protection based on the optimization of their structure.

Key words: protection of information, information security, matrix of graph connectivity, elements of strong connectivity.

Статья поступила в редакцию Интернет-журнала 12 февраля 2016 г.

Введение

Лавинообразный рост технологий в сфере вычислительной техники выявил ряд важных вопросов, связанных с обеспечением информационной безопасности (ИБ) автоматизированных систем (АС). В чрезвычайных ситуациях функционирования АС, в том числе при нарушении их ИБ, эти системы могут стать источником поражения людей, повреждения техники, материалов и т.д.

Функционирование АС включает ряд видов работ с информацией ограниченного доступа. ИБ России требует реализации комплекса мер обеспечения защиты информации (ЗИ) от несанкционированного доступа (НСД) [1-3].

Обоснование требований к системам защиты информации (СЗИ) АС является важнейшей задачей, выполняемой при их эксплуатации и построении [4-6]. ЗИ АС направлена на обеспечение защищённости их субъектов, обрабатываемой информации и информационных процессов.

Актуальность предложенной методики определяется существующим в настоящее время в теории и практике ИБ АС несоответствием между необходимостью обоснования требований к СЗИ и отсутствием научно-методического аппарата их количественного обоснования на основе оптимизации структуры данных систем [6].

Обобщённая математическая постановка задачи обоснования требований к ИБ АС

Обобщённая математическая постановка задачи может быть представлена в следующем виде [6].

Необходимо найти такой вектор значений показателей ИБ АС $\vec{K} = \langle k_1, k_2, ..., k_p \rangle$, который удовлетворяет совокупности исходных данных $\{Y, O_s, S, O_k, \Phi_c\}$ и обладает при этом характеристикой наилучшего, в смысле выбранного критерия, предпочтения, где:

k_i – числовая характеристика защищённости, связанная с эффективностью ЗИ монотонной зависимостью. Чем меньше k_i, тем лучше система при прочих равных условиях, то есть при неизменных $\{Y, O_s, S, O_k, \Phi_c, O_э\}$ и неизменных значениях остальных $m-1$ показателей качества защиты;

y – совокупность условий применения СЗИ вида $Y = \{Y_1, Y_2, Y_l\}$;

O_S – совокупность ограничений на структуру параметров СЗИ вида $O_s = \{O_{s1}, O_{s2}, ..., O_{sq}\}$;

s – комплект реализуемых или проектируемых СЗИ АС (вариантов построения системы) вида $S = \{S_1, S_2, ..., S_d\}$;

d – допустимое множество СЗИ, как существующих так и перспективных;

O_k – ограничения на показатели качества $O_k = \{O_{k1}, O_{k2}, ..., O_{kh}\}$. В случае выбора показателей качества в вероятностном виде ограничения принимают следующий вид: $0 < O_i < 1$ (в виде диапазона);

Φ_c – векторная функция связи показателей числовых характеристик защищённости с эффективностью АС.

Непосредственное решение задачи обоснования требований к СЗИ АС, вследствие большой структурной сложности, невозможно. Как показывает опыт решения подобных задач теории систем [5], целесообразно провести кластеризацию технической структуры АС. Полученные в результате кластеры позволят существенно снизить размерность решаемой задачи обоснования требований к ИБ и могут стать основой для проведения процедуры типизации архитектурных особенностей АС.

Формализация технической структуры АС

Суть метода состоит в формализации структуры АС в графоаналитическом представлении и заключается в построении вершинного графа $G_u(X,U)$, отображающего её структуру [6]. При этом элементам структуры ставят в соответствие вершины графа $X=\{x_1,x_2,...,x_n\}$. Связям между элементами ставятся в соответствие дуги графа $U=\{u_1,u_2,...,u_m\}$.

Методика кластеризации технической структуры АС при решении задачи обеспечения ИБ

Решение задачи декомпозиции информации возможно с применением алгоритма, разработанного в [7-10]:

1. Используется матрица смежности А графа $G_u(X,U)$, полученного на этапе формализации технической структуры АС.

2. Вычисляется матрица $R_1=A+E$, где E – единичная матрица, а "+" – знак логического сложения; R_1 – матрица первой достижимости, i-я строка которой представляет собой все ориентированные пути по графу из i-й вершины до всех остальных, если длинна пути равна одному ребру.

3. Определяется матрица $R_2=R_1^{*2}$, где знак "*" означает, что при вычислении $R_1\times R_1$ применяются логическое умножение и суммирование элементов матриц. Далее аналогично определяются все матрицы вплоть до $R=R_n=R_1^{*n}$, где R – матрица достижимости графа $G(X,U)$, i-я строка которой представляет все ориентированные пути по графу длиной от одного до n рёбер из i-й вершины ко всем остальным. Матрицы A и R имеют размерность $n\times n$. Если $R=Q$, где $Q=|q_{ij}|$, – универсальная матрица, в которой для всех i и j $q_{ij}=1$, то граф бисвязан, и декомпозиция системы невозможна, так как в системе существует одна сильносвязанная подсистема. При $R\neq Q$ декомпозиция системы осуществима. При этом необходимо определить матрицу основного (неориентированного) графа $G^0(X,U)$, соответствующего ориентированному графу $G(X,U)$ $R^0=(A+A^T+D)^{*n}$, где знак Т означает транспонирование.

4. Определяются связные подграфы ориентированного графа $G(X,U)$. Известно [8], что множество вершин связного подграфа, содержащего вершину i, определено единицами в i-й строке матрицы R^0. Если $R^0=Q$, то граф

$G(X,U)$ состоит из одного связного подграфа, и декомпозиция не реализуется. Если $R^0 \neq Q$, то производится упорядочивание вершин графа $G(X,U)$ (матрицы A) по связным подграфам. Далее необходимо образовать матрицу связности $C = R + R^T$. Здесь выполняется обычное арифметическое сложение. Выделяются из матрицы C бисвязные подграфы. Бисвязный подграф, содержащий вершину i, определён двойками в i-й строке матрицы C. Матрица A упорядочивается так, чтобы бисвязные подграфы образовывали квадратные подматрицы $E_\varphi \subset A$, $\varphi = 1, 2, \ldots, p$.

5. Образовывается матрица $R_+^0 = \left(A_+^0 + A_+^T + E_+\right)^{*\delta}$, где A_+^0 – матрица смежности подграфа с множеством вершин $V = W \Big| \bigcup_{\varphi=1}^{p} B_\varphi$ и B_φ – подмножество составных частей φ-й сильно связанной подсистемы.

Пример проведения расчётов кластеризации технической структуры АС при обосновании требований к ИБ

В качестве примера проведём декомпозицию технической структуры АС, представленной на рис. 1 в виде графа. Дуги графа представляют собой передаваемые между разными подразделениями АС информационные сообщения при выполнении работ с ними: (1, 5) и (6, 7) – агенты и т.п.

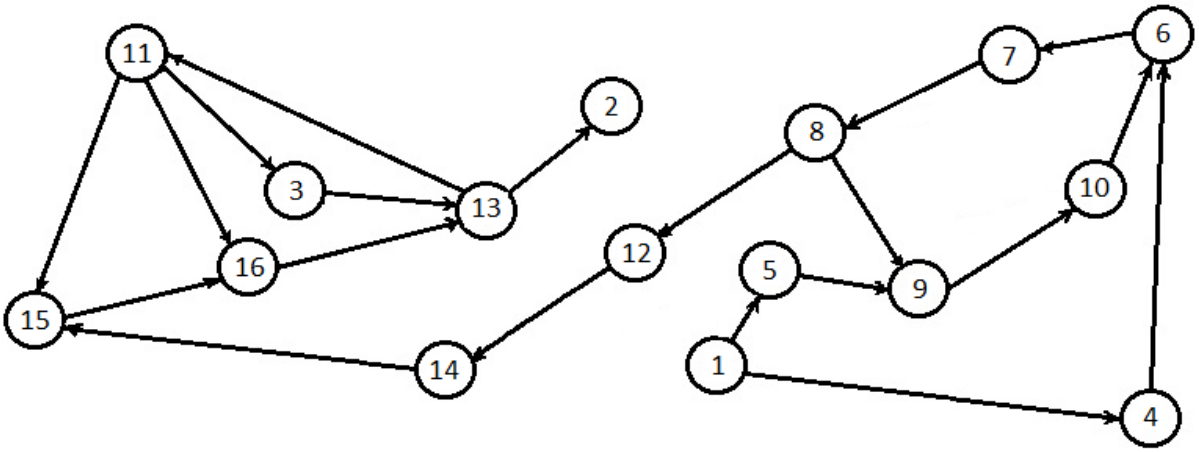

Рис. 1. Граф информационной структуры АС

Матрица смежности для графа, представленного на рис. 1, выглядит следующим образом:

$$A = \begin{vmatrix} 0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0 \\ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 \\ 0,0,0,0,0,0,0,0,0,0,0,1,0,0,0 \\ 0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0 \\ 0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0 \\ 0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0 \\ 0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0 \\ 0,0,0,0,0,0,0,0,1,0,0,1,0,0,0,0 \\ 0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0 \\ 0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0 \\ 0,0,1,0,0,0,0,0,0,0,0,0,0,0,1,1 \\ 0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0 \\ 0,1,0,0,0,0,0,0,0,0,1,0,0,0,0,0 \\ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0 \\ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1 \\ 0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0 \end{vmatrix}.$$

Далее в соответствии с методикой получаем матрицу достижимости графа степени n вида:

$$R = \begin{vmatrix} 1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1 \\ 0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0 \\ 0,1,1,0,0,0,0,0,0,0,1,0,1,0,1,1 \\ 0,1,1,1,0,1,1,1,1,1,1,1,1,1,1,1 \\ 0,1,1,0,1,1,1,1,1,1,1,1,1,1,1,1 \\ 0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1 \\ 0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1 \\ 0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1 \\ 0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1 \\ 0,1,1,0,0,0,0,0,0,0,1,0,1,0,1,1 \\ 0,1,1,0,0,0,0,0,0,0,1,1,1,1,1,1 \\ 0,1,1,0,0,0,0,0,0,0,1,0,1,0,1,1 \\ 0,1,1,0,0,0,0,0,0,0,1,0,1,1,1,1 \\ 0,1,1,0,0,0,0,0,0,0,1,0,1,0,1,1 \\ 0,1,1,0,0,0,0,0,0,0,1,0,1,0,1,1 \end{vmatrix}.$$

Так как R не является универсальной матрицей, в которой для всех i и j $q_{ij}=1$, то дальнейшая декомпозиция целесообразна. Матрица связности C для графа выглядит следующим образом:

$$C=\begin{vmatrix}
2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0\\
0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0\\
0,0,2,0,0,0,0,0,0,0,2,0,2,0,2,2\\
0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0\\
0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0\\
0,0,0,0,0,2,2,2,2,2,0,0,0,0,0,0\\
0,0,0,0,0,2,2,2,2,2,0,0,0,0,0,0\\
0,0,0,0,0,2,2,2,2,2,0,0,0,0,0,0\\
0,0,0,0,0,2,2,2,2,2,0,0,0,0,0,0\\
0,0,2,0,0,0,0,0,0,0,2,0,2,0,2,2\\
0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0\\
0,0,2,0,0,0,0,0,0,0,2,0,2,0,2,2\\
0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0\\
0,0,2,0,0,0,0,0,0,0,2,0,2,0,2,2\\
0,0,2,0,0,0,0,0,0,0,2,0,2,0,2,2
\end{vmatrix}.$$

Из анализа матрицы связности можно сделать вывод, что в составе информационной структуры рассматриваемой АС существуют два кластера информационных объектов, характеризуемых сильной связностью $B_1=\{6,7,8,9,10\}$ и $B_2=\{11,13,15,16\}$. При упорядочении матрицы связности C матрица связности R_+^0 будет иметь вид:

$$R_+^0=\begin{vmatrix}
1,0,1,1,0,0\\
0,1,0,0,0,0\\
1,0,1,1,0,0\\
1,0,1,1,0,0\\
0,0,0,0,1,1\\
0,0,0,0,1,1
\end{vmatrix}.$$

Анализ упорядоченной матрицы R_+^0 позволяет выделить из информационной структуры АС кластеры со слабой связностью $B_3=\{1,4,5\}$, $B_6=\{12,14\}$, $B_7=\{2\}$.

Результаты кластеризации технической структуры АС и их применение

Полученные с использованием методики кластеризации информационной структуры элементы сильной связности B_1, B_2 и элементы слабой связности B_3, B_4, B_5 являются исходными данными для обоснования комплектов СЗИ.

Существующие в настоящее время подходы к построению методического обеспечения для решения подобного рода задач (имеющиеся методики и алгоритмы) не носят комплексного характера, недостаточно учитывают взаимосвязь и взаимозависимость решаемых частных задач. В них также не уделяется достаточного внимания вопросам оптимальности формирования и выбора наиболее рациональных вариантов СЗИ, что не позволяет существенно снизить размерность решаемой задачи обоснования требований к ИБ АС с учётом заданных значений параметров эффективности. Предложенная методика кластеризации информационной структуры АС избавлена от указанных недостатков.

Заключение

В статье предложена методика кластеризации информационной структуры АС, позволяющая выделить элементы на основе анализа их связности в составе структуры. Полученные в результате кластеры дают возможность значительно снизить размерность решаемой задачи обоснования требований к ИБ АС и могут использоваться при проведении мероприятий, связанных с типизацией архитектуры защищённых АС, что позволит задавать количественные требования к СЗИ на основе их структурной оптимизации.

Литература

1. ***Гостехкомиссия*** РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: Воениздат, 1992.

2. ***Рогозин Е.А. и др.*** Защита информации в экономических информационных системах: учеб. пособие. Воронеж: ВЭПИ, 2011. 207 с.

3. ***ГОСТ*** Р 22.10.01-2001. Безопасность в чрезвычайных ситуациях. Оценка ущерба. Термины и определения (введён в действие 01.01.2002).

4. ***Домарев В.В.*** Безопасность информационных технологий. Методы создания систем защиты. Киев: ООО ТИД ДС, 2001. 688 с.

5. ***Герасименко В.А.*** Защита информации в автоматизированных системах обработки данных. В 2 кн.: Кн. 1. М.: Энергоатомиздат, 1994. 400 с.

6. ***Хвостов В.А. и др***. Методы и средства повышения защищённости автоматизированных систем: монография. Воронеж: Воронежский институт МВД России, 2013. 108 с.

7. ***Макаров О.Ю. и др.*** Метод построения информационной структуры автоматизированной системы при нормировании требований к информационной безопасности // Вестник Воронежского государственного технического университета. 2011. Т. 7. № 9. С. 61-64.

8. ***Оре О.*** Графы и их применение. М.: Мир, 1965. 174 с.

9. ***Нечипоренко В.И.*** Структурный анализ систем (эффективность и надёжность). М.: Сов. Радио, 1977. 216 с.

10. ***Кирсанов М.Н.*** Графы в MAPLE. Задачи, алгоритмы, программы. М.: изд-во ФИЗМАТЛИТ, 2007. 168 с.