Published in the Slovak Republic
European Journal of Computer Science
Has been issued since 2015.
ISSN: 2412-2033
E-ISSN 2500-1035
2017, 3(1): 17-22

DOI: 10.13187/ejcs.2017.1.17
www.ejournal39.com

The Task of Determining the Optimal Technological Scheme for the Operation of Information Security Systems

Simon Zh. Simavoryan [a, *], Arsen R. Simonyan [a], Elena I. Ulitina [a], Irina L. Makarova [a], Rafik A. Simonyan [b]

[a] Sochi State University, Russian Federation
[b] Kuban State University, Russian Federation

Abstract

The work deals with the problem of the substantiation of structure and technological schemes of functioning of systems of information protection in automated systems of information protection in automated data processing systems.

The problem of determining the optimal technological scheme for the operation of a GIS is considered. The problem is solved using the method of fuzzy dynamic programming. The conditionality of the application of this method is given in the text of the paper.

Keywords: information security, malicious acts, security system, schema, information processing, automated data processing system.

1. Введение

Одной из важнейших задач проектирования систем защиты информации (СЗИ) является задача обоснования структуры и технологических схем ее функционирования (Симаворян, Симонян и др., 2013). Анализ ожидаемых структур СЗИ неразрывно связан с анализом технологических схем функционирования самой автоматизированной системы обработки данных (АСОД), в том смысле, что технологическая схема функционирования АСОД является основным параметром, характеризующим ожидаемую структуру СЗИ. Таким образом, для анализа и оценки структуры СЗИ необходимо провести анализ и оценку технологических схем функционирования АСОД. Следовательно, задача анализа и оценки структуры СЗИ сводится к задаче нахождения оптимальной технологической схемы функционирования СЗИ для данной структуры АСОД.

2. Обсуждение

Универсальным способом формального представления развитой структуры АСОД является представление ее в виде графа, вершинами которого являются выделенные структурные элементы АСОД, а ребрами – линии передачи информации управления между ними. Стрелки на ребрах показывают направление передачи информации и управления. Следовательно, по структуре АСОД однозначно можно определить структуру СЗИ, а по ребрам – линии передачи информации и управления.

* Corresponding author
E-mail addresses: simsim58@mail.ru (S.Zh. Simavoryan)

Технологические схемы, по которым может осуществляться циркуляция информации в процессе автоматизированной ее обработки, имеют самую разнообразную структуру и разделяются на простой технологический маршрут; развитую (сложную), но хорошо структурированную схему; сложную неструктурированную схему. Хорошо структурированной технологической схемой обработки информации называется схема, которая может быть разложена на несколько простых маршрутов. Сложной неструктурированной схемой называется такая схема, которая не может быть разложена как на простые технологические маршруты, так и на хорошо структурированные схемы.

Простой технологический маршрут автоматизированной обработки информации задается упорядоченной последовательностью пар номеров типовых структурных компонент (ТСК), участвующих в обработке информации и их состояний, т.е. $\left\{J_s, K_S^{(j)}\right\}$, где переменный индекс S означает порядковый номер пары в последовательности. Данная последовательность формируется следующим образом (Герасименко, Малюк, 1997):

1) Пары упорядочиваются в строгом соответствии с последовательностью участвующих ТСК в обработке информации;

2) Если продолжительность обработки информации на одном и том же ТСК в одном и том же состоянии превышает стандартный интервал времени ΔT, то данная пара повторяется несколько раз с последовательно возрастающими значениями S;

3) Если в течении ΔT состояние ТСК изменяется, то последовательно формируется число пар по числу состояний ТСК, причем S растет в соответствии с последовательностью смены состояний;

4) Если на технологическом маршруте обработки информации встречаются циклы, то повторяющиеся пары заключаются в прямоугольные скобки, причем снаружи вверху у закрывающей скобки указывается число повторений цикла или выражение (условие), определяющее это число;

5) Если же на технологическом маршруте встречаются разветвления, то они описываются следующим образом:

1. Производится идентификация всех ветвлений (например, арабскими цифрами), причем начальный и конечный узлы каждого разветвления обозначаются одним и тем же идентификатором;

2. Все пары, входящие в одну и ту же ветвь, заключаются в фигурные скобки, причем снаружи вверху у открывающей и закрывающей скобок проставляется идентификатор ветви.

Для простого технологического маршрута выделяется следующие участки технологического процесса: линейный участок, циклический участок (который может быть трансформирован в линейный путем повторения зацикленного участка столько раз, сколько предусматривается повторение циклического участка) и ветвящийся участок.

Для определения оптимальной технологической схемы функционирования СЗИ применим метод нечеткого динамического программирования. Применение этого метода обуславливается тем, что:

- показатели уязвимости информации (защищенности) имеют лингвистический характер;
- зависимости показателей защищенности информации от средств (задач) защиты информации имеют качественный, лингвистический характер;
- некоторые ограничения, предъявляемые к средствам (задачам) защиты информации в сложных неструктурированных схемах полностью трудно формализуемы.

Перейдем к изложению задачи. Пусть СЗИ, состоящая из N подсистем, задана матрицей связей $A = \|a_{ij}\|(i, j = \overline{1, N})$, где

$$a_{ij} = \begin{cases} 1, \text{если j-ая подсистема связана с i-ой подсистемой защиты информации,} \\ 0, \text{в противном случае,} \end{cases}$$

Определим множество $X_{ij}^{\alpha} \subseteq X$ как возможное множество состояний защищенности информации при ее передаче из i-го ТСК в j-ый, $\alpha \in [0, 1], X_{ij}^{\alpha} \subseteq [0,1]$- подмножества

уровняα, $X \subseteq [0,1]$- конечное множество всевозможных состояний защищенности информации при его хранении, обработке и передаче из произвольного ТСК АСУ СН в любой другой ТСК. Элементы множества X_{ij}^{α} обозначим через $x_{ij}^{\alpha}, x_{ij}^{\alpha} \in X_{ij}^{\alpha}$.

Введем конечное множество $Y_{ij} = \{y_{ij}\}$ способов (вариантов) передачи информации из i-го ТСК в j-ый. Ясно, что для каждого способа передачи информации y_{ij} используется свой способ управления обеспечением защиты информации U_{ij}, осуществляемый i-ой и j-ой подсистемами защиты информации в АСОД. Каждый способ управления характеризуется совокупностью ограничений (характеристик) $C_{\gamma m_\gamma}^{ij}$, $\gamma = \overline{1,e}$, каждая из которых принимает m_γ значений, $m_\gamma = \overline{1,r_\gamma}$. Функция принадлежности $M_{C_{\gamma m_\gamma}}^{ij}(U_{ij})$ характеризует степень выполнения ограничения $C_{\gamma m_\gamma}^{ij}$ для конкретного способа управления обеспечением защиты информации. Обобщенная функция принадлежности U_{ij}, характеризующая степень выполнения ограничений определяется как

$$M(U_{ij}) = \min\left\{\beta_1 \sum_{m_1}^{r_1} \alpha_{1_{m_1}} \cdot M_{C_{1_{m_1}}}^{ij}(U_{ij}), \ldots, \beta_e \sum_{m_e}^{r_e} \alpha_{e_{m_e}} M_{C_{e_{m_e}}}^{ij}(U_{ij})\right\},$$

где β_γ - весовой коэффициент $\gamma -$ ойлингвистической переменной $\left(\sum_{\gamma=1}^{e} \beta_\gamma = 1\right)$, а $\alpha_{\gamma_{m_\gamma}}$ - весовой коэффициент m_γ-го значения $\gamma -$ ой переменной $\left(\sum_{m_\gamma}^{r_e} \alpha_{\gamma_{m_\gamma}} = 1\right)$. Если $M(U_{ij}) = 0$, то это означает, что выбранный способ управления не удовлетворяет заданным ограничениям.

Предположим, что информация, передаваемая из j-го ТСК АСОД $(j = i_1)$, передается в i-ый $(i = i_k)$, последовательно проходит через компоненты $i_2, i_3, \ldots, i_{k-1}$. Это означает, что в защите информации должны участвовать все подсистемы защиты информации в этих ТСК. Тогда множество $U_{i_k i_{k-1}}$можно представить как прямое произведение множеств $U_{i_2 i_1}, U_{i_3 i_2}, \ldots, U_{i_k i_{k-1}}$. Введем функцию f перехода состояния защищенности информации на ij-ом участке защиты информации, где

$$X_{ij} = f(x_j, u_{ij}),$$
$$X_i = \min_j \{X_{ij}\}. \qquad (*)$$

Рассмотрим управление защитой информации при передаче информации из i-го ТСК в j-ый. Пусть задана нечеткая цель управления в виде нечеткого подмножества G_{i_k} множества X, представляющая собой нечеткое ограничение на состояние защищенности информации в i_k-ом ТСК. В соответствии с подходом Беллмана-Заде (Беллман, Заде, 1976) нечеткое решение достижения нечеткой цели G_{i_k} можно представить в виде следующей функции:

$$M_D(U_{i_2 i_1}, \ldots, U_{i_k i_{k-1}}) = \min\left\{M_{i_2 i_1}(U_{i_2 i_1}), \ldots, M_{i_k i_{k-1}}(U_{i_k i_{k-1}}), M_{G_{i_k}}(X_{i_k})\right\}.$$

При этом управления $U_{i_2 i_1}, \ldots, U_{i_k i_{k-1}}$ удовлетворяют нечетким ограничениям и обеспечивают достижение нечеткой цели G_{i_k}.

Постановка задачи. Найти из множества D последовательность $U_{i_2 i_1}, \ldots, U_{i_k i_{k-1}}$, имеющую максимальную степень принадлежности нечеткому решению D, т.е.

$$M_D(U_{i_2 i_1}, \ldots, U_{i_k i_{k-1}}) = \max_{U_{i_2 i_1}, \ldots, U_{i_k i_{k-1}}} \min\left\{M_{i_2 i_1}(U_{i_2 i_1}), \ldots, M_{i_k i_{k-1}}(U_{i_k i_{k-1}}), M_{G_{i_k}}(X_{i_k})\right\}.$$

$$M_D(U_{i_2 i_1}, \ldots, U_{i_k i_{k-1}}) = \max_{U_{i_k i_{k-1}}} \min$$

$$\left\{M_{i_2 i_1}(U_{i_2 i_1}), \ldots, M_{i_k i_{k-1}}(U_{i_k i_{k-1}}), \max_{U_{i_2 i_1}, \ldots, U_{i_k i_{k-1}}} \left\{M_{i_k i_{k-1}}(U_{i_k i_{k-1}}), M_{G_k}\left(f(X_{i_k i_{k-1}}, U_{i_k i_{k-1}})\right)\right\}\right\}$$

Решение задачи

Введем обозначение

$$M_{G_{i_{k-1}}}(X_{i_{k-1}}) = \max_{U_{i_k i_{k-1}}} \min \left\{ M_{i_k i_{k-1}}(U_{i_k i_{k-1}}), M_{G_{i_k}}\left(f(X_{i_k i_{k-1}}, U_{i_k i_{k-1}})\right)\right\}.$$

Определим функцию $M_{G_{i_{k-1}}}(X_{i_{k-1}})$ как функцию принадлежности нечеткой цели G_{i_k} при защите информации на участке от i_1-го ТСК до i_{k-1}-го ТСК. Суть этой функции следующая. Пусть $U_{i_2 i_1},.., U_{i_{k-1} i_{k-2}}$ - множество управлений на участке $i_{k-2} i_{k-1}$, G_{i_k}- цель защиты информации. Пусть переход системы защиты информации из состояния X_{i_1} в состояние $X_{i_{k-1}}$ определяется системой уравнений (*). Тогда ясно, что выбором управления $U_{i_k i_{k-1}}$, можно добиться максимальной степени достижения заданной цели G_{i_k} на $i_{k-2} i_{k-1}$ участке защиты информации равной $M_{G_{i_{k-2}}}(X_{i_{k-1}})$.

Продолжая эти рассуждения для t-ых ТСК $(t = k-1, k-2,..., 1)$, получим систему рекуррентных соотношений

$$M_{G_{i_{k-v}}}(X_{i_{k-v}}) = \max_{U_{i_{k-v}}} \min \left\{ M_{i_{k-v+1} i_{k-v}}(X_{i_{k-v+1} i_{k-v}}), M_{G_{i_{k-v+1}}}(X_{i_{k-v+1}})\right\},$$

$$X_{i_{k-v+1}} = f(X_{i_{k-v+1} i_{k-2}}, U_{i_{k-v+1} i_{k-2}}), v = \overline{o, k-2}.$$

С помощью этих соотношений получаем функции $\overline{U}_{i_k i_{k-1}}(X_{i_k i_{k-1}}), \overline{U}_{i_{k-1} i_{k-2}}(X_{i_{k-1} i_{k-2}}),..., \overline{U}_{i_2 i_1}(X_{i_2 i_1})$, затем по заданному начальному состоянию $X_{i_2 i_1}$защищенности информации вычисляем в обратном порядке максимизирующее решение

$$U_{i_2 i_1}(X_{i_2 i_1}), \overline{U}_{i_3 i_2} = \overline{U}_{i_3 i_2}\left(f(X_{i_2 i_1}, \overline{U}_{i_2 i_1})\right), \overline{U}_{i_4 i_3} = \overline{U}_{i_4 i_3}\left(f\left(f(X_{i_2 i_1}, \overline{U}_{i_1 i_1}), \overline{U}_{i_3 i_2}\right)\right) ...$$

Ясно, что нечеткая цель $G_{i_1} \subseteq X_1$, полученная с помощью системы рекуррентных соотношений, определяет множество нечетких состояний защищенности информации, которые при оптимальном управлении приводят к конечной цели G_{i_k}.

3. Результаты

Рассмотрена задача определения оптимальной технологической схемы функционирования СЗИ. Задача решена с помощью применения метода нечеткого динамического программирования. Обусловленность применения этого метода приведена в тексте работы.

4. Заключение

Задача определения оптимальной технологической схемы функционирования СЗИ во всех режимах автоматизированной обработки информации тесно связана с задачами интеллектуального противоборства злоумышленников и службы защиты информации (Симаворян и др., 2014), а именно: с задачей эффективного поиска нечеткого образа злоумышленника, которая является неотъемлемой частью интеллектуальной деятельности службы защиты информации в АСОД (Simavoryan et al., 2016); с задачей поиска нечеткого образа злоумышленника методом итераций (Simavoryan et al., 2016), с задачей создания условий для теоретического и практического решения задачи автоматизированного поиска образа интеллектуального злоумышленника в АСОД (Simavoryan et al., 2017). Вышеперечисленные работы требуют дальнейшего обобщения на базе системного подхода к проектированию интеллектуальных систем защиты информации (Симаворян и др., 2013).

5. Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-01-00527.

Литература

Беллман, Заде, 2013 – *Беллман Р., Заде Л.* Принятие решений в расплывчатых условиях. Мир, М, 1976, 46 с.

Герасименко, Малюк, 1997 – *Герасименко В.А., Малюк А.А.* Москва: МИФИ, 1997. 537 с. ISBN: 5-88852-010-1.

Симаворян и др., 2013 – *Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян Р.А.* Системный подход к проектированию интеллектуальных систем защиты информации // *Известия Сочинского государственного университета*, 2013, № 4-2(28), с. 128-132.

Симаворян и др., 2014 – *Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян А.Р.* Исследование интеллектуального противоборства злоумышленников и службы защиты информации в АСОД // *Известия Сочинского государственного университета*, 2014, № 4-1 (32). С. 15-23.

Simavoryan et al., 2016 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Samarin V.I., Simonyan R.A., Kardashyan M.A.* Enhancing operational efficiency of the fuzzy image of the attacker"s method of iterations // *Modeling of Artificial Intelligence*. 2016. № 4 (12). С. 187-193.

Simavoryan et al., 2017 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A., Pilosyan E.A., Kornienko N.A.* Search fuzzy image of the attacker based on the use of automatic classification methods // *Modeling of Artificial Intelligence*. 2017. № 4 (1). С. 29-38.

Simavoryan et al., 2016 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I.* Creating the Conditions for the Theoretical and Practical Solution of the Problem of Automated Intelligent Search for the Attacker's Image in ADPS // *Modeling of Artificial Intelligence*. 2016. Vol. 11, Is. 3, pp. 166-176.

References

Bellman, Zade, 2013 – *Bellman R., Zade L.* (1976). Prinyatie reshenii v rasplyvchatykh usloviyakh [Decision-making under vague conditions]. Mir, M, 46 s.

Gerasimenko, Malyuk, 1997 – *Gerasimenko V.A., Malyuk A.A.* (1997). Moskva: MIFI [Moscow: MEPhI]. 537 s. ISBN: 5-88852-010-1.

Simavoryan i dr., 2013 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A.* (2013). Sistemnyi podkhod k proektirovaniyu intellektual'nykh sistem zashchity informatsii [A systematic approach to the design of intelligent information security systems]. *Izvestiya Sochinskogo gosudarstvennogo universiteta*, 2013, № 4-2(28), s. 128-132.

Simavoryan i dr., 2014 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan A.R.* (2014). Issledovanie intellektual'nogo protivoborstva zloumyshlennikov i sluzhby zashchity informatsii v ASOD [Investigation of the intellectual confrontation of malefactors and information security services in ASAD]. *Izvestiya Sochinskogo gosudarstvennogo universiteta*, № 4-1 (32). pp. 15-23.

Simavoryan et al., 2016 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Samarin V.I., Simonyan R.A., Kardashyan M.A.* (2016). Enhancing operational efficiency of the fuzzy image of the attacker"s method of iterations. *Modeling of Artificial Intelligence*. № 4 (12). pp. 187-193.

Simavoryan et al., 2017 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A., Pilosyan E.A., Kornienko N.A.* (2017). Search fuzzy image of the attacker based on the use of automatic classification methods. *Modeling of Artificial Intelligence*. № 4 (1). pp. 29-38.

Simavoryan et al., 2016 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I.* (2016). Creating the Conditions for the Theoretical and Practical Solution of the Problem of Automated Intelligent Search for the Attacker's Image in ADPS. *Modeling of Artificial Intelligence*. Vol. 11, Is. 3, pp. 166-176.

Задача определения оптимальной технологической схемы функционирования систем защиты информации

Симон Жоржевич Симаворян [a] , [*], Арсен Рафикович Симонян [a], Елена Ивановна Улитина [a], Ирина Леонидовна Макарова [a], Рафик Арсенович Симонян [b]

[a] Сочинский государственный университет, Российская Федерация
[b] Кубанский государственный университет, Российская Федерация

Аннотация. Работа посвящена задаче обоснования структуры и технологических схем функционирования систем защиты информации в автоматизированных системах защиты информации в автоматизированных системах обработки данных.

Рассмотрена задача определения оптимальной технологической схемы функционирования СЗИ. Задача решена с помощью применения метода нечеткого динамического программирования. Обусловленность применения этого метода приведена в тексте работы.

Ключевые слова: информационная безопасность, злоумышленные действия, система защиты информации, схема обработки информации, автоматизированная система обработки данных.

[*] Корреспондирующий автор
Адреса электронной почты: simsim58@mail.ru (С.Ж. Симаворян)