

БЕЗОПАСНОСТЬ**Качественные показатели безопасности информационных ресурсов****Qualitative indicators of information resources security**

Ключевые слова: глобальные информационные системы – global information systems; информационные ресурсы – information resources; мониторинг безопасности – monitoring of security; показатели защищенности – protection criteria.

Решение проблемы оценки качественных показателей информационных систем, влияющих на конкурентоспособность в нише информационных технологий, следует рассматривать с системных позиций и, прежде всего, с количественной оценкой таких свойств, как «защищенность» и «оснащенность» информационных систем.

Solution of valuation problem of quality factors – information systems, having an effect on competitive ability in the segment and information technologies, should be considered from system positions and, first of all, with quantitative assessment of such features as IS «safety» and «implementation».

Известна система показателей, оценивающая эффективность использования, как информационных ресурсов (далее – ИР) [1, 2], так и механизмов защиты (далее – МЗ) [3] в информационных системах (ИС) корпоративного уровня (уровень микросистем). Актуальна задача оценки качественных показателей ИС макро- и метауровней [4]. Для оценки уровня глобальных информационных систем (ГИС) информационных технологий применима система показателей, аналогичная используемой для оценки защищенности ИС.

Известны показатели для оценки информационных ресурсов [4]: индекс технологической оснащенности, индекс прозрачности коммуникаций, индекс информационного общества и т.д. Индекс технологической оснащенности – ИТО [5] интегрирует 5 распространенных показателей ВТ-продукции: персональные компьютеры, мобильные телефоны, Интернет-хосты, факсы, телевизоры. Индекс прозрачности коммуникаций – ИПК, разработанный специалистами National

СУХАНОВ / SUHANOV A.**Андрей Вячеславович**

(AVSuhanov@eureca.ru)

доктор технических наук, профессор, заведующий кафедрой Санкт-Петербургского университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург

АНДРОНОВ / ANDRONOV A.**Алексей Викторович**

(a_andronov@eureca.ru)

аспирант Санкт-Петербургского национального научно-исследовательского университета информационных технологий, механики и оптики, инженер-программист отдела разработки программного обеспечения ЗАО «Эврика», Санкт-Петербург

КРЫЛОВ / KRYLOV A.**Александр Изотович**

(a_krylov@eureca.ru)

аспирант Санкт-Петербургского национального научно-исследовательского университета информационных технологий, механики и оптики, начальник испытательного центра управления специальных работ ЗАО «Эврика», Санкт-Петербург

Science Foundation [6], предназначен для оценки степени использования ИТ в процессах взаимодействия населения, бизнеса, предпринимателей и властей. Индекс информационного общества (Information Society Index) – ИИО [7] оценивает темпы роста в области создания, распространения и использования ИТ, исходя из 23 переменных, объединенных в инфраструктуры: компьютерную, информационную, социальную и Интернет. Недостаток названных показателей – отсутствие учета ряда важных для анализа составляющих: материальных затрат, необходимых для развития и сопровождения инфраструктуры ГИС, распределения ИР по иерархии ИС [3].

Группа показателей информационной оснащенности может быть детализирована за счет введения

экспертных оценок в контексте иерархии ГИС для различных групп стран и учета материальных затрат, необходимых для эксплуатации и модернизации инфраструктуры ГИС. Формируется группа показателей информационной безопасности (ИБ), учитывающих распределение механизмов защиты по иерархии ГИС и величину предотвращенного ущерба на заданном множестве угроз. Рейтинговые показатели уровня ИТ получаются путем объединения двух названных групп показателей.

Известные показатели ИТО, ИПК и ИИО можно представить в виде матрицы экспертных оценок распределения ИР по странам мира – «страны-ИР» – и дополнить экспертными оценками распределения ИР по иерархии ГИС внутри страны (группы стран с аналогичным уровнем развития ИТ) в виде матриц «ИР – иерархия». Аналогично для ГИС показатели ИБ можно представить в виде матрицы достоверности нейтрализации угроз механизмами защиты «МЗ – угрозы» и матрицы достоверности «угрозы – эшелоны». Рассмотрим подход к оценке защищенности ИС, который может быть распространен на информационные системы макро- и метаяуровней.

Показатели защищенности информационных систем. Результаты экспертных оценок могут быть представлены в виде матрицы достоверности «угрозы – механизмы защиты» ME :

$$ME_{m \times n} = \begin{pmatrix} me_{11} & me_{12} & \dots & me_{1n} \\ me_{21} & me_{22} & \dots & me_{2n} \\ \dots & \dots & \dots & \dots \\ me_{m1} & me_{m2} & \dots & me_{mn} \end{pmatrix},$$

где m – число механизмов защиты, n – число эшелонов средств защиты.

Активность эшелона средств МБ по нейтрализации угроз, входящих в систему правил в качестве посылок, определяется строкой показателей, представленных, например, строкой показателей значимости эшелона в средствах защиты,

$$x_j = \sqrt[m]{\sum_{i=1}^m me_{ij}}, \quad j = 1, \dots, n, \quad \text{нормированных,}$$

например, по значению максимального из x_j , $j = 1, \dots, n$ или по значению суммы элементов строки показателей значимости $\sum_{j=1, \dots, n} x_j$. Сопоставление показателей в пределах строки позволяет выявить наиболее задействованные эшелоны средств МБ по нейтрализации множества действующих на ИС угроз.

Аналогично по матрице достоверности использования механизмов защиты для нейтрализации угроз можно получить столбец показателей активности использования отдельного механизма защиты во всех эшелонах средств МБ для нейтрализации последствий действующего множества угроз

$$x_i = \sqrt[n]{\sum_{j=1}^n me_{ij}}, \quad i = 1, \dots, m.$$

Сопоставление показателей в пределах столбца позволяет выявить наиболее задействованные механизмы защиты средств МБ. Анализ показателей матрицы достоверности «угрозы – МЗ» дает возможность обосновать целесообразность использования механизма защиты в составе соответствующего эшелона средств МБ.

Использование экспертных оценок и последующее отражение в структуре нейронечеткой сети априорного опыта экспертов ИБ сопровождается проверкой на непротиворечивость результатов опроса экспертов. Непротиворечивость оценок экспертов ИБ может быть обеспечена применением метода экспертных оценок матрицы нечетких отношений [8] или метода расчета максимального собственного значения матрицы парных сравнений [9].

Приведенные выше показатели будут более информативными, если учитывать не только достоверность использования механизмов защиты в структуре средств МБ, но и показатели потенциального ущерба, возникающего в результате реализации атак на ИС, который может быть предотвращен средствами МБ. С этой целью по аналогии с [8] оценку защищенности можно косвенно связать с предотвращением ущерба ИС и использовать экспертные оценки для сопоставления, с одной стороны, множества угроз с потенциальным ущербом от их реализации, с другой – размера потенциального ущерба с местом реализации угрозы в структуре ИС.

Показатели оснащенности ИС информационными ресурсами. Рассмотрим первую группу показателей, связанных с уровнем развития информационного общества. Исходные данные – результаты экспертных оценок распределения ИР по странам (группам стран) представляют в виде матрицы CR «страны – ИР»:

$$CR_{m \times p} = \begin{pmatrix} cr_{11} & cr_{12} & \dots & cr_{1p} \\ cr_{21} & cr_{22} & \dots & cr_{2p} \\ \dots & \dots & \dots & \dots \\ cr_{m1} & cr_{m2} & \dots & cr_{mp} \end{pmatrix},$$

БЕЗОПАСНОСТЬ

где m – число стран, p – число показателей ИР. Аналогично формируют матрицу RH «ИР – иерархия» распределения ИР по иерархии ГИС стран, относящихся к одной группе по уровню развития ИТ:

$$RH_{p \times n} = \begin{pmatrix} rh_{11} & rh_{12} & \dots & rh_{1n} \\ rh_{21} & rh_{22} & \dots & rh_{2n} \\ \dots & \dots & \dots & \dots \\ rh_{p1} & rh_{p2} & \dots & rh_{pn} \end{pmatrix},$$

где p – число показателей ИР, n – число уровней иерархии в ГИС страны.

Формируют матрицу материальных затрат на эксплуатацию и модернизацию ГИС страны «иерархия – ИР» HR :

$$HR_{n \times p} = \begin{pmatrix} hr_{11} & hr_{12} & \dots & hr_{1p} \\ hr_{21} & hr_{22} & \dots & hr_{2p} \\ \dots & \dots & \dots & \dots \\ hr_{n1} & hr_{n2} & \dots & hr_{np} \end{pmatrix},$$

где n – число уровней иерархии в ГИС страны, p – число показателей ИР, и матрицу «ИР – страны» RC :

$$RC_{p \times m} = \begin{pmatrix} rc_{11} & rc_{12} & \dots & rc_{1m} \\ rc_{21} & rc_{22} & \dots & rc_{2m} \\ \dots & \dots & \dots & \dots \\ rc_{p1} & rc_{p2} & \dots & rc_{pm} \end{pmatrix},$$

где p – число показателей ИР, m – число подлежащих анализу стран.

Интегральные показатели получают в результате операций над матрицами. В частности, умножение матриц «страны – ИР» CR и «ИР – иерархия» позволяет получить матрицу «страны – иерархия» CH размерностью $m \times n$ – матрицу распределения ИР по странам и иерархии ГИС:

$$CH_{m \times n} = \begin{pmatrix} ch_{11} & ch_{12} & \dots & ch_{1n} \\ ch_{21} & ch_{22} & \dots & ch_{2n} \\ \dots & \dots & \dots & \dots \\ ch_{m1} & ch_{m2} & \dots & ch_{mn} \end{pmatrix},$$

где m – число стран, n – число уровней иерархии в ГИС страны, а умножение матриц материальных затрат HR и RC – матрицу материальных затрат «иерархия – страны» HC размерностью $n \times m$, отражающую распределение затрат на эксплуатацию и модернизацию ГИС:

$$HC_{n \times m} = \begin{pmatrix} hc_{11} & hc_{12} & \dots & hc_{1m} \\ hc_{21} & hc_{22} & \dots & hc_{2m} \\ \dots & \dots & \dots & \dots \\ hc_{n1} & hc_{n2} & \dots & hc_{nm} \end{pmatrix},$$

где n – число уровней иерархии в ГИС страны, m – число стран.

Промежуточные оценки в виде строки и столбца интегральных показателей значимости характеризуют распределение IP по иерархии ГИС и по группе стран, а также позволяют оценить материальные затраты на поддержание информационной инфраструктуры в разрезе стран и иерархии ГИС.

Дальнейшие операции над матрицами CH и HC дают возможность обобщить в диагональных элементах итоговой матрицы как показатель распределения IP , так и материальных затрат на поддержание информационной инфраструктуры стран.

Умножением матрицы распределения ресурсов CH и материальных затрат HC получают квадратную матрицу затрат на поддержание информационной инфраструктуры ГИС при данном распределении IP – матрицу «страны – страны» CC :

$$CC_{m \times m} = \begin{pmatrix} cc_{11} & cc_{12} & \dots & cc_{1m} \\ cc_{21} & cc_{22} & \dots & cc_{2m} \\ \dots & \dots & \dots & \dots \\ cc_{m1} & cc_{m2} & \dots & cc_{mm} \end{pmatrix},$$

где m – число стран, а умножением матрицы HC и матрицы CH получают квадратную матрицу затрат на поддержание информационной инфраструктуры ГИС при данном распределении IP – матрицу «иерархия – иерархия» HH :

$$HH_{n \times n} = \begin{pmatrix} hh_{11} & hh_{12} & \dots & hh_{1n} \\ hh_{21} & hh_{22} & \dots & hh_{2n} \\ \dots & \dots & \dots & \dots \\ hh_{n1} & hh_{n2} & \dots & hh_{nn} \end{pmatrix},$$

где n – число уровней иерархии в ГИС страны.

Для матрицы CC в качестве обобщающего показателя можно рассматривать вектор, образованный диагональными элементами $cc_{ij} = c_i$, $i = j = 1, \dots, m$, матрицы – вектор затрат на поддержание информационной инфраструктуры ГИС при данном распределении $IP C_{1xm} = (c_1, c_2, \dots, c_m)$, а для матрицы HH – вектор из ее диагональных элементов $hh_{ij} = h_i$, $i = j = 1, \dots, n$ – вектор затрат на поддержание информационной инфраструктуры ГИС при данном распределении $IP H_{1xn} = (h_1, h_2, \dots, h_n)$.

В качестве интегральных показателей информационной оснащённости в разрезе группы стран можно использовать рейтинговый показатель R_C – длину m -мерного вектора C_{1xm} :

$$R_C = |C_{1xm}| = \sqrt{\sum_{i=1}^m c_i^2}, \quad i = 1, \dots, m,$$

а в разрезе иерархии ГИС – рейтинговый показатель R_H – длину n -мерного вектора H_{1xn} :

$$R_H = |H_{1xn}| = \sqrt{\sum_{i=1}^n h_i^2}, \quad i = 1, \dots, n.$$

Для математического и методологического обоснования экономической целесообразности затрат на модернизацию ГИС необходим комплекс показателей, связывающих затраты на модернизацию информационных ресурсов ГИС и разработку средств обеспечения безопасности с эффективностью решения заданного множества задач, включая обеспечение безопасности ГИС. Комплекс разнородных показателей, интегрированный в рейтинговый показатель, позволяет использовать рейтинг в качестве целевой функции алгоритма оптимизации ГИС и адекватно отражает, как технические параметры, так и экономические параметры эффективности информационной системы.

Литература

1. Николаев А.Ю., Любимов А.В., Суханов А.В. Автоматизация оценки объектов информатизации в соответствии с требованиями руководящих документов «Безопасность информационных технологий» Гостехкомиссии России // IV Всероссийская конференция «Обеспечение информационной безопасности. Региональные аспекты». – Сочи, 2005. – С. 27–31.
2. Нестерук Ф.Г., Осовецкий Л.Г., Штрик А.А., Нестерук Г.Ф., Жигулин Г.П. К оценке информационных ресурсов и безопасности глобальных компьютерных систем // Перспективные информационные технологии и интеллектуальные системы. – 2004. – № 4. – С. 25–31.

3. Нестерук Ф.Г., Осовецкий Л.Г., Нестерук Ф.Г. К оценке защищенности систем информационных технологий // Перспективные информационные технологии и интеллектуальные системы. – 2004. – № 1. – С. 31–41.
4. Дрожжинов В., Штрик А. Роль ИТ в снижении уровня непрозрачности экономики // PC WEEK/RE. – 2002. – № 15.
5. Rodriguez F., Wilson E. Are Poor Countries Losing the Information Revolution? // InfoDev Working Paper. – May 2000. – University of Maryland at College Park.
6. Science and Engineering Indicators – 2000. – National Science Foundation (NSF). – www.nsf.gov/sbe/srs/seind00/frame.htm.
7. Information Society Index // WorldPaper. – January 2001. – www.worldpaper.com.
8. Жижелев А.В., Панфилов А.П., Язов Ю.К., Батищев Р.В. К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств // Известия вузов. – Приборостроение. – 2003. – Т. 46. – № 7. – С. 22–29.
9. Асаи К., Ватада Д., Иваи С. и др. Прикладные нечеткие системы / Под ред. Т. Тэрано, К. Асаи, М. Сугэно. – М.: Мир, 1993.