Совершенствование системы обеспечения ИБ органов власти субъекта Российской Федерации

En **Improvement of information security in the authorities of Russian Federation**

S. A. Golovin,
OOO «Gazinformservice»
sergo404@mail.ru

A. N. Lulchenko,
OAO «Kontsern „Oceanpribor"»
sch00l@gkspr.ru

D. V. Shved,
ITMO University
dasha@cit.ifmo.ru

This article brings to reader's attention the problems of information security in the authorities of the Russian Federation. The effectiveness of this system is largely determined by the quality of the distributed database. The article provides a mathematical formulation of the optimization problem of rational justification embodiment of a logical structure of a distributed database in the Russian Federation government. The practical implementation of the proposed formulation of the problem will provide high efficiency of decisions made in the system of information security in the Russian Federation government.

Keywords: information-analytical system, distributed database, the logical structure of database, information security, data objects, design stages, indicator of efficiency

Своевременность и качество принимаемых решений в системах информационной безопасности, как правило, определяется уровнем автоматизации процессов управления их функционированием. В статье рассматриваются проблемы автоматизации системы обеспечения информационной безопасности органов власти субъекта Российской Федерации. Основным направлением решения этой проблемы является создание региональной аналитической системы обеспечения информационной безопасности. Эффективность функционирования такой системы во многом определяется качеством создаваемой распределенной базы данных. В статье приводится математическая постановка оптимизационной задачи обоснования рационального варианта построения логической структуры распределенной базы данных распределенной информационно-аналитической системы обеспечения информационной безопасности органов власти субъекта Российской Федерации. Практическая реализация предлагаемой постановки задачи позволит сформировать рациональную структуру распределенной базы данных, которая обеспечит высокую эффективность решений, принимаемых в системе обеспечения информационной безопасности в органах власти субъекта Российской Федерации.

Ключевые слова: информационная безопасность, информационно-аналитическая система, информационное обеспечение, распределенная база данных, логическая структура базы данных, оценка эффективности, обеспечение информационной безопасности, органы власти, объекты данных, стадии проектирования, показатель эффективности, функция принадлежности

Сергей Алексеевич Головин,
ООО «Газинформсервис»
sergo404@mail.ru

Андрей Николаевич Люльченко,
ОАО «Концерн „Океанприбор"»
sch00l@gkspr.ru

Дарья Викторовна Швед,
Университет ИТМО
dasha@cit.ifmo.ru

В соответствии с руководящими документами в сфере обеспечения безопасности ключевых систем информационной инфраструктуры, системы органов государственной власти и органов местного самоуправления относятся к критически важным сегментам информационной и телекоммуникационной инфраструктуры Российской Федерации. Для реализации требований по обеспечению безопасности информации в субъектах Российской Федерации создаются системы защиты информации регионального, муниципального и объектового уровней. В состав этих систем, в зависимости от региона, может входить:

- от 15 до 20 систем обеспечения информационной безопасности

(СОИБ) исполнительных органов государственной власти (ИОГВ);
- порядка 18 СОИБ органов местного самоуправления (ОМСУ);
- более 20 СОИБ организаций подведомственных ИОГВ (далее – организации) [1].

Система обеспечения информационной безопасности должна обеспечивать выполнение следующих основных задач:
- сбор, обработку, анализ, хранение и передачу информации об обобщенных параметрах состояния защищенности объектов защиты органов власти субъектов Российской Федерации;
- информационную поддержку работ, выполняемых в целях подготовки и реализации мер по обеспечению безопасного функционирования объектов защиты;
- подготовку интегральных оценок (моделей) оценки состояния информационной безопасности в органах власти и организациях региона;
- ведение информационных баз данных для обеспечения поддержки принятия и реализации управленческих решений по обеспечению информационной безопасности в регионе;
- формирование единого информационного пространства системы обеспечения информационной безопасности в органах власти и организациях региона.

Успешная реализация таких задач возможна лишь при выполнении следующих условий: адекватном развитии региональной сетевой инфраструктуры и применении действенных технологий создания распределенной информационно-аналитической системы (РИАС).

В рамках указанного направления создания региональной системы управления информационной безопасностью существует необходимость решения такой важной практической задачи как совершенствование информационного обеспечения деятельности подразделений (служб) по защите информации с использованием современных информационных технологий.

Ее решение, в свою очередь, обусловливает актуальность исследования вопросов создания распределенной информационно-аналитической системы обеспечения информационной безопасности органов власти и организаций региона (РИАС ОИБ).

В рамках создания РИАС ОИБ важное значение имеет поддержание в актуальном состоянии общего распределенного информационного ресурса, к которому предъявляются высокие требования по обеспечению его достоверности и безопасности при условии предоставления прозрачного доступа к информации пользователей распределенной информационно-аналитической системы обеспечения информационной безопасности, и использования указанной информации в интересах поддержки принятия решений должностными лицами органов власти и организаций, входящих в состав системы управления субъекта Российской Федерации.

Анализ современных информационных технологий и опыта создания подобных систем [2, 3] показал, что решение задачи построения единой распределенной информационной среды должно осуществляться на основе концепции распределенных баз данных (РБД). Использование данной концепции в интересах создания РИАС обеспечения ИБ определяет необходимость обоснования рационального варианта построения (логической структуры) распределенной базы данных в рамках РИАС ОИБ.

Проведенный анализ известного методического обеспечения обоснования вариантов построения распределенных баз данных различного назначения [4, 5] показал, что имеющийся математический аппарат обоснования требований к распределенной базе данных не в полной мере удовлетворяет особенностям рассматриваемой задачи.

1. Известные подходы (модели, методики и алгоритмы) к решению задач обоснования и построения рациональных структур распределенных баз данных в основном ориентированы на использование временных показателей оценки эффективности их функционирования. Имеются отдельные попытки рассмотрения в качестве не основных показателей таких, как достоверность и безопасность хранения и обработки информации в распределенной базе данных, но без учета их взаимосвязи и взаимозависимости, что неприемлемо в нашем случае. При этом именно в процессе информационного обеспечения деятельности подразделений по защите информации вопросы достоверности информации, используемой при поддержке принятия решений, вопросы ее безопасности при хранении и обработке должны играть определяющую роль.

2. Отсутствуют методы решения задач при совместном рассмотрении (с учетом взаимного влияния) временных характеристик распределенной базы данных, характеристик достоверности и безопасности хранения и обработки информации в распределенной базе данных, которые требуют формулирования задачи обоснования рационального варианта построения распределенной базы данных РИАС ОИБ обеспечения информационной безопасности в многокритериальной постановке.

3. Известный математический аппарат обоснования требований к логической структуре распределенной базы данных не рассматривает особенности проектирования распределенной базы данных РИАС обеспечения информационной безопасности на ранних стадиях при неполноте исходной информации, необходимой для задания большого количества системных, сетевых и структурных ограничений. Упомянутый аппарат применим фактически только в случае, когда имеется достаточно полная информация о составе и структуре информационно-телекоммуникационной сети (ИТКС) РИАС обеспечения информационной безопасности (сеть развернута и функционирует), о характеристиках используемых технических и программных средств. Вместе с тем, учитывая динамику увеличения угроз информационной безопасности, способов и средств обеспечения информационной безопасности, развития информационных технологий, трудно предположить возможность получения и в дальнейшем всей не-

обходимой исходной информации, что обусловливает необходимость создания аппарата, позволяющего решать задачи проектирования распределенной базы данных РИАС ОИБ в условиях неполноты исходной информации.

В связи с вышеизложенным, приобретают актуальность исследования, направленные на разработку методического аппарата обоснования эффективных решений по выбору рационального варианта построения распределенной базы данных РИАС обеспечения информационной безопасности и формированию требований к основным характеристикам ее информационной и логической структур в условиях неполноты исходных данных о предметной области и необходимости рассмотрения множества показателей (временных, достоверности и защищенности информации), определяющих качество вариантов распределенной базы данных РИАС ОИБ обеспечения информационной безопасности органов управления субъекта Российской Федерации.

В общем случае задача синтеза облика распределенной базы данных РИАС обеспечения информационной безопасности может быть сформулирована следующим образом.

Пусть информация, добываемая органами обеспечения информационной безопасности субъекта Российской Федерации различного уровня, распределена по элементам РИАС ОИБ обеспечения информационной безопасности, которые соединены с использованием каналов информационно-телекоммуникационной сети РИАС ОИБ обеспечения информационной безопасности в единое информационное пространство, основу которого составляет ее распределенная база данных.

Считаем заданной в соответствии с местоположением органов обеспечения информационной безопасности субъекта Российской Федерации топологию информационно-телекоммуникационной сети РИАС ОИБ, связывающей их в единое информационное пространство, состоящей из множества L узлов.

Элементы базы данных РИАС ОИБ (разделы распределенной базы данных и репозитория РБД) распределены по узлам информационно-телекоммуникационной сети РИАС ОИБ обеспечения информационной безопасности и содержат в совокупности K объектов данных (ОД), необходимых для реализации запросов пользователей (руководителей ИОГВ, структурных подразделений и/или должностных лиц органов обеспечения информационной безопасности субъекта Российской Федерации) в интересах удовлетворения их информационных потребностей при решении ими своих функциональных задач.

Пусть имеется W пользователей, «прикрепленных» к узлам РИАС обеспечения информационной безопасности субъекта Российской Федерации и удовлетворяющих свои информационные потребности посредством реализации с помощью распределенной базы данных РИАС множества N запросов. Реализация каждого n-го запроса пользователя включает в себя выполнение множества I_n ($n = 1, 2, \ldots, N$) операций манипулирования объектами данных (подзапросов).

Пусть имеется множество из m вариантов построения распределенной базы данных РИАС

$$X = \{X1, X2, \ldots, Xm\}, \quad (1)$$

каждый из которых определяется некоторым планом распределения объектов данных (информационных элементов) по узлам РИАС, который задается матрицей

$$X = |x_{inj}|, \quad (2)$$

где

$$x_{inj} = \begin{cases} 1, \text{ если } i\text{-й объект данных для реализации } n\text{-го запроса размещается на сервере } j\text{-го узла ИТКС ИАС ОИБ,} \\ 0, \text{ в противном случае} \end{cases}, \quad (3)$$

$n = 1, 2, \ldots, N$; $i = 1, 2, \ldots, I_n$; $j = 1, 2, \ldots, J_L$,

где n, i, j – номера запросов, объектов данных и узлов ИТКС ИАС ОИБ соответственно;

N – общее количество запросов;

L – общее количество узлов РИАС.

Как было показано выше, синтез структуры распределенной базы данных РИАС производится в нечеткой многокритериальной среде. Это обусловлено следующими особенностями проектирования указанной распределенной базы данных:

- существенной неполнотой исходной информации, необходимой для задания большого количества системных, сетевых и структурных ограничений на ранних стадиях проектирования распределенной базы данных РИАС ОИБ при использовании известных методов решения рассматриваемой задачи оптимизации;
- необходимостью совместного рассмотрения временных показателей эффективности и показателей эффективности, характеризующих достоверность и безопасность хранения и обработки информации в распределенной базе данных РИАС ОИБ.

С учетом указанных особенностей сформулирован нечеткий векторный критерий выбора варианта построения распределенной базы данных РИАС ОИБ – максимальная степень реализации информационных потребностей пользователей, – который представляет собой оценку варианта построения распределенной базы данных по совокупности частных критериев, характеризующих степень соответствия варианта требованиям реализации информационных потребностей пользователей в процессе обработки их запросов к распределенной базе данных, определяемым минимальным значением времени обработки множества запросов и максимальными значениями показателей, характеризующих достоверность и безопасность хранения информации в распределенной базе данных.

С учетом вышеизложенного, в качестве показателя оценки эффективности варианта построения распределенной базы данных РИАС ОИБ (X) целесообразно использовать нечеткий векторный показатель $П(X)$, характеризующий степень реализации информационных потребностей пользователей с учетом таких характеристик распределенной базы данных, как время обработки множества запросов пользователей, достовер-

ность и безопасность хранения и обработки информации в распределенной базе данных (соответственно, П1(X), П2(X), П3(X)). Тогда можно записать:

$$П(X) = \{П1(X), П2(X), П3(X)\}, \quad (4)$$

где П1(X), П2(X), П3(X) – нечеткие частные показатели эффективности распределенной базы данных РИАС ОИБ, характеризующие степень реализации информационных потребностей пользователей распределенной базы данных в зависимости от значений таких характеристик, как время обработки множества запросов пользователей распределенной базы данных, достоверность и безопасность хранения и обработки информации в распределенной базе данных соответственно.

Тогда нечеткий векторный критерий, использующий выбранный показатель (4), может быть представлен соотношением:

$$C(X) = \{C1(X), C2(X), C3(X)\}, \quad (5)$$

где C1(X), C2(X), C3(X) – частные критерии, максимизирующие соответствующие нечеткие частные показатели П1(X), П2(X), П3(X).

С учетом этого получаем следующее выражение для C(X):

$$C(X) = \{\max П1(X), \max П2(X), \max П3(X)\}. \quad (6)$$

Для каждого компонента C_r (r = = 1, 2, 3) векторного критерия C(X) может быть рассмотрено нечеткое множество

$$C_r = \{\mu_l C_r(X_1)/X_1, m_2 C_r(X_2)/X_2, \ldots, \mu_l Cr(X_m)/X_m\}, \quad (7)$$

где $\mu_l Cr(X_m)/X_m$ – оценка варианта X_i построения распределенной базы данных РИАС ОИБ по критерию Cr, которая характеризует степень соответствия варианта X_i требованию реализации информационных потребностей одного пользователя (класса пользователей) в процессе обработки инициируемых данных пользователем (классом пользователей) множества запросов к распределенной базе данных РИАС, определяемому критерием C_r, $\mu_l Cr(X_i) \in [0, 1]$;

l – номер пользователя (класса пользователей) распределенной базы данных РИАС ОИБ, $l = 1 \ldots L$;

L – общее количество пользователей (классов пользователей) распределенной базы данных РИАС ОИБ.

Тогда правило для выбора рационального варианта построения записывается в виде пересечения D множеств C_1, C_2, C_3:

$$D = C_1 \cap C_2 \cap C_3 \quad (8)$$

Операции пересечения нечетких множеств соответствует операция min, выполняемая над их функциями принадлежности:

$$\mu_D(X_j) = \min_{i=\overline{1,r}} \mu_{C_i}(X_j), \; j = \overline{1, m}. \quad (9)$$

С использованием записи для операций над нечеткими множествами выражение (9) будет иметь следующий вид:

$$\mu_D(X_j) = \mu_{C_1}(X_j) \wedge \mu_{C_2}(X_j) \wedge \mu_{C_3}(X_j), \; j = \overline{1, m}. \quad (10)$$

Тогда в качестве рационального выбирается вариант построения распределенной базы данных РИАС ОИБ X^*, имеющий наибольшее значение функции принадлежности μ_D:

$$\mu_D(X^*) = \max_{i=\overline{1,r}} \mu_D(X_j). \quad (11)$$

Таким образом, фактически осуществляется переход от многокритериальной задачи оптимизации по нечетким критериям (6) к однокритериальной оптимизационной задаче в нечеткой постановке (11) при нечетких ограничениях, в качестве которых рассматриваются нечеткие частные критерии (5).

С учетом вышеизложенного, исследования по выбору рационального варианта построения распределенной базы данных РИАС ОИБ состоят в решении следующей научной задачи.

На исходном множестве $X(X = \{X_j\}, j = 1, 2, \ldots, m)$ допустимых m вариантов построения распределенной базы данных РИАС ОИБ найти такой вариант ее построения (подмножество X^*), для которого показатель степени реализации информационных потребностей пользователей $\mu_D(X^*)$ достигает максимума, то есть найти

$$X^* = \arg \max_{X_j \in X \; 1 \leqslant j \leqslant m} \{\mu_D(X_j)\}. \quad (12)$$

Для решения сформулированной задачи необходимо осуществить генерацию допустимых вариантов построения (логической структуры) распределенной базы данных РИАС ОИБ (в соответствии с [6]) с последующей их количественной оценкой и выбором рационального варианта логической структуры в соответствии с критерием (12) [7].

Предложенная постановка задачи позволяет перейти к формированию технологии обоснования рационального варианта построения распределенной базы данных РИАС ОИБ с учетом реализации представленных математических зависимостей. ■

ЛИТЕРАТУРА

1. *Лаврухин Ю. Н., Обухов А. Я., Швед В. Г. Проблемы обеспечения информационной безопасности в органах управления субъектов Российской Федерации. – Воронеж: Защита информации в радиотехнических системах. – 2003.*
2. *Сиколенко В. В. Поддержка распределенных систем в СУБД Oracle [Электронный ресурс]. – Режим доступа: http://www.osp.ru/dbms/1996/04/13031499/.*
3. *Руководство по технологиям объединенных сетей (Internetworking Technologies Handbook). Серия: Cisco Press Core Series. – Изд-во «Вильямс». – 2005.*
4. *Кузьмина Л. В. Методы решения задач распределения информационных потоков в сетях передачи данных предприятия на основе резервирования ресурсов / В. Т. Еременко, С. И. Афонин, В. Т. Еременко и др. // Информационные системы и технологии. – 2012. – № 1. – С. 78–84.*
5. *Афонин С. И., Еременко В. Т. Создание теоретических основ автоматизации и построения технологической составляющей АСУ территориально распределенных предприятий // Информационные системы и технологии. – 2012. – № 2. – С. 99–105.*
6. *Кузнецов Н. А., Кульба В. В., Ковалевский С. С., Косяченко С. А. Методы анализа и синтеза модульных информационно-управляющих систем. – М.: Физматлит. – 2002.*
7. *Герасименко В. Г. Выбор рационального варианта построения специализированной распределенной базы данных в нечеткой многокритериальной среде / А. А. Бурушкин, В. Г. Герасименко, С. А. Головин, С. В. Жилинский // Телекоммуникации. – 2005. – № 2. – С. 2–4.*
8. *Будько М. Б., Будько М. Ю. Отслеживание изменений в структуре сети и решение задач повышения безопасности на основе анализа потоков данных // Научно-технический вестник информационных технологий, механики и оптики. – 2009. – № 1 (59). – С. 78–82.*