УДК 004.056: 002.338.2

Т.И. Булдакова, А.Ш. Джалолов

ЗАДАЧИ ИНТЕГРАЦИИ, ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ В СИТУАЦИОННЫХ ЦЕНТРАХ

Рассмотрены особенности принятия управленческих решений в ситуационных центрах, их информационное и программное обеспечение, вопросы защиты данных.

E-mail: buldakova@bmstu.ru

Ключевые слова: *ситуационные центры, обработка информации, принятие решений, информационная безопасность.*

Все более широкое применение в совершенствовании управленческой деятельности находят ситуационные центры (СЦ). Ситуационный центр – центр поддержки принятия решений и обеспечения этих решений. Качество работы СЦ в большой степени зависит от того, насколько эффективно он работает как система обработки информации. Если лица, принимающие решения (ЛПР), не будут своевременно обеспечены полной, точной, актуальной и неизбыточной информацией, то это непременно отразится на качестве принимаемых решений. Поэтому основное назначение СЦ – обеспечение непосредственного доступа к территориально распределенной информации, необходимой для поддержки принятия решений на основе сценарного анализа ситуации в политике; экономике; социальной сфере; сельском хозяйстве; реализации национальных проектов; чрезвычайных ситуациях и т. д. [1].

Ситуационный центр – система обработки информации. По функциональному назначению СЦ можно подразделить на три типа: для управления технологическими процессами, для административного управления, для научных исследований. Однако независимо от типа, в СЦ обеспечивается информационно-аналитичекая поддержка выполнения множества функций, процедур, процессов, позволяющих оперативно анализировать, моделировать, прогнозировать и динамично вырабатывать эффективные решения. Важными задачами СЦ являются:

- сбор информации по заданным критериям из различных источников, обработка и хранение данных;
- обеспечение информационной поддержки ЛПР, интеграция различных информационно-аналитических систем и ресурсов;
- мониторинг ключевых индикаторов обстановки, имитационное моделирование и прогнозирование процессов ее развития;
- предоставление ЛПР обобщенной и детализированной информации;

• поддержка интеллектуальных методов коллективного поиска вариантов решений по выявленным ситуациям;

• планирование, координация и контроль реализации принятых решений, оценка результатов выполнения решений;

• обеспечение взаимодействия с территориально-распределенными объектами управления.

Современные СЦ, оснащенные системой информационной и технической поддержки принятия решений, позволяют руководителям государственных и коммерческих структур успешно решать задачи контроля и управления, как в штатных, так и в кризисных ситуациях.

Основной особенностью СЦ как системы обработки информации является разнородность анализируемой информации, а также средств и методов ее обработки. Это связано с тем, что ситуационный анализ подразумевает использование информации из разнородных источников, чтобы ЛПР могло, всесторонне изучив проблему, принять наиболее взвешенное и качественное решение.

Функциональная архитектура СЦ определяется информационными процессами, связанными с принятием решения. К основным процессам относятся: сбор информации; консолидация информации; выявление ситуации; поиск решения; постановка задачи; контроль выполнения. Эти информационные процессы определяют типовую структуру СЦ (рис. 1).

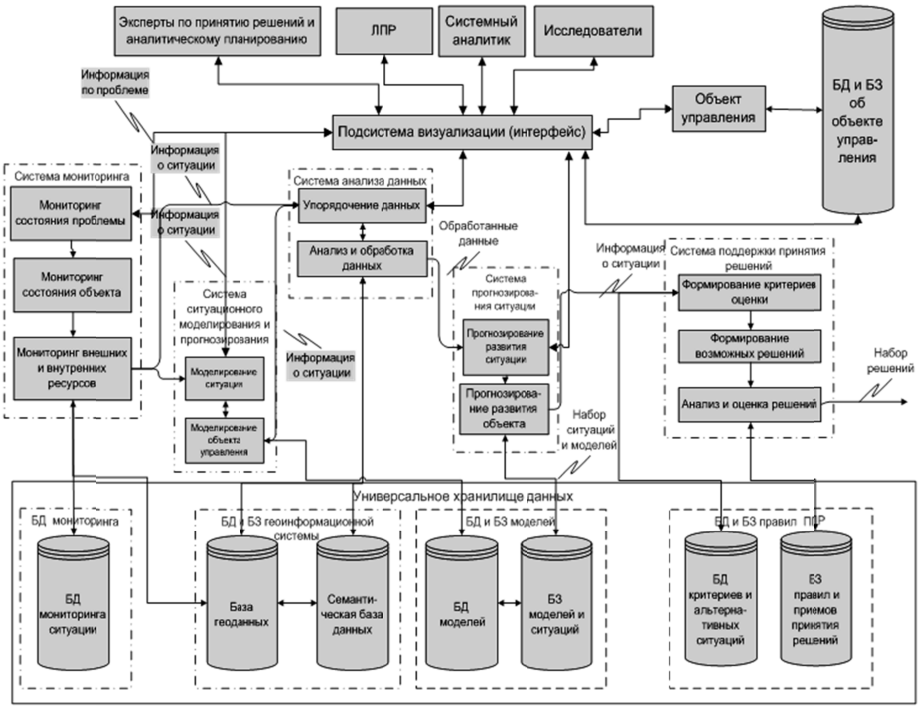

Рис. 1. Типовая структура ситуационного центра:

БЗ – база знаний; БД – база данных

Представленная структура является интегрирующей, способной объединять все возможные источники информации для принятия управленческого решения [2]. Для реализации указанных выше информационных процессов используются система мониторинга, система анализа данных, система прогнозирования ситуации, система поддержки принятия решений.

В работе СЦ можно выделить три основных режима, которые отличаются интенсивностью поступления и обработки данных и сценариями работы с информацией:

- проблемный мониторинг: получение, обработка и наглядное отображение актуальной информации от различных источников, как в фоновом режиме, так и по запросам. Этот режим позволяет постоянно следить за ситуацией по выбранным критериям и выявлять возникновение чрезвычайной ситуации;
- плановое обсуждение ситуаций: запланированное коллективное обсуждение аналитических докладов о положении дел на управляемых объектах или территориях. Кроме того, возможности СЦ должны позволять обращаться за информацией в удаленные или локальные базы данных, получать сведения из внешних источников по каналам связи;
- чрезвычайный режим: оперативное принятие решений и контроль их исполнения по непредвиденным, кризисным, чрезвычайным проблемам с возможным подключением «внешних» экспертов. Элементы чрезвычайного режима могут возникнуть и во время планового обсуждения проблемы, и при анализе данных мониторинга.

Детализированная структура системы анализа данных и ее взаимодействие с информационными компонентами (рис. 2) показывает, что для принятия решений по разнообразным ситуациям требуются различные технологии анализа информации.

В общем случае СЦ предназначен для решения слабоструктурированных проблем, которые характеризуются следующими признаками «ситуационности»: неформализуемостью, неопределенностью, нестереотипностью ситуации, взаимовлиянием множества факторов, конфликтностью, большими объемами неявной информации, хаотичностью изменения ситуации и др. [3]. Это обусловливает необходимость применения интеллектуальных технологий анализа данных, которые эффективно используются для автоматического нахождения скрытых взаимосвязей и нелинейных зависимостей в данных, что позволяет лучше осмысливать предметную область, повышать качество решений, принимаемых на основе анализа ее состояния. Поэтому структура информационно-аналитических систем СЦ должна быть максимально гибкой, чтобы реализовывать любые процедуры обработки и представления данных, которые могут потребоваться в процессе анализа ситуации.

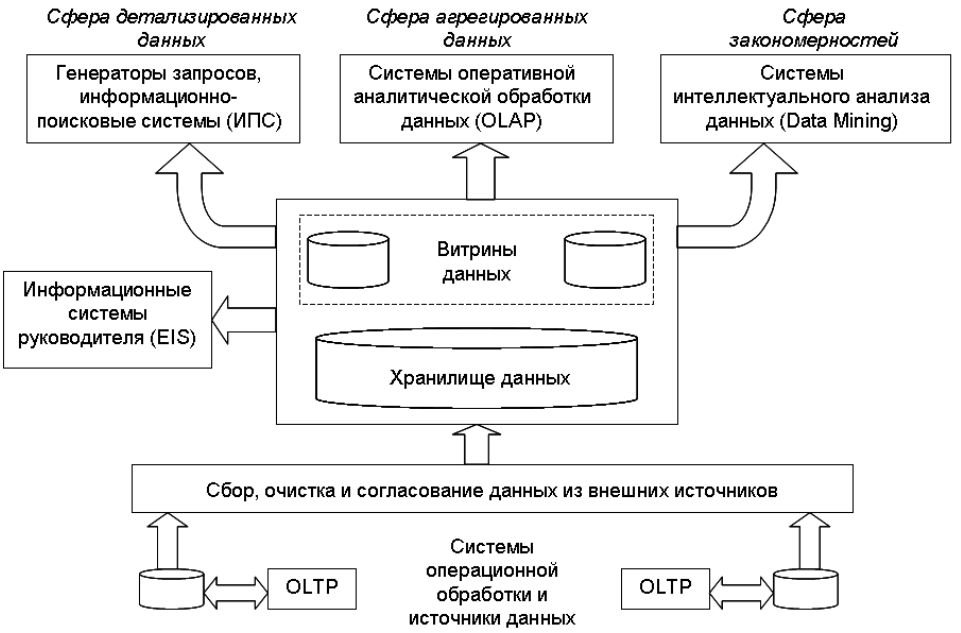

Рис. 2. Детализация системы анализа данных и извлечения знаний

Технологии оперативного (OLAP) и интеллектуального анализа данных (Data mining), в отличие от операционной обработки данных (OLTP) [4], позволят более эффективно выполнять оценку состояния наблюдаемых процессов, выявлять и ранжировать причины значимых изменений, прогнозировать развитие процессов и вырабатывать рекомендации в части подготовки возможных вариантов решений с прогнозом их последствий. Перспективным направлением следует считать применение нейро-нечетких технологий для поддержки принятия управленческих решений.

Информационно-аналитические системы руководителей (EIS) необходимы для непосредственного использования ЛПР. Эти системы дают общую наглядную картину текущей ситуации и представляют тенденции ее развития с возможностью углубления рассматриваемой информации с помощью других аналитических модулей.

Организация информационных хранилищ. Хранилище информации содержит данные, поступающие из многих источников, которые интегрируются, собираются и структурируются таким образом, чтобы их можно было использовать при анализе и в процессе принятия управленческих решений. Данные могут порождаться большим количеством внутренних систем и внешними источниками, включая транзакции, выполняемые через Web-сайты, причем в каждом из таких источников могут использоваться свои модели данных.

Конечной целью создания информационного хранилища является интеграция корпоративных данных в едином репозитории, обращаясь к которому пользователи смогут составлять запросы, генерировать отчеты и выполнять анализ данных. Хранилище данных – рабочая среда для систем поддержки принятия решений, которая извлекает данные, хранимые в различных оперативных источниках, организует их и передает лицам, ответственным за принятие решений в данной организации.

Основное внимание в технологии хранилищ данных уделяется управлению пятью информационными потоками: входным, восходящим, нисходящим, выходным и метапотоком, в каждом из этих потоков выполняются определенные процессы:

1) входной поток охватывает процессы извлечения, очистки и загрузки исходных данных в хранилище;

2) восходящий поток охватывает процессы повышения ценности сохраняемых в хранилище данных путем обобщения, упаковки и распределения исходных данных;

3) нисходящий поток обслуживает процессы архивирования и резервного копирования (восстановления) информации в хранилище;

4) выходной поток охватывает процессы предоставления данных пользователям;

5) метапоток охватывает процессы, связанные с управлением метаданными.

Вслед за появлением и быстрым развитием хранилища данных появилась и близкая ему концепция витрин данных. Витрина данных состоит из некоторого подмножества хранилища данных, которое обычно представлено в виде обобщенной информации, связанной с поддержкой требований отдельных групп пользователей.

Для витрины данных можно выбрать двухуровневую или трехуровневую архитектуру [5]. В трехуровневой структуре первый уровень образует хранилище данных, поставляющее информацию для витрины данных; второй уровень – витрина данных, а третий – рабочая станция пользователя (рис. 3).

В изображенной на рис. 3 архитектуре данные распределены между всеми тремя уровнями. При этом витрина данных предоставляет пользователям доступ к данным, которые приходится анализировать чаще других.

Обеспечение безопасности информации. Организационные мероприятия, направленные на защиту данных, хорошо изучены и широко известны [6, 7]. К этим мероприятиям можно отнести: организацию работы персонала и пользователей в системе; организацию работы и учет носителей информации; планирование мероприятий по защите информации; организацию аналитической работы и контроля и т. д.

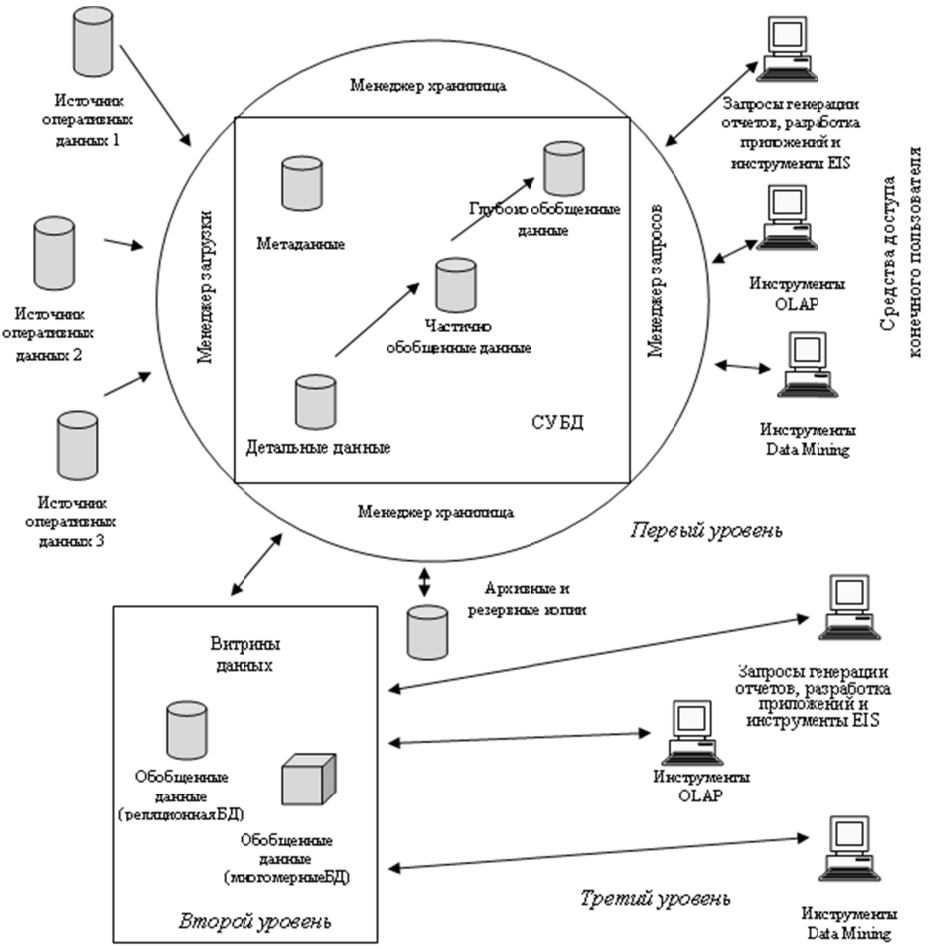

Рис. 3. Трехуровневая архитектура информационного хранилища и витрины данных

Наиболее интересным представляется обеспечение информационной безопасности (ИБ) с помощью программных и программно-аппаратных средств защиты информации. Система защиты данных, обрабатываемых, хранимых и циркулирующих в технических средствах СЦ, с учетом сопряжения программно-технических средств СЦ с внешними системами, включенными в общее информационное пространство, должна быть реализована на основе комплекса средств защиты информации [6]:

- программно-технических средств защиты информации от несанкционированного доступа (НСД);
- программно-технических средств криптографической защиты;
- технических средств защиты оборудования СЦ от утечки информации по побочным каналам;
- технологий специальной проверки импортного оборудования;
- защиты от воздействия окружающей среды.

Комплексный подход к обеспечению ИБ основан на интеграции различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных. Однако использование такого подхода в настоящий момент является недостаточным. Поэтому в структуре СЦ необходимо предусмотреть систему ИБ. В этом случае, с одной стороны, обеспечение ИБ будет связано с встраиванием механизмов защиты в программные и технические компоненты информационных систем. С другой стороны, внешнюю защитную оболочку будет создавать комплексная система информационной безопасности (включая системы мониторинга и управления ИБ, интегрированные с системами мониторинга и управления СЦ).

Разработка системы ИБ СЦ должна проводиться с учетом защиты от выявленных угроз и возможных информационных рисков, для которых определяются способы защиты. При этом учитываются требования, которые предъявляются к созданию таких систем [7]:

- организация защиты информации должна осуществляться с учетом системного подхода, обеспечивающего оптимальное сочетание взаимосвязанных методологических, организационных, программных, аппаратных и иных средств;
- система должна развиваться непрерывно, так как способы реализации угроз информации непрерывно совершенствуются. Управление ИБ – непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования систем ИБ, непрерывном контроле, выявлении ее «узких» и слабых мест, потенциальных каналов утечки информации и новых способов НСД;
- система должна предусматривать разделение и минимизацию полномочий по доступу к обрабатываемой информации и процедурам обработки;
- система должна обеспечивать контроль и регистрацию попыток НСД, содержать средства для точного установления идентичности каждого пользователя и протоколировать действия;
- система должна обеспечивать надежность защиты информации и контроль за функционированием системы защиты, т. е. использовать средства и методы контроля работоспособности механизмов защиты.

Реализация перечисленных требований при создании системы защиты информации в СЦ будет способствовать повышению качества принимаемых управленческих решений, так как ЛПР своевременно будет обеспечено точной и достоверной информацией.

СПИСОК ЛИТЕРАТУРЫ

1. Информационно-аналитические средства поддержки принятия решений и ситуационные центры / Под общ. ред. А.Н. Данчула. – М.: Изд-во РАГС, 2006. – 326 с.
2. Симанков В.С., Колесников Д.А. Режимы работы ситуационного центра регионального уровня // Программные продукты и системы. – 2010. – № 1. – С. 52.
3. Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. – М.: Издательский дом «Парад», 2005. – 392 с.
4. Барсегян А.А., Куприянов М.С., Степаненко В.В. Методы и модели анализа данных: OLAP и Data Mining. – СПб.: БХВ-Петербург, 2004. – 336 с.
5. Конноли Т., Бегг К., Страчан А. Базы данных: проектирование, реализация, сопровождение. Теория и практика. – М.: Издательский дом «Вильямс», 2000. – 1120 с.
6. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.
7. Аскеров Т.М. Защита информации и информационная безопасность / Под общ. ред. К.И. Курobатова. – М.: Российская экономическая академия, 2001. – 386 с.

Статья поступила в редакцию 14.05.2012