А. А. Зацаринный, В. И. Королёв, Особенности подготовки информационно-аналитического продукта средствами сегментированного ситуационного центра, *Системы и средства информ.*, 2017, том 27, выпуск 4, 122–131

DOI: https://doi.org/10.14357/08696527170409

ОСОБЕННОСТИ ПОДГОТОВКИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ПРОДУКТА СРЕДСТВАМИ СЕГМЕНТИРОВАННОГО СИТУАЦИОННОГО ЦЕНТРА

***А. А. Зацаринный*[1], *В. И. Королёв*[2]**

Аннотация: Ситуационный центр (СЦ) представлен как объект в защищенном исполнении, информационная безопасность которого обеспечивается сегментированием ресурсов по признаку выделения контуров безопасности информационно-технологической (ИТ) инфраструктуры. Рассмотрены вопросы интегрирования и консолидации информационных ресурсов (ИР) СЦ для создания информационно-аналитического продукта (ИАП). Дано представление ИТ-ландшафта СЦ в защищенном исполнении. Предложен алгоритм информационного обеспечения при создании ИАП ситуационного управления в ИТ-инфраструктуре с выделенными контурами безопасности.

Ключевые слова: ситуационный центр; информационная безопасность; информационные ресурсы; информационно-технологическая инфраструктура; информационно-аналитический продукт

DOI: 10.14357/08696527170409

1 Особенности ситуационного центра как системы в защищенном исполнении

Ситуационный центр как самостоятельный *объект информационной индустрии* — сложная автоматизированная система (АС), которая является частью системы управления объектом (организация/предприятие как объект управления — далее организационная система) и представляет собой, по существу, подсистему информационно-аналитической и технологической поддержки принятия решений в составе организационной системы. Ситуационный центр концентрирует информацию об объекте управления из различных источников *информационно-технологического пространства* объекта, обеспечивает ситуационное управление объектом и принятие управленческих решений с широким использованием *информационных технологий*, моделей и методов ситуационного анализа [1, 2].

[1]Институт проблем информатики Федерального исследовательского центра «Информатика и управление» Российской академии наук, AZatsarinny@ipiran.ru

[2]Институт проблем информатики Федерального исследовательского центра «Информатика и управление» Российской академии наук; Научно-исследовательский ядерный университет МИФИ; Финансовый университет при Правительстве РФ, vkorolev@ipiran.ru

Базовой реализационной функцией СЦ является формирование и ведение ИР. Контент ИР СЦ, как правило, является разнородным: тексты, изображения (графика), аудио- и видеофайлы, цифровые данные и т. д. При этом одним из главных характеристических факторов является необходимость отнесения этих видов разнородной информации к различной категории доступа (информация ограниченного доступа [3]) и, как следствие, обеспечение соответствующих «публичных, гражданских и иных правовых отношений».

Одним из доверенных механизмов защиты ИР СЦ с большими объемами разнородной поступающей информации является *сегментирование защищаемых ресурсов* (информационных, телекоммуникационной и программно-технической среды) по признаку выделения контуров безопасности ИТ-инфраструктуры в соответствии с категорией обрабатываемой информации. Этот вариант архитектурного построения ИТ-инфраструктуры СЦ достаточно подробно рассмотрен авторами в работе [3].

Архитектура построения ИТ-инфраструктуры СЦ в защищенном исполнении с выделением контуров безопасности имеет как преимущества, так и недостатки. В данной работе авторы рассматривают *технологические аспекты* функциональной реализации задач СЦ с такой организацией ИР.

Общий подход к архитектуре сегментирования защищаемых ресурсов СЦ может быть охарактеризован следующими основными положениями [3].

Создаются ИТ контуры безопасности: секретный «С», конфиденциальный «К» и открытый (публичный) «О». Это обеспечивает баланс требований открытости информации и ее защиты.

Каждый контур безопасности является локальной системой на базе локальной вычислительной сети (ЛВС), в которой вся информация накапливается в своем банке данных (БД) и обрабатывается в соответствии с требованиями наивысшей категории.

Интеграция информации, получение консолидированного ИАП из ИР всех сегментов обеспечиваются однонаправленными каналами информационных потоков через шлюзы по вектору: контур «О» → контур «К» → контур «С».

Для всего сообщества пользователей СЦ выделение контуров безопасности автоматически обеспечивает реализацию мандатной модели разграничения доступа к ресурсам. Внутри контуров возможно дифференцирование разграничения доступа по дискреционной модели. На СЦ выделяется привилегированная группа пользователей — аналитики, имеющие определенные права работать во всех сегментах, основная функция которых — подготовка ИАП по конкретной ситуации. Права и механизмы их доступа могут быть определены по ролевой модели разграничения доступа. Такой подход позволяет построить достаточно гибкую политику разграничения доступа на СЦ.

Вместе с тем при этом возникает непростая проблема функционально-целевой интеграции информации из всей совокупности ИР и ее консолидированного представления в соответствии с определенным сценарием при рассмотрении конкретной ситуации в бизнес-процессах управления объектом. Для разрешения

этой проблемы необходимы информационные технологии, ориентированные на подготовку ИАП по возникающим ситуациям с использованием данных из БД различных контуров СЦ, получением информации из систем и от объектов, с которыми обеспечивается информационное взаимодействие в определенных регламентах.

Под *информационно-аналитическим продуктом* будем понимать результат аналитической работы по рассмотрению ситуации, выполненной с учетом онтологии ситуации, в соответствии с целевыми установками и имеющимися аналитическими моделями и методиками на основе совокупной информации, накопленной в БД СЦ, предоставляемой СЦ в рамках определенного регламента или запрашиваемой конкретно под ситуацию. Информационно-аналитический продукт является исходной информационной платформой для формирования сценария и технологии представления данных в ходе процесса принятия решений лицами, принимающими решения (ЛПР).

Информационно-аналитический продукт является результатом процессов, определяющих сущность аналитики. К числу наиболее значимых процессов аналитической работы можно отнести следующие процессы [4, 5]:

- анализ целей управления и формулирование задачи информационно-аналитической работы;
- управление сбором информации в интересах решения управленческих задач в условиях меняющейся ситуации;
- анализ и оценивание полученной информации в контексте целей управления, выявления сущности наблюдаемых процессов и явлений;
- синтез нового знания (решение функциональных задач СЦ, интерпретация результатов, прогнозирование и т. п.), необходимого для решения задач управления;
- доведение результатов аналитической работы (нового знания) до субъекта управления (структуры или лица, принимающего решение).

2 Особенности обработки информационных ресурсов в ситуационном центре в защищенном исполнении

Работа с ИР в СЦ имеет свою специфику, которая прежде всего обусловлена целевым назначением СЦ как объектом информационной индустрии, осуществляющим информационно-аналитическую поддержку управления.

Объектом управления может быть любой объект, связанный с определенным видом деятельности. *Информационно-технологическое пространство* объекта управления — совокупность ИР, информационных технологий и средств их реализации, образующих и обеспечивающих поддержку должной функциональности и живучести объекта.

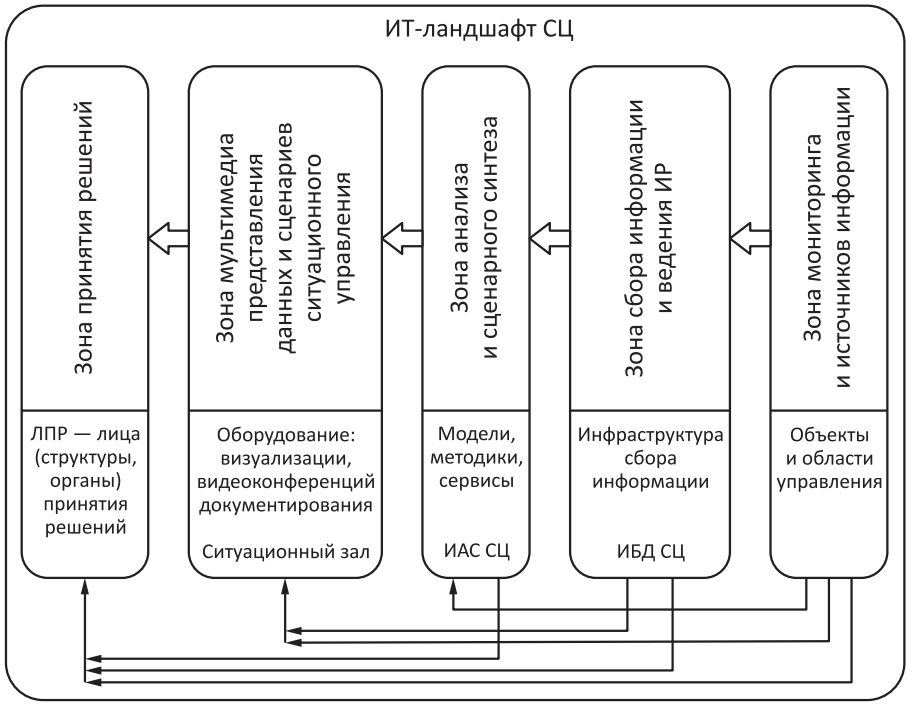

Рис. 1 Схема ИТ-ландшафта СЦ (ИАС — информационно-аналитическая система; ИБД — интегрированный БД)

Характер и технологии работы с ИР обусловливаются ИТ-ландшафтом. В общем случае ИТ-ландшафт объекта информатизации обеспечивает представление ИТ-сервисов для бизнес-процессов в сочетании с развертыванием инженерной, сетевой, вычислительной инфраструктур, систем резервного копирования и восстановления, управления и администрирования (слои ИТ-ландшафта), «накрывает» всю совокупность АС, являясь фундаментальной основой автоматизации бизнес-процессов и построения связной инфраструктуры [6].

Информационно-технологический ландшафт СЦ связан с зонами решения системных обеспечивающих задач ситуационного управления (рис. 1), с их ИТ-сервисами. На схеме ИТ-ландшафта СЦ выделены системные технологические зоны: мониторинга и источников информации, сбора информации и ведения ИР, анализа и сценарного синтеза, мультимедиа представления данных и сценариев ситуационного управления, принятия решений. Базовые информационные потоки последовательно реализуются между зонами от зоны мониторинга и источников информации (объекты и области управления) до зоны принятия решений (ЛПР — лица, структуры, органы принятия решений). Однако не исключается получение

дополнительной информации оперативного характера непосредственно в каждую из зон.

Информационно-технологические сервисы реализуются технологическими комплексами работы с ИР в зонах СЦ, конфигурация которых определяется характеристиками многих компонентов: источниками стационарной и мониторинговой информации, информационными потоками и регламентами поступления информации, базами данных и их взаимодействием в обрабатывающей и телекоммуникационной среде, функциональными задачами СЦ и аппаратом их решения, политикой информационной безопасности, другими составляющими.

Характеристики компонентов зависят прежде всего от характера самой обрабатываемой информации и от инфраструктурных решений по обработке информации.

Учитывая нормативные положения по информационной безопасности, характеристики компонентов существенно зависят от возможностей, прав и требований по распоряжению информацией. В соответствии с установленным в отечественной практике законодательством [7] распоряжение информацией субъектами, участвующими в информационных процессах, необходимо рассматривать с точки зрения прав «обладателя» информации. Отсюда следуют, по крайней мере, два аспекта отношения к используемым в СЦ ИР: ИР и информационные технологии входят непосредственно *в периметр компетенции* распоряжения объекта информатизации или они находятся *вне этого периметра*, но необходимы для управления объектом и функционирования СЦ. В последнем случае регламент предоставления этой информации и границы распоряжения определяются договорными условиями или полномочными административными решениями соответствующего уровня.

Инфраструктура обрабатывающей среды СЦ, соответствующая принятым архитектурным и техническим решениями ее построения, также влияет, а по существу, определяет технологию работы с ИР и должна отвечать требованиям политики информационной безопасности на СЦ и объекте информатизации в целом. В данном случае — архитектурные решения связаны с сегментированием ресурсов СЦ по контурам безопасности как способом обеспечения информационной безопасности [3].

В соответствии с поставленной задачей обеспечения технологического сервиса подготовки ИАП далее рассмотрим в основном процессы сбора, интеграции и предоставления информации для непосредственно выполнения аналитики и принятия решений в условиях сегментирования ресурсов СЦ по признакам контуров безопасности.

3 Алгоритм технологического процесса информационного обеспечения подготовки информационно-аналитического продукта

Сформулируем основные положения, определяющие с позиций информационной безопасности конфигурацию технологического комплекса работы с ИР

в процессах сбора, интеграции и предоставления информации для выполнения аналитики и принятия решений в условиях сегментирования ресурсов СЦ.

Вся информация поступает в СЦ по отдельным каналам, накапливается и обрабатывается в соответствии с конфиденциальностью (метка конфиденциальности — «О», «К», «С», т. е. в соответствующем контуре безопасности; контур безопасности представляет собой ЛВС.

В контурах безопасности создаются базы данных соответствующего уровня конфиденциальности.

В целях интеграции информации по релевантным признакам рассматриваемой ситуации, консолидации ее для выработки решений обеспечивается подъем информации в направлении повышения конфиденциальности.

Для всех пользователей — поставщиков информации, а также внешних пользователей, если таковые имеются, реализуется только мандатный доступ к информации с выделенных удаленных автоматизированных рабочих мест.

Пользователи-аналитики, обеспечивающие подготовку ИАП, а также определенные группы операторов, обеспечивающих в соответствии со сценариями информационное сопровождение процессов принятия решений ЛПР, наделяются правами доступа ко всем контурам безопасности по ролевой модели доступа в рамках своих функциональных обязанностей.

Схема алгоритма реализации технологического процесса информационного обеспечения для создания ИАП, соответствующего сформулированным положениям, представлена на рис. 2.

Принципиальными задачами интеграции исходной информации и эффективной ее консолидации для подготовки ИАП являются обеспечение полноты и актуальности ИР, извлеченного из ИР СЦ в соответствии с заданными показателями релевантности информации по ситуации. Для этого необходимо, по крайней мере, осуществить поиск такой информации во всех контурах безопасности. Необходимые дополнительные данные будут поступать по запросу или в соответствии с регламентами также через ЛВС и БД контуров. Данная технология отражена на схеме алгоритма.

Принципиально важным с точки зрения функциональности использования ИАП по сценарию и обеспечения при этом безопасности является технологическое решение, в какой степени интеграции представлять конечный ИАП. Возможны два варианта:

(1) ИАП представляется как единый информационно-аналитический объект наивысшего уровня конфиденциальности и размещается в соответствующем контуре безопасности;

(2) фрагменты ИАП определенного уровня конфиденциальности размещаются в соответствующих контурах безопасности.

Данные решения принимаются субъектом аналитики (подразделение СЦ, должностное лицо — П «А») в соответствии со сценарием информационно-аналитической поддержки принятия решения и политики информационной безопас-

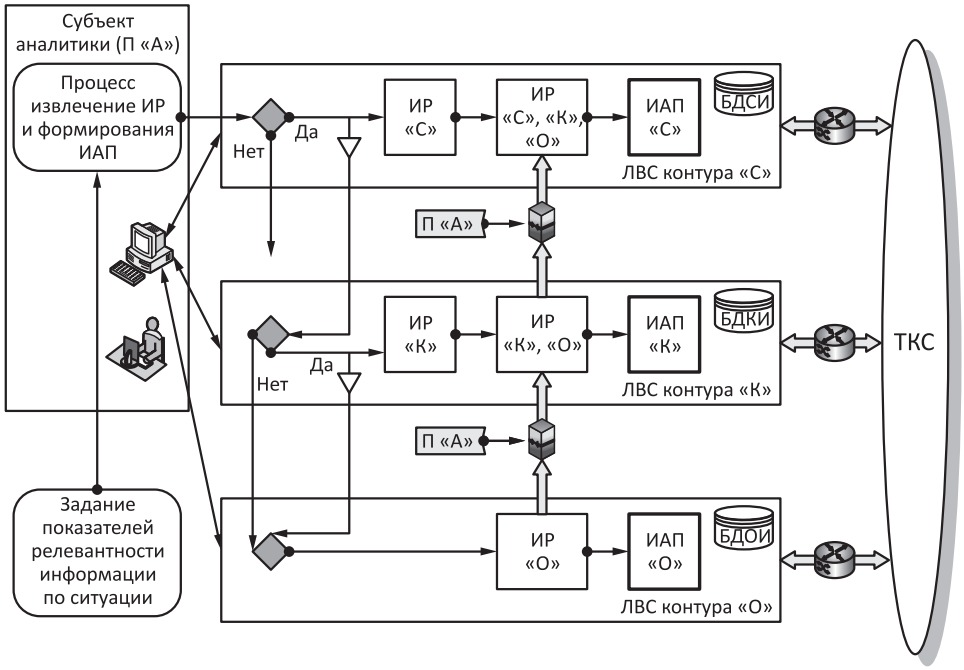

Рис. 2 Схема алгоритма информационного обеспечения при создании ИАП СЦ (ТКС — телекоммуникационная система; БДСИ, БДКИ и БДОИ — БД секретной, конфиденциальной и открытой информации)

ности. Им же дается разрешение на подъем информации по конкретной ситуации для подготовки ИАП из контуров безопасности через однонаправленные шлюзы.

Если ИАП представляется как единый информационно-аналитический объект наивысшего уровня конфиденциальности, то защита его осуществляется по требованиям этого наивысшего уровня конфиденциальности, но в части доступности он может рассматриваться как интегрированный объект разграничения доступа, включающий разделы различного уровня конфиденциальности. Тогда доступ к этим разделам может осуществляться по модели мандатного или ролевого доступа.

4 Заключение

Исследование технологий работы с ИР в современных компьютерных системах подтверждает очевидный вывод о том, что задачи создания информационных систем и обеспечения информационной безопасности становятся неразрывно взаимосвязанными и требуют единого системного подхода в соответствии с поло-

жениями системной инженерии и архитектурным подходом в проектировании [8]. В статье предложены методические подходы и технологические решения по обеспечению подготовки аналитического продукта при функционировании СЦ как наиболее актуального вида информационных систем, функционирование которого обеспечивается в защищенном исполнении путем сегментирования защищаемых ресурсов в рамках контуров безопасности.

Литература

1. *Зацаринный А. А., Шабанов А. П.* Технология информационной поддержки деятельности организационных систем на основе ситуационных центров. — М.: ТОРУС ПРЕСС, 2015. 232 с.
2. *Зацаринный А. А., Королёв В. И.* Информационная безопасность ситуационных центров // Системы и средства информатики, 2016. Т. 26. № 1. С. 121–138.
3. *Зацаринный А. А., Королёв В. И.* Сегментирование информационно-технологической инфраструктуры ситуационного центра по признаку контуров безопасности // Системы и средства информатики, 2016. Т. 26. № 3. С. 136–147.
4. *Демидов А. А., Захаров Ю. Н.* Информационно-аналитические системы поддержки принятия решений в органах государственной власти и местного самоуправления. Основы проектирования и внедрения. — СПб.: НИУ ИТМО, 2012. 100 с.
5. *Сеитов А. П.* Пособие по подготовке аналитических материалов (общепризнанные подходы). — Ташкент, 2013. http://www.proza.ru/2014/02/01/796.
6. *Андреев В.* Ландшафтный дизайн для информационных систем // Технологии и средства связи, 2008. № 3. С. 54–57.
7. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ с изменениями и поправками ФЗ РФ от 13 июля 2015 г. «О внесении изменений в ФЗ «Об информации, информационных технологиях и о защите информации».
8. ГОСТ Р ИСО/МЭК 15288-2005. Системная инженерия. Процессы жизненного цикла систем.

Поступила в редакцию 07.08.17

TECHNOLOGICAL SERVICE PREPARATION OF INFORMATION AND ANALYTICAL PRODUCTS BY MEANS OF A SEGMENTED SITUATIONAL CENTER

***A. A. Zatsarinny*[1] *and V. I. Korolev*[1,2,3]**

[1]Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation
[2]National Research Nuclear University "MEPhI," 31 Kashirskoye Highway, Moscow 115409, Russian Federation
[3]Financial University under the Government of the Russian Federation, 49 Leningrad Prosp., Moscow 125993, Russian Federation

Abstract: The situational center is presented as an object in the protected execution, where the information security is supported by segmentation of the resources on the basis of information-technology (IT) infrastructure security contour. The article considers the matters of integration and consolidation of information resources to create an information-analytical product. It provides general description of the IT-landscape of the situational center. It proposes the algorithm of information support to make the information-analytical product of situational management in IT-infrastructure with dedicated security contour.

Keywords: situational center; information security; information resources; information-technology infrastructure; information and analytical product

DOI: 10.14357/08696527170409

References

1. Zatsarinny, A. A., and A. P. Shabanov. 2015. *Tekhnologiya informatsionnoy podderzhki deyatel'nosti organizatsionnykh sistem na osnove situatsionnykh tsentrov* [A technology of information support of operations of organizational systems based on situation centers]. Moscow: TORUS PRESS. 232 p.
2. Zatsarinny, A. A., and V. I. Korolev. 2016. Informatsionnaja bezopasnost' situatsionnykh tsentrov [Information security of situation centers]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 26(1):121–138.
3. Zatsarinny, A. A., and V. I. Korolev. 2016. Segmentirovanie informatsionno-tekhnologicheskoy infrastruktury situatsionnogo centra po priznaku konturov bezopasnosti [The segmentation of situation center informational and technological infrastructure by safety circle attribute]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 26(3):136–147.
4. Demidov, A. A., and Yu. N. Zakharov. 2012. *Informatsionno-analiticheskie sistemy podderzhki prinyatiya resheniy v organakh gosudarstvennoy vlasti i mestnogo samoupravleniya. Osnovy proektirovaniya i vnedreniya* [Information and analytic systems of

decision making support in government and local authorities. Groundwork of design and implementation]. St. Petersburg: NIU ITMO. 100 p.

5. Seitov, A. P. 2013. Posobie po podgotovke analiticheskikh materialov (obshchepriznannye podkhody) [A tutorial for analytic material preparation (universal approaches)]. Tashkent. Available at: http://www.proza.ru/2014/02/01/796 (accessed August 15, 2017).
6. Andreev, V. 2008. Landshaftnyy dizayn dlya informatsionnykh sistem [Landscape design for information systems]. *Tekhnologii i sredstva svyazi* [Technologies and Means of Telecommunication] 3:54–57.
7. Federal'nyy zakon 149-FZ [Federal Law No. 149-FZ]. July 27, 2006. "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" s izmeneniyami i popravkami FZ RF ot 13 iyulya 2015 g. "O vnesenii izmeneniy v FZ "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" [On amending the Federal Law "About information, information technologies, and information protection," including amendments and corrections of July 13, 2015].
8. State Standard of Russia GOST R ISO 15288-2005. 2005. Sistemnaya inzheneriya. Protsessy zhiznennogo tsikla sistem [Systems engineering. Systems lifecycle processes].

Received August 7, 2017

Contributors

Zatsarinny Alexander A. (b. 1951) — Doctor of Science in technology, professor, Deputy Director, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; AZatsarinny@ipiran.ru

Korolev Vadim I. (b. 1943) — Doctor of Science in technology, professor; leading scientist, Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; professor, National Research Nuclear University "MEPhI," 31 Kashirskoye Highway, Moscow 115409, Russian Federation; professor, Financial University under the Government of the Russian Federation, 49 Leningrad Prosp., Moscow 125993; Russian Federation; VKorolev@ipiran.ru