

О сложности подсистем разграничения доступа крупномасштабных информационных систем

Н.Ф. Богаченко
nfbogachenko@mail.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация

Описываются признаки сложных систем. Определяются возможные метрические характеристики этих признаков. Рассматриваются крупномасштабные информационные системы и их подсистемы разграничения доступа. Доказывается принадлежность таких подсистем разграничения доступа классу сложных систем. Обосновывается необходимость автоматизации процессов управления подсистемой разграничения доступа в крупномасштабных информационных системах.

Введение

В настоящее время наблюдается рост проблем, возникающих при работе подсистем разграничения доступа крупномасштабных информационных систем, в первую очередь связанных с ошибками проектирования и администрирования политики разграничения доступа. Объясняется это тем, что в силу своих размеров крупномасштабные системы обладают рядом характеристик, из которых следуют особенности разграничения доступа к информации в таких системах. Эти особенности существенно влияют на работу подсистемы разграничения доступа и обосновывают необходимость разработки новых методов и средств управления разграничением доступа к информационным ресурсам с учётом специфики крупномасштабных информационных систем. При этом управление включает в себя такие процессы как формальный анализ, проектирование, построение, оптимизация и т. д.

В данной статье при помощи признаков и метрик сложных систем обосновывается актуальность задачи построения автоматизированных систем управления подсистемой разграничения доступа к ресурсам крупномасштабных информационных систем.

1 Признаки сложных систем

В системном анализе и в общей теории систем под сложной (большой) системой понимается множество, элементы которого находятся в некоторых отношениях (связях) друг с другом и которые образуют определённую целостность (единство). В свою очередь, эта целостность обладает новым качеством, не присущим отдельным элементам множества [1]. В рамках развития теории сложных систем в работе [2] сложные (большие) системы определяются как сети, содержащие множество компонент, которые взаимодействуют друг с другом, как правило, нелинейным способом.

Copyright © by the paper's authors. Copying permitted for private and academic purposes.

In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data, Modeling and Security 2018 (DMS-2018), Omsk, Russia, October 2018, published at <http://ceur-ws.org>

Понятие «сложная (большая) система» вводится в первую очередь не с целью классифицировать системы на «сложные (большие)» и «простые (небольшие)», а чтобы выделить общие принципы, присущие крупномасштабным системам с учётом их многообразия и сложности. Тем не менее, и в общей теории систем, и в теории сложных систем, остаётся открытой проблема формализации критериев сложной системы в виде соответствующих метрик. Наличие метрик сложных систем позволило бы сравнивать и ранжировать системы между собой на основе формальных критериев.

Одним из признаков сложной системы является большое число её элементов – *масштабность*. Но этой характеристики не достаточно для того, чтобы отнести систему к классу сложных систем. Сложная система – это масштабный комплекс *сложно взаимодействующих* элементов, сбой или потери в одной части системы могут непредсказуемым образом сказаться на системе в целом. Формально сложная система может быть представлена набором

$$S = \langle A, N, R_1, \dots, R_k \rangle,$$

где $A = \{a_1, \dots, a_N\}$ – множество элементов, N – мощность множества A , $R_i \subseteq A \times \dots \times A = A^{m_i}$ ($m_i > 1$, $i = 1, \dots, k$) – отношения на множестве A . В простейшем случае $k = 1$, $m_1 = m = 2$. Это означает, что на множестве A определено одно бинарное отношение R . Нередко такое отношение обладает свойствами антисимметричности и транзитивности, то есть является отношением порядка.

Согласно [3], «сложные системы часто являются иерархическими и состоят из взаимосвязанных подсистем, которые в свою очередь также могут быть разделены на подсистемы, и т.д., вплоть до самого низкого уровня». Этот признак назовём *возможностью декомпозиции*:

- 1) элемент сложной системы является системой более низкого порядка сложности:

$$a_i = \langle A_i, N_i, R_{i1}, \dots, R_{ik_i} \rangle;$$

- 2) сложная система является элементом системы более высокого порядка сложности:

$$S \in \{S_1, \dots, S_\nu\}.$$

Для сложной системы характерна *гетерогенность (разнородность)* элементов множества A . Данный признак хорошо укладывается в концепцию представления элементов сложной системы в виде подсистем более низкого порядка сложности: множества A_i ($i = 1, \dots, N$) могут иметь различную природу элементов, то есть принадлежать разным универсумам $U_1, \dots, U_n$, $0 < n \ll N$.

Для информационных и технических систем значимым и даже определяющим является ещё один признак: *иерархическая структура управления* системой [4]. Это означает, что на множестве субъектов управления задаётся отношение порядка – первый шаг к увеличению сложности уже самой системы управления.

Указанные качественные признаки сложных систем и возможные количественные характеристики (метрики) представлены в таблице 1. Первые четыре метрики позволяют сравнивать сложные системы между собой. Для ранжирования сложных систем целесообразно использовать дополнительную метрику – порядок сложности системы. Данная характеристика является относительной и определяется допустимым уровнем абстракции.

Таблица 1: Характеристики сложных систем

	Признак	Метрика
1.	Масштабность	Число элементов N
2.	Сложность взаимодействия	Число связей, определяемое как сумма мощностей всех заданных на множестве A отношений: $ R_1 + \dots + R_k $
3.	Разнородность (гетерогенность)	Число универсумов n
4.	Иерархия управления	Метрические характеристики теоретико-графового представления отношения порядка на множестве субъектов управления
5.	Возможность декомпозиции	Порядок сложности

Определение сложной системы по-прежнему возможно дать лишь на качественном уровне в виде следующих достаточных условий.

Предположение 1. Система относится к классу сложных систем, если она обладает следующими признаками: масштабностью, сложностью взаимодействия, разнородностью, иерархией управления и возможностью декомпозиции.

Следует отметить, что для сложных *информационных* систем возможность декомпозиции заложена в само понятие алгоритма и реализована в современных языках программирования. Поэтому далее, рассматривая сложные информационные системы, этот признак будем считать присутствующим по умолчанию.

В силу своих признаков сложная система характеризуется нехваткой ресурсов для эффективного управления [5]. Поэтому в таких системах должна быть подсистема принятия решения, что обосновывает следующий постулат.

Предположение 2. *Управление сложной системой осуществляется на основе совместного участия человека и автоматизированной системы управления.*

2 Управление политикой разграничения доступа

В рамках проблемы проектирования и администрирования политики разграничения доступа в современных информационных системах рассмотрим иерархию сложности систем и место подсистемы разграничения доступа в этой иерархии (см. рис. 1).

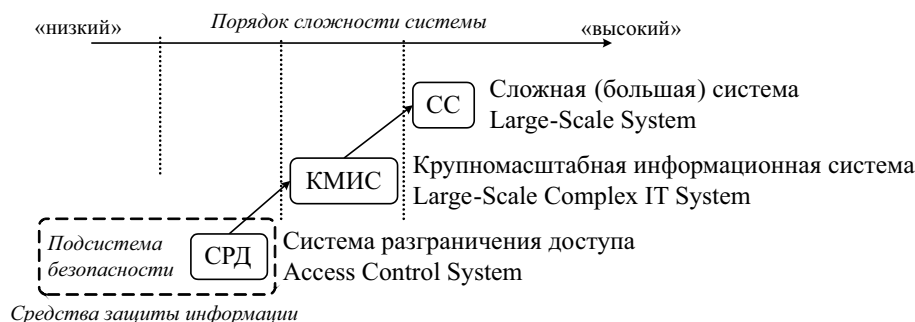


Рис. 1: Порядок сложности систем

Примерами сложных систем (Large-Scale Systems) наиболее высокого порядка являются транспортные, экономические, биологические, социальные и др. системы. Для их изучения и возможности управления разрабатываются автоматизированные системы управления или, в более широком смысле, информационные системы.

Информационные системы, также удовлетворяющие требованиям, предъявляемым к сложным системам, принято называть крупномасштабными информационными системами (КМИС, Large-Scale Complex IT Systems).

Далее наблюдается в некотором смысле самоподобный процесс (процесс мета-управления¹): с ростом сложности информационных систем возрастает сложность их управления. В связи с этим модели сложных систем приходится использовать уже в управлении.

В рамках подсистемы безопасности КМИС выделяется система разграничения доступа (СРД, Access Control System), которая реализует политику разграничения доступа к ресурсам информационной системы. СРД относится к информационной системе более низкого порядка сложности, чем КМИС в целом. Но современные программно-технические комплексы таковы, что их СРД также обладают признаками сложной системы. В работе [6] выделены следующие основные особенности разграничения доступа в КМИС:

- 1) существенное увеличение числа пользователей и объектов;
- 2) распределённость и иерархичность объектов доступа;
- 3) изменяемость правил разграничения доступа;
- 4) необходимость совмещения политик разграничения доступа.

Эти особенности являются основными свойствами СРД КМИС и характеризуют её как сложную систему (см. рис. 2). В том случае, когда управление СРД, то есть управление самой политикой разграничения доступа, уже не может осуществляться одним или несколькими не взаимодействующими между собой администраторами безопасности, возникает необходимость в иерархии управления. Востребованность иерархической структуры администрирования СРД КМИС подтверждена как теоретическими, так и практическими решениями. В частности, иерархия управления разграничением доступа заложена в ролевую модель

¹ Метауправление (metamanagement) – управление самой системой управления, призванное, во-первых, обеспечить согласованную и эффективную работу подсистем и элементов системы управления и, во-вторых, обеспечить в случае необходимости её изменение (развитие).



Рис. 2: Характеристика СРД КМИС как сложной (большой) системы

в виде иерархии административных ролей [7], а набор иерархически организованных административных ролей в современном программном обеспечении нередко задаётся «по умолчанию» [8, 9].

Согласно предположению 1, СРД с иерархией управления принадлежит классу сложных систем. Для таких СРД предположение 2 обосновывает востребованность автоматизированных систем управления политикой разграничения доступа – систем управления разграничением доступа (СУРД, Access Control Management Systems). Эти системы на первом этапе своего развития могут представлять собой системы поддержки принятия решений и позволят автоматизировать процессы проектирования и администрирования политики разграничения доступа КМИС.

Подводя итог, ещё раз отметим, что для управления сложной системой разрабатываются КМИС, для управления КМИС используются в частности СРД, а для управления СРД востребованы СУРД в том случае, когда возникает необходимость в иерархии управления политикой разграничения доступа (см. рис. 3).

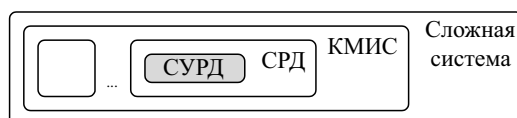


Рис. 3: Место системы управления разграничением доступа в иерархии сложности систем

Заключение

В настоящее время предлагаются программно-технические решения в области управления разграничением доступа к информационным ресурсам – системы управления идентификационными данными и доступом пользователей (Identity and Access Management System). Как показано в [6], основной недостаток таких систем заключается в том, что большинство операций по управлению политикой разграничения доступа перекладывается на «плечи» администратора безопасности или задаётся «по умолчанию» и через шаблонные решения. Это приводит к серьёзным проблемам в случае, когда подсистема разграничения доступа относится к классу сложных систем. По сути полноценной автоматизированной управляющей надстройки над системой разграничения доступа не происходит. Вышесказанное обосновывает актуальность задачи разработки и развития СУРД.

Остаётся открытым вопрос об оценке эффективности внедрения СУРД. Возможно предложить следующие критерии: сложность администрирования и защищённость КМИС. Сложность информационной системы может пониматься как число элементарных операций, необходимых для получения результата при любом допустимом входном наборе данных. Если в качестве меры сложности управления СРД определить число элементарных операций, выполняемых администратором безопасности, то очевидно, автоматизация процессов управления существенно снизит сложность администрирования. Возможно сопоставление числа настраиваемых параметров, которые администратором безопасности задаются «в ручном режиме», до и после внедрения СУРД в зависимости от масштабов информационной системы. Чтобы оценить, повысилась ли защищённость КМИС при переходе от «ручного» управления политикой разграничения доступа к СУРД, следует проанализировать, на сколько уменьшилось количество ошибок администрирования, связанных с управлением доступом к информационным ресурсам.

Список литературы

- [1] V.J. Cvetkov. Systematics of complex systems. *Modern Management Technology*, 7(79), 2017 (In Russian). URL: <https://sovman.ru/article/7903/>.
- [2] H. Sayama. *Introduction to the Modeling and Analysis of Complex Systems*. Open SUNY Textbooks, Milne Library, State University of New York at Geneseo, 2015, 498 p.
- [3] G. Booch. *Ob"ektno-orientirovannyj analiz i proektirovanie s primerami prilozhenij na C++*. M., Binom, Laboratoriya znaniy, 2001 (In Russian).
- [4] A.A. Volodina, I.M. Levkin. Adaptivnyi Podkhod k Zashchite Informatsii v Bol'shikh Informatsionnykh Sistemakh. *Problema Kompleksnogo Obespecheniia Informatsionnoi Bezopasnosti i Sovershenstvovanie Obrazovatel'nykh Tekhnologii Podgotovki Spetsialistov Silovykh Struktur*. Mezhevuzovskii Sbornik Trudov VI Vserossiiskoi Nauchno-Tekhnicheskoi Konferentsii KONFIB'15. SPb, Universitet ITMO, 65–73, 2016 (In Russian).
- [5] V.M. Kaziev. *Vvedenie v sistemnyj analiz i modelirovanie* (In Russian). URL: <http://bigc.ru/theory/books/kvisam/>.
- [6] N.F. Bogachenko. The Analysis of Problems of Access Control Administration in Large-Scale Information Systems. *Mathematical Structures and Modeling*, 2(46):135–152, 2018 (In Russian).
- [7] R.S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman. Role-Based Access Control Models. *IEEE Computer*, 29(2): 38-47, 1996.
- [8] URL: <https://msdn.microsoft.com/ru-ru/library/mt592917.aspx>.
- [9] URL: <https://helpx.adobe.com/ru/enterprise/using/admin-roles.html>.

On the Complexity of Access Control Subsystems of Large-Scale Complex IT Systems

Nadezda F. Bogachenko

Signs of large-scale systems are described. Possible metric characteristics of these signs are defined. Large-scale complex IT systems and their access control subsystems are considered. Belonging of such access control subsystems to a class of large-scale systems is proved. The automation need of the management processes by the access control subsystem in the large-scale complex IT system is explained.