О СТРУКТУРЕ И КРИТЕРИЯХ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

ON THE STRUCTURE AND EFFICIENCY CRITERIA IN INFORMATION SYSTEM

A. Nikitenko

Summary. The article is devoted to the study of the composition, structural relations of the main elements of the information system, functional links between them, as well as criteria for the effectiveness of such a system. As a result of the analysis of scientific sources the variant of structuring of information system on elements of task and technological blocks is presented. Conditionally presents the relationship between these components. As an example of a possible organization of the information system, a description of the user authentication system according to the Schnorr scheme is given.

Keywords: information system, structure, performance criteria, Schnorr scheme.

Никитенко Андрей Владимирович
К.п.н., доцент, Ярославский государственный технический университет
rabota2142@mail.ru

Аннотация. Статья посвящена изучению состава, структурных соотношений основных элементов информационной системы, функциональных связей между ними, а также критериев эффективности такой системы. В результате анализа научных источников представлен вариант структурирования информационной системы по элементам задачного и технологического блоков. Условно представлены взаимосвязи между данными составляющими. В качестве примера возможной организации информационной системы приведено описание системы аутентификации пользователя по схеме Шнорра.

Ключевые слова: информационная система, структура, критерии эффективности, схема Шнорра.

На современном этапе развития науки изучение любого процесса или явления производится с использованием системного подхода. Его сущность заключается в том, что объекты рассматриваются под углом зрения внешних и внутренних свойств и связей, которые обуславливают единство и целостность объекта, его устойчивую внутреннюю организацию и функционирование как определенного целого. При этом учитываются их многомерность и иерархичность, когда целостный объект наряду с другими рассматриваются как часть или элемент целого более высокого порядка. Таким образом, реализуется комплексное изучение объектов.

С развитием информационных технологий все более широкое распространение получает понятие «информационная система», которое в зависимости от контекста интерпретируется по-разному. Исследуем некоторые трактовки и особенности данного явления с точки зрения образующего конструкта — слова «система».

Согласно Толковому словарю русского языка под системой понимается «нечто целое, представляющее собой единство закономерно расположенных и находящихся во взаимной связи частей» [3, с. 719]. С точки зрения философии, система представляет «совокупность элементов, находящихся в отношениях и связях друг с другом, которая образует определенную целостность, единство» [2, с. 552]. При этом выделяются следующие основные системные принципы:

- целостности (под которой понимается зависимость каждого компонента, отношения и свойства системы от его функций, места внутри целого; а также принципиальная несводимость свойств системы к сумме свойств составляющих ее элементов и невыводимость из последних свойств целого);
- структурности (возможность через установление структуры системы описания ее свойств, т.е. совокупности связей и отношений ее элементов; а также обусловленность поведения системы не столько поведением ее отдельных элементов, сколько свойствами ее структуры);
- взаимозависимости системы и среды (система, являясь ведущим активным компонентом взаимодействия, формирует и проявляет свои свойства непосредственно в процессе взаимодействия со средой);
- иерархичности (рассматриваемая система может быть описана как один из элементов более широкой системы, но в то же время каждый компонент изучаемой системы, в свою очередь, может быть представлен как особая отдельная система со своими уникальными свойствами и отношениями структурных составляющих);
- множественности описания каждой системы (поскольку каждая система может быть представлена бесконечно сложным объектом, то для ее достаточного познания требуется построить набор различных вариантов моделей, каждая из кото-

рых отражает только одну определенную грань или свойство такой системы).

В системном анализе система понимается как средство достижения цели, при этом выделяются основные особенности систем: целостность, относительная обособленность от окружающей среды, наличие связей со средой, наличие частей и связей между ними (структурированность), подчиненность всей организации системы некоторой цели [4, с. 359].

Таким образом, все процитированные описания близки в понимании системы как определенной целостности, состоящей из совокупности частей (элементов, компонентов), находящихся в связях друг с другом и средой. Выделим также положения о возможности описания системы через установление ее структуры, т.е. сети связей и отношений, а также о подчиненности всей организации системы некоторой цели. Опираясь на данные заключения, опишем структуру и некоторые особенности информационных систем (далее ИС).

Согласно Федеральному закону Российской Федерации об информации, информационных технологиях и о защите информации, ИС представляет собой совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств. Таким образом, к структурным компонентам ИС отнесем: базу данных, в которой содержится информация, информационные технологии и технические средства для ее обработки. В данном случае под информационными технологиями Федеральный закон понимает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

В глоссарии по информационному обществу уточняется, что ИС включает вычислительное и коммуникационное оборудование, программное обеспечение, данные и метаданные, лингвистические средства, а также системный персонал, и обеспечивает поддержку информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей [1, с. 59]. В данной трактовке вычислительное и коммуникационное оборудование, программное обеспечение, лингвистические средства отнесем к техническим средствам обработки информации, а данные и метаданные — к базе данных в терминах Федерального закона Российской Федерации об информации, информационных технологиях и о защите информации. Однако, системный персонал выделим отдельным элементом ИС. Отметим также то, что в глоссарии указана возможная цель, которой подчиняется вся организация системы — это «удовлетворение информационных потребностей пользователей». При этом самих пользователей будем рассматривать как один из элементов ИС, т.к. пользователи, взаимодействуя с каждым другим элементом ИС, способны их менять, например, редактируя базу данных, обрабатывая и распространяя информацию из нее. Кроме того, корректируя свои информационные потребности, пользователи ИС способны изменить всю ее организацию. Поэтому пользователей ИС будем рассматривать основополагающим компонентом, под который строится вся система. Как было сказано выше, пользователи способны корректировать цель ИС, поэтому данный элемент расположим на втором месте иерархии всей системы. В свою очередь цель ИС, взаимодействуя с остальными элементами системы, оказывает первостепенное влияние на информацию, хранящуюся в базе данных.

Отметим, что в структуре ИС, как и любой другой системы, выделяются два исходных понятия научной теории: ее задачи и технологии их решения. Поэтому условно структурируем первые три элемента ИС (пользователи, цель, база данных) в задачный блок (в нем генерируется задача всей системы).

Каждая задача блока разрешается с помощью адекватной технологии, организуемой в технологическом блоке ИС, целостность которого обеспечивается взаимосвязанной разработкой и использованием трех оставшихся элементов системы: системного персонала, технических средств обработки информации и соответствующими информационными технологиями. В частности, для достижения цели ИС системный персонал с помощью технических средств производит поиск, сбор, хранение, обработку, предоставление и распространения информации в базе данных.

При определении структуры любой сложной системы одним из важнейших этапов является также выделение и описание критериев эффективности ее работы. При этом отметим, что эффективность информационных систем является во многом комплексной характеристикой совокупности нескольких показателей. К таким показателям можно отнести набор технических, эксплуатационных, экономических и других условий, что в совокупности требует постоянного совершенствования не только отдельных показателей, но и возможностей по оцениванию эффективности ИС как единого объекта. Вместе с тем решение задач по оценке эффективности и прогнозирования ИС связано с развитием и повышением качества средств и методов по обработке информации, координации работы сложных объектов и организации поддержки принятия решений. Суть такой проблемы заключается в совершенствовании известных, а также создании и внедрении инновационных методов системного анализа. Так в экономической трак-

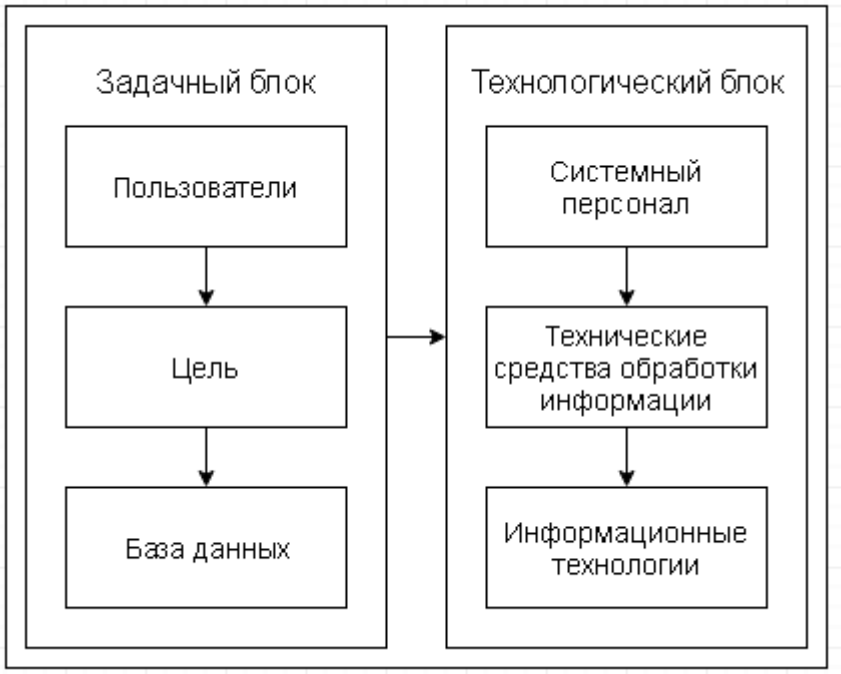

Рис. 1. Структура информационной системы.

Этап 1. Генерация ключей (выполняет А).

№	Описание операции	Пример
1	Выбираются два простых числа p и q такие, что (p - 1) mod q = 0.	p = 23, q = 11
2	Выбирается секретный ключ x ∈ {1, …, q-1}.	x=3
3	Выбирается g такое, что g^q mod p = 1.	g=3 3^{11} mod 23 = 1
4	Вычисляется открытый ключ y такой, что (g^x * y) mod p = 1.	y=6 (3^3 * 6) mod 23 = 162 mod 23 = 1
5	Публикация открытого ключа y.	

Этап 2. Аутентификация.

№	Описание операции	Пример
1	А выбирает случайное число k ∈ {1, …, q-1}, вычисляет r = g^k mod p и посылает r Б.	k = 6 r = 3^6 mod 23 = 16
2	Б выбирает случайное число e ∈ {0, …, 2^t-1}, где t — некоторый параметр, и посылает e А.	e=4
3	А вычисляет s = (k + x * e) mod q и посылает s Б.	s = (6 + 3 * 4) mod 11 = 7
4	Б проверяет соотношение r = (g^s * y^e) mod p и, если оно выполняется, принимает доказательство, в противном случае — отвергает.	16 = (3^7 * 6^4) mod 23=16

```
enter prime number p
23
enter prime number q
11
number x= 3
enter  number g
3
public key y equals to 6
k=6
A send r16
enter  number e
4
B send e
A send s7
OK
```

Рис. 2. Пример работы системы аутентификации по схеме Шнорра.

товке проблему оценки эффективности действий системы можно интерпретировать как задачу оптимизации использования средств, направляемых на бесперебойное функционирование и развитие ИС. При этом задача может быть поставлена следующим образом: выявить такой оптимальный объем информации, используемой в процессе принятия решений, который обеспечивает соответствующий уровень качества принимаемых решений, но также минимизирует затраты на его обеспечение.

Таким образом, для анализа продуктивности ИС нужно оценить ее влияние на уровень удовлетворения информационных потребностей пользователей и качество принимаемых решений. Опыт внедрения и сопровождения информационных систем показывает, что можно выделить следующие принципы выбора критериев эффективности работы информационной системы. Это принципы: сбалансированности объема информации, требуемой для качественного принятия решений с объемами информации, которые способна переработать система; взаимосвязанного изучения совокупности показателей эффективности и качества информационных процессов; обоснованности стоимости, временных и других ресурсов в контексте решения каждой функциональной задачи системы; эффективного распределения затрат между компонентами системы.

Таким образом, определены состав и структурные соотношения основных элементов ИС, а также функциональные связи между ними (рис. 1). По нашему мнению, в описании такой структуры содержится полная информация о любых информационных системах, достаточная для анализа сущности системы, сравнения различных ИС между собой, а также для их проектирования, прогнозирования их развития и экспериментального исследования.

Далее приведем вариант организации информационной системы на примере системы аутентификации пользователя по схеме Шнорра [5]. Присутствуют 2 участника А и Б. Все расчёты по генерации ключей проводит участник А. Для начала выбираются два простых числа p и q такие, что (p-1) mod q = 0. Затем выбирается секретный ключ $x \in \{1, \ldots, q-1\}$. После этого выбираем g такое, что gqmod p = 1. Далее вычисляем открытый ключ y такой, что (gx * y) mod p = 1 и публикуем его. На этом этап генерации ключей завершен. Аутентификация начинается с выбора участником А числа $k \in \{1, \ldots, q-1\}$ и расчёта r = gkmod p, которое посылается Б. Б выбирает случайное число e и отправляется его А. А вычисляет s = (k + x*e) mod q и посылает s Б. Б проверяет соотношение r = (gs * ye) mod p и, если оно выполняется, принимает доказательство, в противном случае — отвергает.

Вся работа может быть разбита непосредственно на 2 этапа.

Появившееся в последней строке слово «ОК» свидетельствует об успешности аутентификации пользователя.

Таким образом, описаны состав, структурные соотношения основных элементов информационной системы, функциональные связи между ними, критерии эффективности такой системы, а также приведем вариант организации информационной системы на примере системы аутентификации пользователя по схеме Шнорра.

ЛИТЕРАТУРА

1. Глоссарий по информационному обществу / Под общ. ред. Ю. Е. Хохлова. — М.: Институт развития информационного общества, 2009. — 160 с.
2. Новая философская энциклопедия / Ин-т философии РАН, Нац. общ.-научн. фонд. — М.: Мысль, 2010.
3. Ожегов, С. И. Толковый словарь русского языка. Российская академия наук. Институт русского языка им. В. В. Виноградова. — 4-е изд., дополненное / С. И. Ожегов, Н. Ю. Шведова. — М.: Азбуковник, 1997. — 944 с.
4. Перегудов, Ф. И. Введение в системный анализ / Ф. И. Перегудов, Ф. П. Тарасенко. — М.: Высшая школа, 1989. — 364 с.
5. Schnorr C. P. Efficient Signature Generation by Smart Cards. — J. Cryptology, 1991. — С. 161–174.

Журнал «Современная наука: актуальные проблемы теории и практики»