Eurocrypt '95, 1995. ***25.*** *K. Ohkuma, H. Shimizu, F. Sano, S. Kawamura, "Security assessment of Eurocrypt and Rijndael against the differential and linear cryptanalysis (extended abstract)." in Proceedings of the Second NESSIE Workshop, 2001.* ***26.*** *E. Biham and N. Keller, "Cryptanalysis of reduced variants of Rijndael." in Proceedings of the Third Advanced Encryption Standard Conference. NIST. 2000.* ***27.*** *S. Lucks "Attacking seven rounds of Rijndael under 192-bit and 256-bit keys." In Proceedings of the Third Advanced Encryption Standard Conference. NIST. 2000.* ***28.*** *A. Biryukov, D. Wagner. Slide Attacks. In FSE'99, Volume 1636 of LNCS, Springer-Verlag, Berlin, 1999.* ***29.*** *J. Daemen, R. Govaerts, J. Vandevalle. Weak Keys for IDEA. Proceedings of Crypto'93, Advances in Cryptology, Springer-Verlag, 1993.* ***30.*** *J. Moore, G. Simmons. Cycle Structure of the DES with Weak and Semi-Weak Keys. Advances in Cryptology — CRYPTO'86, Springer-Verlag, Berlin 1987.* ***31.*** *J. Fuller, W. Millan. "On linear redundancy in S-boxes." in Proceedings of FSE'03 . LNCS, Springer-Verlag, 2003.* ***32.*** *A. M. Youssef, S. E. Tavares. "On some algebraic structures in the AES round function." http://cryptonessie.org.* ***33.*** *S. Murphy, M.J.B. Robshaw, "Essential algebraic structure within the AES." in Proceedings of Crypto'02, no. 2442 in LNCS, Springer-Verlag, 2002.* ***34.*** *N. T. Courtois, J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. Proceedings of Asiacrypt'02, LNCS. Springer-Verlag, 2002.* ***35****. D. Coppersmith. XSL Against Rijndael. CRYPTO-GRAM, October 2002.* ***36.*** *T. Moh. On the Courtois-Pieprzyk's attack on Rijndael. University of San Diego. 2002.* ***37.*** *N. Ferguson, R. Schroeppel, D. Whiting, "A simple algebraic representation of Rijndael." In Proceedings of Selected Areas in Cryptography'01 no. 2259 in LNCS. Springer-Verlag, 2001.* ***38.*** *Elad Barkan and Eli Biham. "In how many ways can you write Rijndael?" Proceedings of Asiacrypt'02, LNCS. Springer-Verlag, 2002.* ***39.*** *E. Barkan, E. Biham. The Book of Rijndaels. http://www.cs.technion.ac.il/~biham/.* ***40.*** *E. Filiol. Plaintext Dependant Repetition Codes Cryptanalysis of Block Ciphers – The AES Case. ESAT/DEASR/SSI. France, 2003.* ***41.*** *N. T. Courtois. About Filiol's Observations on DES, AES and Hash Functions (draft). CP8 Crypto Lab, SchlumbergerSema, 36-38 rue de la Princesse BP 45, 78430 Louveciennes Cedex, France.* ***42.*** *Nicolas T. Courtois, Robert T. Johnson, Pascal Junod, et. al. Did Filiol Break AES ? University of California, Berkeley, USA.* ***43.*** *NESSIE public report D21. Performance of Optimized Implementations of the NESSIE Primitives. http://cryptonessie.org.* ***44.*** *М. Ф. Бондаренко, И. Д. Горбенко, А. В. Потий и др. Улучшенный стандарт симметричного шифрования XXI века: концепция создания и свойства кандидатов. Радиотехника. 2000. Вып. 114. С. 5-14.* ***45.*** *И. Д. Горбенко, Д. А. Чекалин. Свойства и возможности оптимизации криптографических преобразований в AES – Rjndael. Радиотехника. 2001. Вып. 119. С. 36-42.*

УДК 681.5

ТЕОРЕТИКО-КОНЦЕПТУАЛЬНЫЙ ПОДХОД К ПРОБЛЕМЕ КАЧЕСТВА И ЦЕННОСТИ ИНФОРМАЦИИ В ЭРГАСИСТЕМЕ

Дмитрий Кабелев, Александр Князев, Дмитрий Ловцов
ФГУП "Институт точной механики и вычислительной техники имени С. А. Лебедева РАН", г. Москва

Аннотация: **Рассматривается теоретико-концептуальный подход к проблеме качества и ценности информации в эргасистеме, включающий выбор и определение видов и качественных форм проявления информации, характерных для эргасистем, рациональное распределение в эргасистеме апробированных информационных мер, основные требования к мерам количества и качества структурной и содержательной информации, принцип информационной ценности.**
Summary: **The theoretical and conceptual approach to information quality and value problem is considered. The approach includes the choice and determination of types and qualitative forms of information manifestation that are characteristic of the ergatic systems, the efficient distribution in ergatic system of the accepted information measures, the main requirements on measures of quantity and quality of structural and content information, the principal of information value.**
Ключевые слова: **Информация, качество информации, информационная ценность.**

I Введение

Термин *информация* многозначен (от наиболее общего философского значения – информация есть отраженное разнообразие объективного мира, до наиболее частного прикладного – информация есть сведения, являющиеся объектом переработки), а закономерности получения и преобразования информации еще мало изучены (отсутствует универсальный математический аппарат для их описания). Поэтому уточним, с учетом известных определений, смысл этого термина следующим образом. Под информацией в "широком" смысле будем понимать особое свойство объектов (процессов) окружающего материального мира порождать

разнообразие состояний, которые посредством отражения передаются от одного объекта к другому (пассивная форма), и средство ограничения разнообразия, т. е. организации, управления, дезорганизации и др. (активная форма) [1, 2].

Использование данного методологического определения информации как одного из основных свойств (атрибутов) объективного мира, связанного с наличием в нем особого рода процессов, называемых информационными, позволяет на практике, во-первых, осознать наличие и, отсюда, необходимость учета в эргатической системе (сложной человеко-машинной системе управления предприятием, корпорацией, ведомством, государством, и др.) объективных информационных характеристик (ограничений) обслуживающих и обслуживаемых объектов (процессов) любой физической природы – как разнообразия состояний последних и разнообразия их влияния на информационные характеристики субъективных сведений (знаний), циркулирующих между объектами, способными их осмыслить. Такой учет, в частности, обеспечит формализацию объективной и субъективной части информационного ресурса эргатической системы (эргасистемы) с целью его рационального употребления (расходования) для более полного использования целевых возможностей объектов управления.

Во-вторых, согласно данному определению можно и следует применять информацию как средство ограничения разнообразия состояний объектов (процессов), осуществляя тем самым активное воздействие на их информационные характеристики в соответствии с поставленными целями.

Известен подход к определению информации на основе учета ее неразрывной взаимосвязи и взаимообусловленности с системой и управлением. Такое рассмотрение информации позволяет не только уточнить понимание информации как особого свойства объектов-систем, но и формализовать определения информации различных видов и форм, характерных для эргасистемы.

II Классификация и определение видов информации

Применим к определению понятия “информация” синтетический атрибутивно-функциональный подход, т. е. подход, частично объединяющий идеи философско-методологического и кибернетического подходов. Согласно атрибутивно-функциональному подходу в эргасистеме можно рассматривать два рода информации (объективную и субъективную), которые представляют собой [3, 4]:

внутреннюю структурную (преобразующую) информацию объектов эргасистемы, заключенную в структурах эргасистемы, элементов управления, алгоритмов и программ переработки информации и являющуюся физической величиной;

внешнюю содержательную (специальную, главным образом осведомляющую, измерительную и управляющую, а также научно-техническую, технологическую, планово-экономическую и др.), извлекаемую из информационных массивов (сообщений, команд и пр.) относительно индивидуальной модели предметной области (тезауруса) получателя (человека, подсистемы, эргасистемы).

Первая связана с качеством информационных процессов в эргасистеме, с внутренними технологическими эффектами (получаемыми в информационном процессе в результате применения определенной совокупности подсистем, элементов, алгоритмов и программ по сравнению с другой), с затратами на переработку информации.

Вторая связана, главным образом, с внешним целевым (материальным) эффектом, получаемым в управляемом объекте (процессе).

Структурная информация – это отраженная в знаковой форме организованность (сложность, разнообразие) материальных объектов-систем, являющаяся универсальной физической величиной, используемой для описания процессов функционирования объектов.

Поскольку структурная информация является физической величиной, она измерима (а значит, можно указать алгоритм получения ее количества) и объективна, т. е. количество информации не зависит от потребителей и не уменьшается при последующих получениях ее потребителями; следовательно, его нельзя измерять через априорную вероятность информационного сообщения для получателя (как это делается, например, в информационной теории связи К. Шеннона и Н. Винера). Наличие (содержание, порождение) в структурной информации некоторого количества есть внутреннее свойство эргасистемы, и любая выбранная информационная мера должна опираться именно на внутренние характеристики (особенности) эргасистемы (иначе структурная информация не является физической величиной, и в различных экспериментах в связи с различными внешними факторами-условиями значения количества структурной информации будут различными). Структурная информация, содержащаяся в эргасистеме, представляет собой ее структурно-информационный ресурс и, в конечном счете, – частичное (полное) описание-модель этой эргасистемы как информационной. Учет используемого (употребляемого) количества структурной информации в эргасистеме (объекте, информационном узле) может способствовать получению от нее различных технологических

эффектов. Так количество структурной информации фактически характеризует затраты (информационные, вещественные и энергетические) в эргасистеме на переработку содержательной информации.

Содержательная информация – это совокупность сведений (знаний) о конкретном материальном объекте-системе или процессе (семантический аспект), содержащаяся в информационных массивах (массивах данных, массивах программ, сообщениях, фактах), воспринимаемая получателем (человеком-оператором, информационным узлом, эргасистемой и др.) и используемая им для выработки (с учетом его индивидуального или общесистемного тезауруса – накопленных знаний, целей и задач) и принятия управляющего решения (прагматический аспект); имеет субъективный характер. Наличие (получение) содержательной информации в эргасистеме (элементе принятия решений) позволяет получателю уменьшить имеющуюся неопределенность (разнообразие) истинной ситуации и на основе этого сделать выбор одного или нескольких вариантов из множества возможных равноправных альтернатив.

Важной разновидностью содержательной информации является коммуникационная информация, характеризующая процессы взаимодействия (взаимосвязи) функциональных элементов и подсистем эргасистемы (т. е. “шенноновская” информация).

Коммуникационная информация – это совокупность сведений (знаний) о конкретном процессе взаимодействия в ансамбле материальных объектов-систем, содержащаяся в статистических структурах заданного множества информационных массивов (сообщений), воспринимаемая получателем (человеком-оператором, системой и др.) и используемая им (с учетом его индивидуального или связного тезауруса – накопленных знаний) для определения состояния источника информации.

Применительно к информационному узлу (подсистеме) эргасистемы можно определить взаимоотношение рассмотренных видов информации следующим образом:

на вход поступает информация осведомляющая (контрольная, сигнальная и др.), объединяющая содержательную (семантическую и прагматическую) информацию массивов-сообщений и коммуникационную (структурно-статистическую);

в эргасистеме хранится и используется при переработке поступающей осведомляющей информации преобразующая информация, объединяющая структурную информацию эргасистемы и содержательную информацию общесистемного тезауруса;

на выходе эргасистемы формируется преобразованная информация или информация для принятия решения, которая после реализации исполнительным органом управления обслуживаемого объекта эргасистемы становится управляющей.

III Декомпозиция качества и определение ценности информации

Для оценки целевого материального эффекта в эргасистеме требуется оптимизация по многим критериям, и в результате вместо получения экстремальных значений показателей эффективности часто приходится рассматривать рациональные (компромиссные, сатисфакционные) решения. Последние могут характеризоваться некоторой системой требований, аксиоматически описывающих такие содержательные понятия как приемлемость, равноправие, равнозначность, справедливость, и др. Очевидно, что возможность удовлетворять такой ансамбль требований зависит от информационных ограничений, действующих в эргасистеме, т. е. от качества информации, под которым понимают совокупность таких ее свойств, которые характеризуют степень ее соответствия потребностям (целям, ценностям) пользователей (эргасистемы, персонала и др.)

Можно выделить внутреннее качество информации (присущее именно ей и сохраняющееся при ее переносе в другую эргасистему или подсистему) и внешнее (присущее информации, находящейся или используемой только в конкретной эргасистеме, подсистеме). Эти качества определяются, главным образом, следующими иерархиями конструктивных свойств, соответственно [5, 6]:

<*содержательность*> := {<значимость (идентичность, полнота)>, <кумулятивность (гомоморфизм, избирательность)>, и др.};

<*защищенность*> := {<достоверность (помехоустойчивость, помехозащищенность)>, <сохранность (целостность, готовность)>, <конфиденциальность (доступность, скрытность, имитостойкость)>, <юридическая значимость (аутентичность, легитимность, верифицируемость)>, и др.}.

Известные подходы к решению проблемы соответствия информации потребностям пользователей или, иначе, к решению проблемы ценности информации, имеют принципиально общие черты:

ценность информации предлагается измерять через ее количество (М. Гавурин, Б. Гришанин, Р. Стратонович, и др.);

ценность информации предлагается связывать с поставленной задачей (М. Бонгард, Д. Конторов, А. Харкевич, и др.).

Однако, при этом не учитывается множество качественных характеристик информации. Поэтому при дальнейшем развитии подхода к определению ценности информации нужно, в частности, учитывать:

качество информации, включая как внутренние свойства информации (содержательность), так и внешние (защищенность);

информационный ресурс эргасистем и способ его использования для переработки информации.

Тогда можно сформулировать следующее определение. Под *ценностью* информации понимается ее значимость, определяемая способом динамического отображения множества ее качественных свойств и количественных характеристик на множество возможных управляющих решений, ведущих к достижению целей управления (функционирования) объектом.

Согласно предложенному определению ценности информации можно сформулировать принцип оптимальности переработки информации в эргасистеме как трехэкстремальный принцип информационной ценности: информационный структурно-содержательный ресурс (преобразующую информацию) эргасистемы следует использовать *рациональным* способом и только для переработки *наиболее ценной* осведомляющей информации, на основе которой действительно возможна выработка *оптимальных* (при данном ограничении на количество информации) управляющих решений, ведущих к достижению целей управления.

Под способом использования (употребления) информационного ресурса эргасистемы понимается специальная информационная технология как совокупность информационных процедур формирования (рецепции), интерпретации (преобразования, поиска, реорганизации) и коммуникации (передачи, хранения) информации на основе проблемно-ориентированной базы данных и знаний, элементами которой являются логико-лингвистическая модель предметной области, рациональная стратегия, продукционные правила и комплекс эффективных алгоритмов выработки решений, а также средства диалога с оператором-парапрограммистом, позволяющие ему заполнять (уточнять) содержание информационной базы и интерпретировать результаты.

В соответствии с сформулированным принципом информационной ценности в эргасистеме необходимо выполнить три экстремальные условия для обеспечения требуемого уровня качества и эффективности применения эргасистемы в целом, поскольку данные условия в совокупности определяют степень рациональности двух основных типов информационных процедур, реализуемых в эргасистемах, т. е. процедуры формирования информации для управления (первое и второе условия) и процедуры выработки целевых управляющих решений (второе и третье). Причем обеспечение первого и второго экстремумов связано с возможным противодействием сторон (т. е. в условиях так называемой “информационной борьбы”, включающей радиоэлектронную борьбу, инфильтрацию дезинформации, блокировку полезной информации, и др.).

IV Определение качественных форм проявления информации

Определение качественно различных форм проявления информации, циркулирующей в эргасистеме, возможно на основе анализа эргасистемы (процесса управления). В инвариантной модели кибернетической системы, базирующейся на применении фундаментальных принципов управления (принципа дуальности А. Фельдбаума и Р. Калмана, принципа оптимальности Р. Беллмана, принципа разделения Р. Калмана, принципа централизации), можно выделить такие качественно различные формы информации, как [1 – 3]:

1) *осведомляющая* информация, к которой относится вся информация об объективных характеристиках состава, структуры и свойств управляемого объекта (процесса), а также действующих на него управляющих и дестабилизирующих факторов внешней среды, выступающая как в пассивной, так и в активной формах;

2) *преобразующая* информация, которая заключена в структурах эргасистемы, ее элементов (пунктов, узлов) управления, алгоритмов и программ переработки информации, объединенных в информационной базе (информация и язык) эргасистемы, и обеспечивает сам информационный процесс в функциональных подсистемах измерения, наблюдения, идентификации, выработки управляющих решений, централизованной координации и информационного обмена;

3) *преобразованная* информация, в том числе:

информация измерения (восприятия), характеризующая отражение в подсистеме измерения полезных, с точки зрения решаемой задачи управления, свойств осведомляющей информации;

информация наблюдения (распознавания), характеризующая отражение ситуаций, определяемых осведомляющей информацией, на конечном множестве эталонных образцов, заданных элементами подсистемы;

информация идентификации (предсказания), характеризующая отражение на конечном множестве элементов подсистемы идентификации состояние или поведение управляемого объекта, которые с определенной вероятностью должны иметь место с заданным временем опережения;

информация выработки (принятия) решения, характеризующая отражение образов и целей (текущих и предсказываемых) на конечном множестве решений, заданных элементами подсистемы принятия решений;

информация централизованной координации и организационного управления, характеризующая отражение внешних целей и состояний всех подсистем на конечном множестве эталонных образцов, заданных элементами подсистемы централизованной координации;

информация связи, характеризующая отражение взаимодействия всех подсистем на конечном множестве элементов подсистемы информационного обмена;

4) *управляющая* информация – это вся информация, реализуемая в средствах организации (исполнительных органах) и являющаяся руководством (причиной) для их действия по целенаправленному изменению состава, структуры и свойств управляемого процесса (объекта).

В подсистеме централизованной координации воспринимается и распознается внешняя управляющая информация, задающая главную цель управления объектами, а также предсказывается изменение главной цели и принимается решение о том, какую цель взять в качестве задающей для контура управления объектом в целом и для каждой подсистемы контура в частности. Преобразованная в подсистеме координации информация содержит информацию о целях всех подсистем, являющуюся для них осведомляющей в активной форме. Последнее, как правило, приводит к накоплению полезной информации на выходах подсистем и установлению ассоциативных и других связей, что соответствует эффекту самообучения. В контуре формируется преобразованная информация, которая реализуется исполнительным органом управления обслуживаемого объекта.

V Сравнительный анализ информационных мер и требования к ним

Результаты проведенного анализа показывают, что основные особенности (достоинства, недостатки) наиболее известных мер информации (моделей измерения количества структурной и содержательной информации) сводятся к следующим [3, 4].

Классические меры информации Р. Хартли, К. Шеннона и А. Колмогорова наиболее приемлемы при описании динамики функционирования подсистемы информационного обмена и подсистем функционального преобразования информации (подсистем наблюдения и идентификации) соответственно. На основе их модификации и комплексирования возможен синтез мер информации, учитывающих архитектуру эргасистемы и управляемых объектов, виды и формы проявления информации в эргасистеме, ценность информации и пр.

С помощью синтетических информационных мер А. Шилейко и В. Кочнева, Ю. Шрейдера можно оценить информационно-структурный и информационно-содержательный ресурсы эргасистемы, что позволяет обеспечить рациональное использование совокупного информационного ресурса в функционирующей эргасистеме для получения различных целевых и технологических эффектов. Оценка последних возможна на основе соответствующих информационных показателей, использующих данные информационные меры в качестве компонентов.

При описании динамики функционирования подсистем эргасистемы можно также дополнительно использовать специфические меры информации, например, меру С. Кульбака – для подсистемы измерения, меру А. Харкевича – для подсистемы выработки (принятия) управляющих решений, и др.

Интегральные качественно-количественные меры А. Харкевича, Н. Моисеева, Б. Петрова используются для определения эффективности совместного функционирования подсистем сбора и переработки информации в эргасистеме в процессе выработки и принятия управляющих решений в условиях информационной неопределенности (неполноты информации).

Поскольку информация в эргасистемах имеет различные виды и качественные формы проявления, для измерения информационного структурно-содержательного) ресурса эргасистем следует использовать множество (обоснованную совокупность) различных мер информации. При этом, как показывают результаты сравнительного анализа мер информации, для рационального их применения на практике они должны отвечать следующим основным требованиям:

адекватность (соответствие виду и качественной форме проявления информации);

согласованность (отражение специфики предметной области, т. е. функциональной подсистемы эргасистемы и реализуемого в ней информационного процесса);

эффективность (алгоритмическая, регулярная вычислимость);

аддитивность (обеспечение определения совокупного информационного ресурса эргасистемы путем сложения количеств информации);

понятность (допущение рациональной информационной интерпретации).

Использование обоснованной совокупности (комплекса) мер информации, удовлетворяющих эти требования для конкретной эргасистемы, позволит реализовать “трехэкстремальный” принцип

оптимальности переработки информации в эргасистеме, сформулированный как принцип информационной ценности.

Прагматически рациональные меры информации (модели), а также совокупность информационных показателей эффективности реальных подсистем и эргасистемы в целом целесообразно разрабатывать согласно принципу оптимальности переработки информации. Это позволит учесть ценность информации, в частности, той, которая содержится в эргасистеме и с которой эргасистема оперирует в соответствии с целевой задачей, а также учесть затраты информационного ресурса при определении эффективности функционирования эргасистемы как информационной. Учет ценности информации, в свою очередь, позволит обеспечить своевременное и качественное регулирование, координацию и оптимизацию информационных процессов в эргасистеме.

VI Пример реализации подхода в реальной эргасистеме

В последнее десятилетие в мировой практике наметился переход от проблемы обеспечения защищенности (безопасности) информации в эргасистеме к проблеме обеспечения информационной защищенности (безопасности) эргасистемы.

Это связано с тем, что защищенность не является атрибутивным свойством информации, а является внешним ее свойством, присущим информации, находящейся в определенной эргасистеме, и изменяющимся при ее переносе в другую эргасистему. Следовательно, для обеспечения информационной защищенности (безопасности) эргасистемы необходимо учитывать специфику конкретной эргасистемы, ее архитектуру, а также виды и качественные формы проявления информации в эргасистеме, выявляя при этом *прагматическую* значимость и ценность информации. Например, существуют эргасистемы, такие, в частности, как межбанковские системы электронных платежей (СЭП), в которых информационная избыточность минимальна и, следовательно, прагматическая ценность информации в эргасистеме равна, что называется “живым деньгам”.

Группа сотрудников ИТМ и ВТ разработала на базе предложенного подхода оригинальную концепцию информационной безопасности СЭП, предполагающую комплексность решения проблемы информационной безопасности СЭП как защищенности ее информационных потребностей (а не только защищенности информации в СЭП). Концепция позволяет обеспечить *требуемое* внешнее качество информации с учетом специфики СЭП.

Разработанная концепция реализована, в частности, в межбанковской СЭП Центрального банка (ЦБ) России АСБР-“Москва” (автоматизированная система банковских расчетов), атрибутивная специфика которой характеризуется следующими основными особенностями [7]:

активностью участников-абонентов (банков) АСБР, соблюдающих исключительно личные интересы (в частности, допускающих недобросовестность, не доверяющих друг другу, и др.);

функциональной децентрализованностью эргасистемы, так как ЦБ выполняет только организующую функцию;

информационной безызбыточностью циркулируемых и перерабатываемых электронных документов (т. е. имеющих максимальную прагматическую ценность);

важностью человеческого фактора, обусловленной реальной возможностью “миграции” специальных кадров между банками (следствием чего являются, в частности, серьезные конфликтные ситуации, связанные с крупными суммами денег).

В таких условиях, кроме того, возникает самостоятельная научно-прикладная проблема правового выхода из конфликта, решение которой представляется возможным на основе создания соответствующих организационно-технических средств, обеспечивающих юридическую значимость (аутентичность, легитимность и верифицируемость) электронных документов в АСБР [8].

Организационно-технические средства (организационно-методическое и аппаратно-программное обеспечение) реализации концепции с учетом специфики реальной СЭП разработаны сотрудниками ООО “Криптоком” в виде лицензионного продукта “МагПро”, успешно применяемого в АСБР-“Москва” более двух лет [7]. Продукт “МагПро” с незначительной адаптацией возможно использовать в аналогичных СЭП других корпораций и в крупномасштабных автоматизированных системах межбанковских расчетов.

VII Резюме

Реализация рассмотренного теоретико-концептуального подхода (включающего, в частности, выбор и определение видов и качественных форм проявления информации, характерных для эргасистем; рациональное распределение информационных мер в эргасистеме, требования к мерам количества и качества структурной и содержательной информации, принцип информационной ценности, и др.) к проблеме качества