Российский государственный гуманитарный университет
Russian State University for the Humanities

RSUH/RGGU BULLETIN
№ 14 (115)

Academic Journal

Series:
Computer Science. Data Protection. Mathematics

Moscow 2013

ВЕСТНИК РГГУ
№ 14 (115)

Научный журнал

Серия «Информатика. Защита информации.
Математика»

Москва 2013

УДК 94 (560)
ББК 63.3(5)я5

ISSN 1998-6769

СОДЕРЖАНИЕ

Вехи истории

Моделирование

Интеллектуальные системы

Технологии

CONTENTS

Mathematical models

Intelligent systems

Technology

ОТ РЕДАКЦИИ

Предлагаем вашему вниманию очередное издание серии «Информатика. Защита информации. Математика» журнала «Вестник РГГУ», в котором продолжается обсуждение таких актуальных вопросов, как анализ угроз информационной безопасности, проектирование систем защиты, семантические аспекты информатики, функциональная устойчивость информационных систем и др.

В разделе «Тема номера» размещены статьи, посвященные междисциплинарным аспектам информатики. Современный период развития России принято определять как фазу активного формирования информационного общества. Проблема развития информационного общества и обеспечения его безопасности носит междисциплинарный характер и затрагивает одновременно гуманитарные, естественно-научные и технические области. Это определяется возникновением новых угроз, связанных с социоориентированной деятельностью. В информационной сфере в настоящее время все больше говорят о когнитивной метапарадигме. Когнитивная наука междисциплинарна по своей природе, будущее – за исследованиями, которые не ограничиваются только техническими или только гуманитарными методами. В современном мире, при огромной степени влияния информации на все сферы жизни целесообразна консолидация знания различных областей для решения возникающих проблем. Кроме того, отметим междисциплинарность таких вопросов, как управление безопасностью, и в целом обеспечение защищенности информационных систем, которое включает в себя не только информационную безопасность, но и надежность, функциональную безопасность, непрерывность бизнеса.

Приглашаем авторов – преподавателей РГГУ и его филиалов, сотрудников научных центров, представителей большого и малого бизнеса, аспирантов, докторантов – для публикации результатов

научных исследований по современной проблематике информационных технологий и математики.

Материалы для журнала просим оформлять в соответствии с принятыми нормами, установленными ВАК для рецензируемых научных изданий, и направлять их электронной почтой по адресу: vestnik@rggu.ru на имя ответственного редактора серии А.А. Тарасова.

Е.И. Познякова

ОБ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ С WEB-РЕСУРСАМИ НА ОСНОВЕ ФУНКЦИОНАЛЬНОЙ РЕКОНФИГУРАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ*

В статье рассматриваются основные задачи обеспечения безопасности информационно-аналитической системы «Американистика в России, русистика в США». Предложен метод обеспечения информационной безопасности на основе функциональной реконфигурации системы защиты информации (СЗИ).

Ключевые слова: функциональная безопасность, устойчивость, система защиты информации, стратегии деградации, реконфигурация, управление информационной безопасностью.

Основной целью работы любой информационной системы является безотказное выполнение заявленных функций. Для конечного пользователя важен результат, который должен был достоверным, своевременным и полным. С этой точки зрения целесообразно говорить не только об информационной, но и функциональной безопасности (ФБ), которую можно интерпре-

* Статья выполнена в рамках федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007–2013 годы» по государственному контракту № 11.519.11.4021 от 21 октября 2011 г. по теме «Разработка интегрированной информационно-аналитической системы для стимулирования развития международных интеграционных процессов в сфере науки и образования в целях содействия формированию устойчивых кооперационных связей российских и американских научно-исследовательских, образовательных организаций и оценки эффективности российско-американского сотрудничества, в том числе в гуманитарной сфере».

тировать как способность системы предотвращать последствия от деструктивных воздействий, приводящих к недопустимому ущербу или способность минимизации последствий от таких воздействий[1]. ФБ охватывает не только обеспечение доступности и вопросы надежности, но и защиту внешней среды от воздействий самой системы. Подробнее вопрос взаимосвязи функциональной и информационной безопасности, а также непрерывности бизнеса рассматривается в статье[2]. Совместное использование методов и средств надежности, информационной и функциональной безопасности позволяет реализовать комплексный подход к обеспечению безопасности информационной системы.

В рамках настоящего исследования рассматривается модель системы защиты информации (СЗИ), поскольку она обладает рядом особенностей и является одним из самых критичных компонентов любой системы, так как зачастую именно от уровня безопасности зависят вопросы функционирования всей информационной системы.

ФБ и отказоустойчивость любой системы не может быть обеспечена только с помощью технических мер, например путем установки резервных элементов инфраструктуры. Необходим тщательно выстроенный процесс управления информационной и функциональной безопасностью, поскольку только в этом случае возможна эффективная реализация мер защиты и предотвращения ущерба. В таком случае может быть гарантирован контроль на протяжении всего жизненного цикла системы и выполнение всех необходимых функций.

Управление ИБ зачастую сводится к мониторингу сетевой активности и контролю доступа, в то время как сама система защиты остается обособленной и ее отказы не в полной мере учитываются при оценке уровня защищенности. Основной задачей управления информационной и функциональной безопасностью должно стать поддержание работоспособности необходимого набора функций защиты. Уровень защищенности определяется исходя из набора выполняемых функций. Если часть функций не выполняется, например, в результате деструктивного воздействия, то целесообразно говорить о процессе функциональной деградации системы, т. е. о снижении ее функциональных возможностей без увеличения числа полностью отказавших модулей системы.

Однако, поскольку ввиду сложности современных систем невозможно гарантировать абсолютную безотказность, целесообразно рассматривать вопросы функциональной устойчивости с позиций теории надежности, что подразумевает использование

вероятностных характеристик и понятия уровня деградации как некоторого допустимого состояния системы после деструктивных воздействий, при котором происходит ухудшение характеристик самой системы, либо уменьшение количества решаемых задач, либо снижение качества их решения, проявляющиеся в процессе ее функционирования. Будем различать структурную, функциональную и структурно-функциональную деградацию.

Таким образом, одной из задач защиты информации является обеспечение функционирования системы на допустимом уровне.

В современных системах, как правило, даже в случае внедрения универсального средства защиты, используются и специализированные. Различные средства защиты могут реализовывать одинаковые функции защиты, связанные с определенными уязвимостями. Таким образом, эту избыточность СЗИ (в части дублирования функций защиты) целесообразно использовать для функциональной реконфигурации системы, т. е. перераспределения функций между элементами системы с целью поддержания требуемого уровня работоспособности[3]. Возникает задача выбора стратегии резервирования и реконфигурации системы в случае функциональных отказов.

При анализе систем целесообразно выделить типовые сценарии отказов и типовые стратегии реконфигурации, чтобы хотя бы частично автоматизировать процесс принятия решений. В условиях информационного противоборства необходимо обеспечить оперативное реагирование на деструктивное воздействие и своевременно предпринять меры по снижению риска для поддержания требуемого уровня безопасности. Анализ и формализация типовых сценариев позволит администратору безопасности оперативно среагировать на инцидент, а в некоторых случаях автоматически переконфигурировать СЗИ для обеспечения бесперебойной работы.

При организации защиты информации и поддержании работоспособности систем решаются такие традиционные задачи информационной безопасности и надежности, как, например, определение и обоснование требуемого уровня защищенности и надежности систем, определение видов и уровня избыточности, вводимой в систему, выбор (разработка) и реализация методов защиты от несанкционированного доступа, а также методов поддержания работоспособности систем при заданной модели преднамеренных и случайных деструктивных воздействий и т. п.[4] Уровень защищенности является ключевым показателем для анализа допустимости применения выбранной стратегии реконфигурации. Отметим, что для реализации той или иной стратегии реконфигурации необхо-

димо смоделировать возможные типовые сценарии и определить комплекс превентивных мер для модернизации существующей инфраструктуры СЗИ, например мер по внедрению резервных узлов системы и настройки параметров средств защиты.

Следует отметить, что функциональная реконфигурация является эффективным противодействием отказам, приводящим к деградации системы. При перестройке системы проводятся анализ ситуации, определение спектра сохраняемых в системе функций в условиях воздействия неблагоприятных факторов, возможная корректировка состава функций и алгоритмов их реализации. Иными словами, нарушение работы некоторой функции не приведет к деградации всей системы, если возможно применение такой стратегии реконфигурации, при которой выполнение этой функции будет переложено на другой узел системы.

Таким образом, функциональная реконфигурация должна стать важной составляющей процесса обеспечения безопасности, поскольку она является эффективной мерой предотвращения ущерба от возможных отказов СЗИ.

Задача организации процесса управления безопасностью, анализа типовых сценариев функциональных отказов и определения возможности функциональной реконфигурации возникла, в частности, при рассмотрении вопросов безопасности информационно-аналитической системы (ИАС) «Американистика в России, русистика в США» (http://ra-studies.com), созданной совместными усилиями РГГУ и ИВИ РАН[5, 6]. Система включает в себя интернет-портал, который позволяет специалистам искать необходимую информацию для проведения исследований, информировать о новых данных, осуществлять коммуникацию пользователей портала между собой, а также модуль подготовки данных для автоматизации процесса сбора информации. С точки зрения функциональной безопасности и отказоустойчивости можно выделить следующие проблемы:

- необходима достаточно высокая доступность материалов сайта: администратор сайта, расположенного на сервере в России (сервер ИАС находится на базе РГГУ), не может обеспечивать круглосуточную поддержку, в то же время материалы должны быть доступны и в США (разница во времени);
- существует высокая вероятность отказов при поиске информации в сети (необходима блокировка подозрительных сайтов, которую осуществляет модуль подготовки данных);
- необходимо обеспечить кроссплатформенность (возможность размещения на других серверах) и обеспечить при этом необходимый уровень работоспособности системы.

Для организации защищенного взаимодействия с web-ресурсами, прежде всего, следует учитывать вопросы функциональной безопасности, а именно, как обозначено выше, провести анализ влияния отказов системы на внешнюю среду, в том числе на конечного пользователя. Необходимо обеспечить высокий уровень доступности web-ресурсов при условии открытого доступа к ним, т. е. высокой вероятности реализации различных деструктивных воздействий.

В связи с вышеперечисленным систему защиты, как и саму ИАС, необходимо создавать таким образом, чтобы при большинстве возможных отказов обеспечивалось выполнение ключевых функций путем функциональной реконфигурации системы. Например, после некоторого отказа доступ к материалам сайта остается, но дополнительные модули, позволяющие редактировать данные или осуществлять автоматический поиск данных, недоступны.

Иными словами, целесообразно проработать вопросы функциональной реконфигурации как самой ИАС, так и системы ее защиты с целью обеспечения бесперебойной (непрерывной) работы системы практически без участия администратора. Проведение анализа и разработка эффективной системы управления безопасностью ИАС является одним из основных направлений для дальнейших работ, поскольку позволит добиться достаточной автономности и независимости системы от внешних факторов.

В рамках настоящего исследования была разработана методика формирования стратегий функциональной реконфигурации СЗИ, а также проработаны типовые функциональные структуры СЗИ и сценарии сбоев с целью формирования эффективных стратегий деградации с учетом приемлемого уровня защищенности. В дальнейших исследованиях вопросов функциональной реконфигурации СЗИ целесообразно учесть положения теории принятия решений, многозначной логики, адаптации сложных систем[7] и системного анализа.

Примечания

[1] См.: *Шубинский И.Б., Тарасов А.А.* Современная парадигма безопасности критически важных систем информационной инфраструктуры // Безопасность информационных технологий. М.: МИФИ, 2005. № 3. С. 22–31.

[2] См.: *Тарасов А.А., Познякова Е.И.* Функциональная устойчивость критически важных информационных систем как основа непрерывности бизнеса (тезисы доклада) // Материалы V Всероссийской научно-технической школы-семина-

ра «Информационная безопасность – актуальная проблема современности». Краснодар, 2012.

3 См.: *Тарасов А.А.* Стратегии функциональной перестройки отказоустойчивых информационных систем при различных видах деградации // Безопасность информационных технологий. М.: МИФИ, 2012. № 2. С. 22–31.

4 См.: *Тарасов А.А.* Функциональная реконфигурация отказоустойчивых систем. М.: Логос, 2012. 151 с.

5 См.: *Журавлёва В.И.* Американистика в России, русистика в Соединенных Штатах: опыт создания международной Информационно-аналитической системы // История: электронный научно-образовательный журнал. 2012. Вып. 4: История США [Электронный ресурс]. Доступ для зарегистрированных пользователей. – URL: http://mes.igh.ru/magazine/content/amerikanistika-v-rossii.html (дата обращения: 30.04.2013).

6 См.: *Заботкина В.И., Познякова Е.И.* Опыт реализации международного исследовательского проекта «Американистика в России, русистика в США: интегрированная информационно-аналитическая система» // История: электронный научно-образовательный журнал. 2012. Вып. 4: История США [Электронный ресурс]. Доступ для зарегистрированных пользователей. – URL: http://mes.igh.ru/magazine/ content/opit-realizazii.html (дата обращения: 16.11.2012).

7 См.: *Воробьев А.А., Непомнящих А.В.* Адаптивное управление защищенностью информации в автоматизированных системах // Информационные технологии. 2003. № 12. С. 26–30.

А.Е. Аносов

МЕТОДЫ ФИЛЬТРАЦИИ «СТИХИЙНОГО» ТРАФИКА В ДИНАМИЧЕСКИХ ИНТЕРНЕТ-РЕСУРСАХ*

В статье предложен принцип автоматизации систем административного мониторинга, который основан на интеграции модуля анализа и фильтрации трафика в динамическую часть веб-ресурсов. Особое внимание уделяется разработке модуля фильтрации контента в динамической части информационно-аналитической системы «Американистика в России, русистика в США».

Ключевые слова: контентная фильтрация, мониторинг, негативная информация, методы анализа трафика.

Развитие информационного общества порождает все новые угрозы, связанные с обработкой недостоверной, неполной, неточной информации, а также с воздействием негативной информации. Это особенно актуально в связи с широким использованием сети Интернет. Доступность информации расширила возможности поиска, мониторинга, категоризации и систематизации этой информации, но есть и обратная сторона. Все чаще возникают ситуации,

* Статья выполнена в рамках федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007–2013 годы» по государственному контракту № 11.519.11.4021 от 21 октября 2011 г. по теме «Разработка интегрированной информационно-аналитической системы для стимулирования развития международных интеграционных процессов в сфере науки и образования в целях содействия формированию устойчивых кооперационных связей российских и американских научно-исследовательских, образовательных организаций и оценки эффективности российско-американского сотрудничества, в том числе в гуманитарной сфере».

когда на некоторый вид информации необходимо наложить определенные ограничения. Чистота контента в динамической части сайта остается одной из главных проблем любого интернет-ресурса. Этот контент определяет не только уровень ресурса, но и степень доверия к нему поисковых систем, а также государственных служб, работающих в рамках ФЗ № 436 от 2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию» и ФЗ № 139 от 2012 г. «О внесении изменений в Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию”».

Одним из наиболее распространенных путей решения этой проблемы становится постоянный мониторинг пополняемого контента. Как следствие, такой мониторинг не всегда является эффективным, так как круглосуточный контроль трафика может привести к ошибкам, связанным с так называемым человеческим фактором, а также это не всегда экономически выгодно владельцам интернет-ресурсов.

Предложенный в этой статье принцип автоматизации систем административного мониторинга основан на интеграции модуля анализа и фильтрации трафика в динамическую часть веб-ресурсов. Эти модули могут быть реализованы на основе любых существующих методов и алгоритмов анализа контента. Рассмотрим некоторые из них:

- DNS-фильтрация;
- морфологический анализ;
- вероятностно-синтаксический анализ;
- графическая фильтрация.

DNS-фильтрация

Этот метод используется на государственном уровне, в рамках вышеперечисленных федеральных законов. Основным плюсом данного метода является гибкая фильтрация по базе черных и белых списков URL- и IP-адресов, где белый список всегда имеет приоритет над черным. В данном подходе достигается возможность ограничения доступа только к некоторым страницам сайтов. Таким образом, пользователь ограждается лишь от информации «нежелательного характера», которая может располагаться на некоторых страницах крупных порталов и социальных сетей, не блокируя при этом остальные страницы. Также в это решение можно включить дополнительные функции, такие как работа по расписанию, распознавание пользователей по IP-адресам, что даст нам возмож-

ность учета трафика и получения конкретной статистики. Недостаток данного метода заключается в необходимости постоянного обновления списков и категорий, так как ежемесячно появляется огромное число новых сайтов. Еще один минус заключается в том, что ресурс в Интернете легко может сменить имя и адрес, поэтому более сложные и эффективные методы фильтрации основываются на анализе непосредственно самого контента.

Морфологический анализ

Данный метод работает с конкретным контентом на сайте. Он определяет запрещенные слова и блокирует их на основе существующих баз. Недостатком метода является большое количество так называемых омонимичных форм в различных языковых группах, что усложняет принципы фильтрации. Проблема решается включением таких слов, а также словосочетаний с измененной смысловой нагрузкой в метод вероятностно-синтаксического анализа.

Вероятностно-синтаксический анализ

Идея метода базируется на присвоении каждой структурной единице базы слов некоторого значения. Это значение иногда называют «весом», и представлено оно целым числом. Вес каждой структурной единицы, содержащейся в предложении, суммируется. Если общий вес превысит пороговый лимит, заданный в конфигурации метода, то страница будет заблокирована. Таким образом, можно настроить данную ступень на корректный анализ специализированных текстов, относящийся к различным языковым группам.

Графический анализ

На некоторых веб-ресурсах основную смысловую нагрузку несет изображение, поэтому основной акцент системы фильтрации необходимо сосредоточить на анализе этих изображений. Остальные методы будут вспомогательными. Для определения принадлежности изображения к «нежелательному» контенту предлагается нижеприведенный алгоритм. Он состоит из трех основных этапов.

1. Цветовая фильтрация.
2. Анализ объектов, получившихся после цветовой фильтрации.
3. Принятие решения на основе полученных признаков.

Признаками в данном методе являются:

- коэффициент формы объекта;
- отношение координат объекта к соответствующим линейным размерам изображения;
- отношение размеров главных полуосей объекта к размеру изображения по горизонтали;
- угол наклона объекта;
- отношение площади объекта к площади прямоугольника, описанного вокруг всех объектов.

Кроме этого, количество больших объектов тоже считается признаком. Признаком также является наличие или отсутствие лица человека на изображении. При дальнейшем анализе выяснилось, что наилучшей разделяющей способностью имеющейся представительной выборки обладает такой признак, как отношение размера большой полуоси объекта к размеру изображения по горизонтали (k). Сравнение этого значения с порогами (k1, k2), заданными в конфигурационном файле, и является решающим правилом при принятии решения. При значении $k<k1$ – изображение не принадлежит к «нежелательному» контенту, при $k1<k<k2$ – однозначное решение принять невозможно, при $k>k2$ – изображение принадлежит к «нежелательному» контенту.

Внедрение

Основной задачей стала разработка модуля фильтрации контента в динамической части информационно-аналитической системы «Американистика в России, русистика в США» и его интеграция в систему управления порталом. Для автоматизации систем административного мониторинга динамической части ИАС «Американистика в России, русистика в США» необходимо проанализировать структуру и предметную область.

Администрирование проекта, изменение его содержания осуществляется при помощи специально созданной системы управления сайтом. Система управления сайтом базируется на системе управления базами данных «MySQl». В случае программных сбоев предусмотрено изменение портала посредством веб-приложения phpMyAdmin, позволяющего осуществлять удаленное администрирование сервера MySQL. Сервер ИАС находится на базе РГГУ. Однако главным инструментом редактирования портала стала система управления содержимым сайта (CMS).

CMS ИАС «Американистика в России, русистика в США» строилась на следующих принципах:

– дружественность системы редактирования портала основным ОС и офисным программам, что позволяло бы копировать текстовую информацию в ИАС без дополнительной конвертации;
– удобство интерфейса программы редактирования портала, частично повторяющего интерфейс основных офисных программ;
– упрощенная система упорядочивания данных внутри разделов – администратору не требуется формировать алфавитный указатель, он формируется сам при внесении информации, связанной с той или иной буквой;
– простая система удаления или добавления подразделов.

Структура ИАС состоит из нескольких взаимосвязанных модулей:

- хранилище портала;
- модуль редактирования портала;
- модуль подготовки данных;
- форум;
- модули авторизации (для гостей и администраторов).

Портал состоит из открытого и закрытого разделов. Открытый раздел предназначен для всех пользователей Интернета, которые могут осуществлять поиск и отбор информации на портале по заданным критериям.

Закрытый раздел (вход на него осуществляется через пару пароль–логин) позволяет размещать на портале различную информацию, удалять неактуальные данные, изменять дизайн портала, администрировать работу форума, анализировать действие различных модулей и знакомиться с информацией, автоматически обнаруженной модулем подготовки данных в сети Интернет.

В ходе анализа структуры портала была выделена одна открытая динамическая часть – Форум[1]. Форум является составной динамической частью хранилища портала. При помощи специально разработанного интерфейса на форуме администраторами портала и пользователями размещается информация по тематике портала.

Для решения проблем, связанных с возможным распространением пользователями «нежелательного» контента на форуме, необходимо интегрировать один из методов анализа и фильтрации контента[2]. Результат работы системы фильтрации контента зависел от методов, которые она могла бы использовать, ведь информация может быть представлена буквенно-цифровой или графической формой, и каждая форма представления информации имеет свои особенности, которые можно и нужно использовать для осуществления фильтрации.

После проведения статистического анализа на основе полученных результатов было принято решение разработать модуль анализа и фильтрации контента «Управление цензурой», основанного на алгоритмах морфологического анализа. Этот метод определяет запрещенные слова и блокирует их на основе существующих баз.

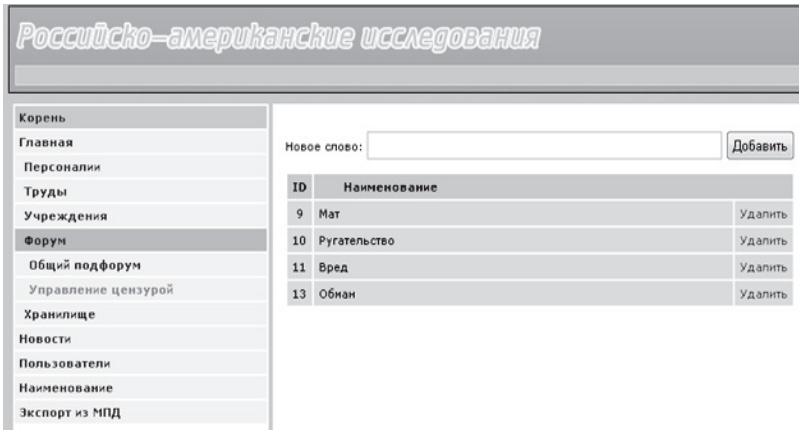


Рис. 1. Интеграция модуля морфологического анализа и фильтрации контента «Управление цензурой» на форуме портала ИАС «Американистика в России, русистика в США»

Подводя итог, можно сказать, что созданный модуль «Управление цензурой», предназначенный для автоматической блокировки «нежелательного» контента, решает поставленные задачи в полном объеме.

В дальнейшей перспективе планируется интегрировать модуль DNS фильтрации ссылок, а также интегрировать модуль графического анализа. Такая модификация позволит на 100% оградить распространение «нежелательного» контента на форуме ИАС «Американистика в России, русистика в США». Кроме того, такой модуль можно позиционировать на рынке как отдельный продукт.

Примечания

[1] См.: *Медведь А.И.* Информационно-аналитическая система «Американистика в России, русистика в США»: система редактирования портала и некоторые пользовательские возможности // История: электронный научно-образовательный журнал. 2012. Вып. 4: История США [Электронный ресурс]. Доступ для зарегистрированных пользователей. – URL: http://mes.igh.ru/magazine/content/informacionno-analiticheskaya-systema.html (дата обращения: 15.11.2012).

[2] См.: *Тарасов А.А., Аносов А.Е., Сорокин А.В.* Подходы к анализу нежелательного контента в открытых информационных сетях // Материалы IV Всероссийской научно-технической школы-семинара «Информационная безопасность – актуальная проблема современности». Краснодар, 2012.

В.И. Заботкина

ИНТЕГРАЦИОННЫЙ ВЫЗОВ В КОГНИТИВНОЙ НАУКЕ: ВОЗМОЖНЫЕ ПУТИ РЕШЕНИЯ

В статье рассмотрены основные понятия когнитивистики, процесс становления когнитивной науки и вклад российских ученых, а также основные проблемы, стоящие перед исследователями. Представлены модели для решения проблемы разработки единого каркаса, который позволит определить взаимоотношения между различными дисциплинами, относящимися к когнитивным наукам.

Ключевые слова: когнитивная наука, интеграция, междисциплинарность, модель порождения знания, когниция.

Современный этап развития общества и науки характеризуется переходом к новой модели порождения знания. Если традиционная модель была узкоспециальной, гомогенной, иерархической и определялась, как правило, академическим сообществом[1], то новая модель – междисциплинарна, генерируется в прикладном контексте и не укладывается в конвенциональные дисциплинарные схемы. Эта модель гетерогенна – она востребует широкий спектр навыков и умений и вовлекает разнообразные формы передачи знаний. По своей сути новая модель знания является мультимодальной (мультимодусной) и вовлекает такие типы знания, как визуальное, аудиальное, синестетическое и т. п. В отличие от традиционной, она имеет гетерархическую структуру, то есть подвержена изменениям и не следует заранее определенной системе организации знания[2].

Вторая модель знания более рефлексивна, расплывчата и социально контекстуализирована. Она показывает, как социальные практики, такие как генерация знания и дискурса, отражаются на социальных акторах – участниках социального взаимодействия.

Когнитивная мегапарадигма, утвердившаяся в научном познании в последние десятилетия, является своеобразным откликом на вызовы времени. Вторая когнитивная революция, основанная на достижениях в области компьютерной техники, когнитивной психологии и лингвистики, заложила основы перехода ко второй модели генерации знания. Одним из основных вызовов XXI в., стоящим перед когнитивной наукой, является интеграция различных областей знания и дисциплин, входящих в данную науку.

Когнитивная наука в самом широком смысле слова – совокупность наук о приобретении, хранении, преобразовании и использовании знания. Более узкую трактовку предложил английский психолог Майкл Айзенк: «междисциплинарное исследование приобретения и применения знаний»[3]. В России когнитивные исследования активно развиваются в нескольких направлениях. Прежде всего, это лингвистика, психология, философия, искусственный интеллект и нейронауки. Немало работ посвящено проблемам управления и процессам принятия решений. Сложность задач, решаемых когнитивистикой, на практике делает подобное деление весьма условным, размывая границы между этими направлениями.

Значительный вклад в развитие когнитивных наук в России внесли такие известные академические журналы, как «Вопросы философии», «Вопросы языкознания», «Психологический журнал», «Вопросы психологии» (издание РАО), «Вопросы психолингвистики», «Вопросы филологии», на страницах которых в разные годы публиковались статьи и рецензии, связанные с когнитивистикой. Последние годы были отмечены появлением новых периодических изданий, полностью посвященных когнитивной отрасли научного знания. Прежде всего, следует упомянуть ежегодник Межрегиональной ассоциации когнитивных исследований «Когнитивные исследования», а также журнал Российской ассоциации лингвистов-когнитологов «Вопросы когнитивной лингвистики»[4].

Итак, когнитивная наука междисциплинарна по своей природе и объединяет несколько дисциплин, объект изучения которых един, это – человеческое сознание, но предмет исследования для каждой из перечисленных выше наук собственный. Когнитивная философия описывает общие онтологические и эпистемологические основы всех когнитивных процессов. Когнитивная психология практически создала весь инструментарий когнитивной науки – такие понятия, как гештальт, фон, фигура, прототип, пришли к нам именно из этой дисциплины. Этими же понятиями пользуется современная когнитивная лингвистика, которая, в свою очередь, становится связующим, системообразующим началом для всех наук когнитивного

цикла, как об этом говорит Е.С. Кубрякова, основатель российской когнитивно-дискурсивной парадигмы. Когнитивная лингвистика связывает воедино и философию, и психологию, и лингвистику, и искусственный интеллект, поскольку язык по-прежнему служит единственным и уникальным инструментом, обеспечивающим нам доступ к сознанию, своего рода «окном» в сознание. Когнитивная лингвистика обогащает философию: привнеся идею образных схем, она позволила философам-когнитологам использовать этот образный компонент в процессе категоризации, концептуализации мира.

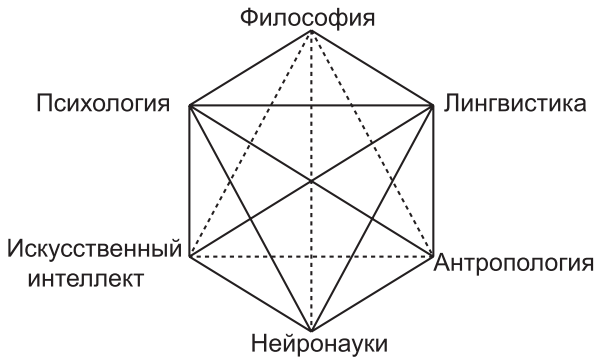
Искусственный интеллект – научное направление, решающее задачи компьютерного моделирования механизмов обработки информации человеком. Содержанием когнитивных исследований в области искусственного интеллекта является имитация и формализация познавательных процедур, реализующих приобретение нового знания. Тесная взаимосвязь, переплетение нескольких составляющих в когнитивной науке и обеспечивает возможность в будущем ответить на главные вопросы о том, как происходит порождение знания, переработка информации, хранение знаний и взаимодействие человека с внешним миром. Одной из главных проблем, стоящих перед учеными-когнитологами, является определение роли гуманитарного знания в науках когнитивного цикла.

В России в настоящий момент все подобные исследования ведутся в нескольких центрах Москвы, Санкт-Петербурга и других регионов. Прежде всего необходимо назвать Курчатовский Центр конвергентных нано-, био-, инфо- и когнитивных наук под руководством М. Ковальчука, в котором ведется разработка когнитивного направления, Институт психологии РАН, Институт мозга человека РАН, Институт языкознания РАН, МГУ им. М.В. Ломоносова, МГЛУ, лабораторию под руководством Т.В. Черниговской Санкт-Петербургского государственного университета, Центр когнитивных программ и технологий РГГУ. Среди региональных центров необходимо отметить прежде всего Тамбовский государственный университет имени Г.Р. Державина, лабораторию когнитивных наук на базе Института информатики Казанского государственного университета, когнитивный центр в Иркутске, центры когнитивных исследований в Калининграде, Екатеринбурге, Пятигорске, Воронеже, Барнауле, Тюмени и других городах.

Основу когнитивным исследованиям в России во многом заложили фундаментальные труды великого русского психолога Льва Выготского[5]. На современном этапе важнейший вклад в развитие когнитивной науки в России вносят такие ученые, как В.А. Лекторский, Д.И. Дубровский (когнитивная психология),

В.Ф. Спиридонов, В.М. Аллахвердов, Д.В. Ушаков, М.А. Холодная (когнитивная психология), В.К. Финн, О.М. Аншаков (искусственный интеллект), Е.С. Кубрякова, Ю.С. Степанов, Н.Д. Арутюнова, В.И. Заботкина, Е.В. Рахилина, Н.Н. Болдырев, В.З. Демьянков, Л.Г. Бабенко, О.В. Александрова (когнитивная лингвистика), Т.В. Черниговская[6], К.В. Анохин (нейронауки).

Интеграционный вызов, стоящий перед когнитивной наукой, которая по своей сути является междисциплинарной (трансдисциплинарной), заключается в необходимости разработки общего каркаса (*framework*), который мог бы объединить все составляющие данной науки на основе общих принципов, общего объекта исследования. Взаимосвязь между этими составляющими может быть представлена в виде восьмиугольника, как на нижеследующей схеме[7].



На схеме представлены: сильные междисциплинарные связи в виде сплошных линий (всего 11 связей) и слабые междисциплинарные связи в виде пунктирных линий (всего 4 связи), объединяющие 6 дисциплин – когнитивную психологию, философию, лингвистику, антропологию, искусственный интеллект и нейронауки. Каждая из этих дисциплин приносит свой инструментарий, рамки и методологию в исследование сознания. Каждая из них изучает сознание с различных точек зрения и на различных уровнях. При всем многообразии связей между элементами восьмиугольника, объединяющим началом всех наук когнитивного цикла является, как указывалось выше, общий объект исследования, то есть сознание (*mind*), изучаемое с точки зрения процесса обработки, хранения и извлечения информации.

Итак, основной вызов, стоящий перед сегодняшней когнитивной наукой, как указывалось выше, заключается в разработке

единого каркаса, который позволит определить взаимоотношения между различными дисциплинами, относящимися к когнитивным наукам, а также выявить различные уровни организации работы сознания, которые изучает когнитивная наука.

Проблема организации сознания занимает умы многих исследователей. Одной из самых распространенных теорий в этой области является теория модулярности. В соответствии с ней определенные формы переработки информации закреплены за отдельными когнитивными модулями в нашем сознании (и далее – за определенной группой нейронов или их пучков-нодов). Некоторые радикальные психологи трактуют сознание как набор специализированных модулей. Современные инструменты исследований, такие как функциональный магнитно-ядерный резонанс, позволяют более полно изучить организацию сознания (мозга). Так, в соответствии с последними исследованиями американского исследователя М. Андерсона[8] нейроны (и их пучки-ноды), отвечающие за языковую деятельность, не концентрируются в одном конкретном участке головного мозга, а разбросаны по различным областям. Один и тот же нод может отвечать за несколько когнитивных функций.

Вернемся к главному теоретическому положению, на котором базируется когнитивная наука. Это положение о том, что сознание (и мозг) – это система переработки информации. Как известно, в процессе становления когнитивной науки большую роль играла лингвистика. Генеративная (трансформационная) лингвистика Н. Хомского[9] и его последователей, основанная на формальном анализе синтаксиса, явила пример того, как с помощью определенных алгоритмов можно анализировать большие объемы информации, лежащие в основе некоторых базовых когнитивных способностей (таких, как понимание и говорение на языке). В конце 50-х годов XX в. идея о том, что работа сознания основана на переработке информации, проникла в психологию. За десятилетие до этого в прикладной математике появилась теория информации. Ученые связывают зарождение новой теории со статьей К. Шеннона «Математическая теория коммуникации»[10]. В своей статье Шеннон показал, как можно измерить информацию. Он предложил точные математические инструменты для изучения передачи информации. Эти инструменты, включающие в себя и единицу измерения информации – бит, оказали влияние на психологию и на когнитивную науку в целом. Так, в статье известного психолога Дж. Миллера «Мистическое число семь плюс или минус два. О некоторых пределах нашей способности перерабатывать информацию»[11] для определения основных параметров

работы нашего сознания (*mind*) используются основные понятия теории информации. Второй фундаментальной публикацией, в которой вводились модели обработки информации в психологии, была монография Д. Броудбента о восприятии и коммуникации[12]. Модель (*flow chart*), предложенная Броудбентом, стала стандартным способом описания различных аспектов когниции. Ранние формы когнитивизма, таким образом, основываются на общем фундаменте, объединившем экспериментальную психологию, теоретическую лингвистику и математическую логику.

Таким образом, главными элементами каркаса, объединяющего все науки когнитивного цикла, были два положения: 1) когниция понимается как форма переработки информации; 2) процесс переработки информации подчиняется определенному алгоритму. На следующем этапе развития когнитивной науки был поставлен вопрос о том, как работают когнитивные системы, распределяющие стоящие перед ними когнитивные задачи. Одним из возможных путей решения данной проблемы является развитие так называемой модели ментальной архитектуры[13]. Такая модель включает две составляющие: 1) определение того, каким образом работа сознания распределяется между различными когнитивными функциями; 2) каким образом происходит обработка информации в каждой отдельной когнитивной системе. В соответствии с этой моделью дисциплины, входящие в когнитивную науку, различаются по трем параметрам:

- по типу изучаемой когнитивной деятельности;
- по уровню организации, на котором изучается этот вид когнитивной деятельности;
- по степени точности методов и инструментов, которые используются в данной науке.

Однако данная модель требует дополнительной разработки и уточнения.

Как указывалось выше, когнитивная наука фокусирует внимание на вопросе о том, как мы описываем систему переработки информации[14]. Одним из подходов к анализу когнитивных систем с точки зрения создания общего объединяющего каркаса может быть методика многоуровневого анализа когнитивных систем, предложенная Д. Марром[15]. Марр выделяет следующие уровни анализа, отличающиеся степенью абстрактности.

1. Вычислительный уровень (анализ определенного типа задания, которое выполняет когнитивная система):

- перевод общего описания когнитивной системы в конкретную задачу по переработке информации, которую необходимо решить;

– идентификация ограничений, связанных с решением данной конкретной задачи по обработке данных.

2. Алгоритмический уровень:
   – объяснение того, как задача по обработке информации может быть выполнена в соответствии с определенным алгоритмом.
3. Уровень внедрения:
   – уровень реального воплощения алгоритма в действие (применение его на практике).

Марр не только различает уровни когнитивной деятельности, но показывает связи между ними (от верхнего к нижнему), поскольку считается, что анализ на вычислительном уровне ограничивает область анализа на алгоритмическом уровне, который, в свою очередь, ограничивает анализ на уровне внедрения. Таким образом, уровни отличаются степенью абстрактности.

Основное возражение относительно трехуровневой гипотезы как глобальной исследовательской модели для когнитивной науки состоит в том, что различие, которое Марр проводил между вычислительным, алгоритмическим и уровнем внедрения, часто принималось за общий принцип всей когнитивной науки. Алгоритмический анализ в большей степени пригоден для исследования четко выделяемых когнитивных систем. Если же это так, то трехуровневая гипотеза применима лишь для небольшого участка всего поля когнитивных исследований.

У представителей когнитивной науки принято четко разграничивать модулярные и немодулярные когнитивные системы. Это, по сути, различие между когнитивными процессами высшего уровня, которые характеризуются вовлечением большого объема поступающей информации не только частного, но и общего характера, и когнитивными процессами низшего уровня, которые характеризуются быстрой обработкой информации для принятия решений по конкретным проблемам. Модулярные системы характеризуются такими параметрами, как:

Ограниченные домены. Это очень конкретные механизмы, которые выполняют определенную работу в определенной области применения.

Информационная инкапсуляция. Выполняя «свою» работу, модулярные системы не подвергаются воздействию других процессов, которые происходят в это время в мозгу. Модулярные системы не могут пройти фильтрацию посредством вовлечения в процесс мышления фоновых знаний или ожиданий.

Модулярная применимость. Модулярные системы автоматически реагируют на стимулы соответствующего вида.

Быстрота. Модулярные системы преобразуют ввод информации (например, структуры, воспринятые рецепторами сетчатки глаза) в вывод (например, трехмерные репрезентации объектов) достаточно быстро, чтобы осуществлять контроль за происходящими процессами.

Фиксированная структура нейронных связей. Часто представляется возможным идентифицировать конкретные области мозга с определенными типами модулярной переработки информации.

Конкретные признаки нарушения деятельности модуля. Нарушение модулярной переработки информации имеет четкие признаки. По характеру сбоев можно получить данные о форме и структуре самой модульной переработки[16].

Таким образом, основная проблема относительно принятия трехуровневой гипотезы Марра в качестве общей методологии когнитивной науки состоит в том, что когнитивные системы, которые больше всего подходят для анализа по Марру, должны носить модулярный характер. Лишь относительно модулярных систем понятно, как ставить вычислительные задачи, чтобы они были достаточно ограниченными и определенными, поскольку должен существовать алгоритм, на основе которого проводится вычисление. Эти ограничительные рамки создают особые проблемы для систем (немодулярного характера), которые не являются информационно инкапсулированными.

В последние годы широкое признание получила гипотеза динамических систем в когнитивной науке в качестве альтернативы традиционным моделям когниции как систем переработки информации. Основные положения этой теории сводятся к следующим:

- динамическая система – это некая система, которая закономерно развивается во времени;
- динамические модели используют вычислительные методы, чтобы проследить развивающиеся отношения между небольшим числом переменных во времени;
- динамические системы часто демонстрируют связь, основанную на взаимозависимости между переменными, и стремление к аттрактору;
- когнитивные системы, смоделированные на основе теории динамических систем, не демонстрируют многие из классических черт систем переработки информации.

Динамические модели не носят репрезентационный, компьютационный, алгоритмический или ограниченный характер[17].

Некоторые сторонники подхода динамических систем высказывают слишком решительные идеи в этом направлении. Ван Гельдер,

например, предположил, что модель динамических систем со временем полностью вытеснит вычислительные модели[18]. Однако подобные утверждения игнорируют одну из наиболее важных характерных черт когнитивной науки. Когнитивная наука – наука междисциплинарная и многоуровневая. Мышление – слишком сложное явление, чтобы его можно было полностью понять посредством одной дисциплины или на одном уровне исследований. Подобное относится к гипотезе динамических систем в не меньшей степени. Возможностей получить полную картину работы сознания/мозга посредством теории динамических систем не больше, чем с помощью полного набора данных, предоставленных нейробиологами или, скажем, представителями искусственного интеллекта. Все эти дисциплины дают нам глубокое, но лишь частичное понимание проблемы. Реальная задача когнитивной науки – интегрировать достижения всех наук в объединенную и полную картину работы сознания.

Данная динамическая теория применима к анализу интеграции наук в рамках когнитивного цикла на нескольких уровнях: 1) локальная интеграция на уровне отдельно взятой области знания (например, когнитивно-дискурсивная парадигма в лингвистике); 2) на уровне кластера наук (например, интеграция между отдельными дисциплинами в рамках наук гуманитарного профиля); 3) на уровне взаимодействия кластеров наук (то есть синтеза гуманитарного и естественно-научного знания).

Примечания

1 См.: *Fox R.* The contribution of linguistics towards transdisciplinary in organizational discourse // International Journal of Transdisciplinary Research. 2009. Vol. 4. № 1.

2 См.: *Nowotny H., Scott P., Gibbons M.* Re-Thinking Science: Knowledge and the Public in the Age of Uncertainity. Cambridge: Polity Press, 2004; *Gibbons M., Limoges C., Nowotny H., Schwartzman S., Scott P., Trow M.* The Dynamics of Science and Research in Contemporary Societes. L.: Sage Publications, 2005; *Polimeni J.M.* Transdiscipli-nary Research: Mowing Forward, Mowing Forward // International Journal of Transdisciplinary Research. 2006. Vol. 1. № 1. P. 1–3; *Pohl C.* From Science to Policy through Transdisciplinary Research // Environmental Science and Policy. 2008. Vol. 2. P. 46–53.

3 См.: The Blackwell Dictionary of Cognitive Psychology / M.W. Eysenck (ed.). L.: Wiley-Blackwell, 1990.

4 Общероссийский академический научный журнал «Вопросы когнитивной лингвистики» был учрежден в 2003 г. Общероссийской общественной орга-

низацией «Российская ассоциация лингвистов-когнитологов» и издается совместно с Институтом языкознания РАН и Тамбовским государственным университетом имени Г.Р. Державина. Главный редактор Н.Н. Болдырев – заслуженный деятель науки РФ, доктор филологических наук, профессор, президент Российской ассоциации лингвистов-когнитологов, проректор по научной работе Тамбовского государственного университета имени Г.Р. Державина.

5 См.: *Выготский Л.С.* Мышление и речь // Выготский Л.С. Собр. соч. Т. 2. М.: Педагогика, 1982.

6 См.: *Черниговская Т.В.* Нейролингвистика // Учебные программы по специализации «Психолингвистика» 021728. СПбГУ, филологический факультет, кафедра общего языкознания. СПб., 2002. С. 44–54; *Она же.* Человеческое в человеке: сознание и нейронная сеть // Проблема сознания в философии и науке. М.: ИФ РАН; Канон, 2008. С. 786–788.

7 Схема заимствована из доклада в фонд Слоана в 1978 г., см.: *Gardner H.* The Mind's New Science: A History of the Cognitive Revolution. N. Y.: Basic Books, 1985.

8 См.: *Goodmon L.B., Anderson M.C.* Semantic integration as a boundary condition on inhibitory processes in episodic retrieval // Journal of Experimental Psychology: Learning, Memory and Cognition. 2011. P. 416–436.

9 См.: *Chomsky N.* Syntactic Structures. Gravenhage: Mouton, 1957.

10 См.: *Shannon C.E.* A mathematical theory of communication // Bell System Technical Journal. 1948. Vol. 27. P. 379–423, 623–656.

11 См.: *Miller G.A.* The Magical Number Seven Plus or Minus Two: Some Limits on Our Capacity for Processing Information // Psychological Review. 1956. Vol. 63. P. 81–97.

12 См.: *Broadbent D.E.* Perception and Communication. L.: Pergamon Press, 1958.

13 *Bermúdez J.L.* Cognitive Science: an introduction to the science of the mind. N. Y.: Cambridge University Press, 2011. P. 492.

14 См.: *Лекторский В.А.* Исследование интеллектуальных процессов в современной когнитивной науке: философские проблемы // Естественный и искусственный интеллект: методологические и социальные проблемы. М., 2011. С. 3–16; *Он же.* Когнитивная наука как вызов эпистемологии // Эпистемология: новые горизонты: Материалы конференции (Москва, 24–25 июня 2010 г.). М., 2011. С. 5–34.

15 См.: *Marr D.* Vision: A Computational Investigation into the Human Representation and Processing of Visual Information. San Francisco: W.H. Freeman, 1982.

16 *Bermúdez J.L.* Op. cit. P. 140.

17 Ibid. P. 453.

18 См.: *Gelder T. van.* The dynamical hypothesis in cognitive science // Behavioral and brain sciences. 1998. Vol. 21. Issue 5. P. 615–628.

Д.В. Кондратьев, А.Н. Ненашев,
С.Т. Петров, А.А. Тарасов

ПРОБЛЕМЫ СОХРАНЕНИЯ ЦИФРОВОГО КУЛЬТУРНОГО НАСЛЕДИЯ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматривается проблематика информационной безопасности в сфере культуры, порождаемая взрывным ростом использования информационных технологий в процессах формирования, хранения и доступа к культурному наследию, определяющим, по сути, направленность «вектора» перехода к цифровому его представлению. С позиций цифрового наследия как сложной системы анализируются основные угрозы нарушения его целостности и доступности, а также вопросы автоматизации управления им. В качестве одной из тенденций в развитии учреждений культуры рассматривается концепция «умного музея», включающего «умные экспонаты», способные к диалогу с посетителем.

Ключевые слова: безопасность культуры, целостность культурного наследия, цифровое наследие, умный музей, одухотворенный аватар.

1. Общие положения

Одним из основных показателей развития цивилизации является целостность и доступность культурного наследия, отражающего преемственность поколений, возможности институтов памяти, свободу получения информации.

Целостность отечественного культурного наследия является одной из основных ценностей, которую в полной мере осознавали наши предки. Так, раскол в Русской православной церкви[1], начавшийся в XVII в., связан с нарушением, с точки зрения староверов, целостности православного наследия, выразившегося в исправлении книг и обрядов. При этом православный обряд, на наш взгляд, можно считать концентрированным выражением, своеобразной

«контрольной суммой» православной веры и изменение данной «контрольной суммы» стало свидетельством поврежденности самой веры. За целостность православного наследия старообрядцы отдали десятки тысяч жизней, умирая за «единый аз». Ими были выработаны особые механизмы обеспечения безопасности, сохранения, а также воспроизводства старой веры и старой культуры, включая методы распознавания «свое–чужое», социально-бытовые и информационные «защитные экраны», конструкции «защитных кодов» и системы материального обеспечения сохранности и трансляции культуры.

Осмысление православной традиции, создание национальных библиотек, появление телеграфа, фотографии, грамзаписи привело к появлению отечественной философии памяти, связанной, прежде всего, с именем Н.Ф. Федорова. Его идеи подразумевали «грандиознейшее предприятие собирания, хранения, изучения всех остатков прошлого, всех малейших отпечатков ушедших людей на их делах, вещах, документах, преданиях, книгах, произведениях искусства и т. п. Речь идет о тотальной консервации памяти, причем в идеале четко индивидуализированной. При этом единственный глубокий смысл собирания мертвых вещей в том, чтобы за ними видеть, по ним воссоздавать их авторов»[2]. Очевидный путь такой консервации – отображение всего многообразия культурного наследия в цифровую форму, т. е. формирование цифрового наследия.

Проблема организации надлежащего управления культурным наследием всегда актуальна, а особенно остро проявляется при смене социальных формаций. Социалистическому перевороту потребовался «полный пересмотр всего наличного культурного наследства, полученного пролетариатом от старых классов, – пересмотр с новой, коллективно-трудовой точки зрения, которая есть вместе с тем научно-организационная; и одновременно с пересмотром – необходимое дополнение этого наследства всюду, где оно недостаточно для новых задач, собственным идеологическим творчеством рабочего класса, научным, художественным, практически-нормативным»[3]. Такой пересмотр потребовал жестких критериев отбора и доступа к произведениям всей мировой и отечественной культуры и привел к нарушению целостности культуры (что выразилось как в уничтожении и массовой миграции культурных ценностей, так и в их конъюнктурном «поновлении») и ограничениям в свободе творчества. Но, с другой стороны, реорганизация культурного наследия дала импульс к созданию мощной системы учета, хранения и доступа к «дозволенным» и «недозволенным» культурным ценностям. Для защиты социалистического

образа жизни и пролетарской культуры использовались все возможности армии и силовых структур, а также в значительной мере модернизированный старообрядческий «защитный экран» в форме «железного занавеса».

Распад СССР, разрушение информационных барьеров, вызванное лавинообразным распространением Интернета, интенсивное формирование информационного общества определили спектр внутренних и внешних угроз отечественному культурному наследию[4], круг проблем обеспечения информационной безопасности в сфере культуры, пути их решения, в том числе и в рамках участия России в программах по сохранению «Памяти мира»[5] и цифровому наследию.

Основным предметом рассмотрения в данной статье является цифровое наследие сферы культуры, представляющее собой совокупность информационных ресурсов, информационной инфраструктуры, информационных технологий, обеспечивающих сохранность и доступ к культурным ценностям, представленным в цифровой форме. Ключевой проблемой представляется формирование цифрового наследия, поддержание его целостности и доступности, а также надлежащего управления им, что осуществляется при помощи комплекса законодательных, организационных и технологических мер из арсенала информационной безопасности, а также ряда инновационных разработок, использующих методы искусственного интеллекта. При этом такие меры требуют реализации на всем жизненном цикле объекта культуры: от замысла до бессрочного хранения самого объекта или его цифрового образа.

2. Проблемы безопасности культуры в информационном обществе

С «легкой руки» отечественного законодателя сфера культуры чрезвычайно широка и включает совокупность присущих обществу или социальной группе отличительных признаков, ценностей, традиций и верований, находящих выражение в образе жизни и искусстве[6]. Не менее широко понимается уже мировым сообществом цифровое наследие, которое охватывает ресурсы в области культуры, образования, науки и управления, а также информацию технического, правового, медицинского и другого характера, созданную в цифровом виде или переведенную в цифровую форму из существующих аналоговых ресурсов[7].

Еще в середине 1990-х годов стал обсуждаться проект создания системы бессрочного хранения информации (автохронной систе-

мы[8]), как распределенной системы, способной обеспечить максимально возможные гарантии неизменности хранимой информации на данном уровне развития цивилизации. Были выделены три группы угроз: антропогенные (прежде всего идеологические, политические, военные), природные (локальные катастрофы, угрозы из космоса), технологические (высокая динамика смены цифровых форматов, носителей, программного обеспечения). При этом начало приходить понимание наследия «как основы жизнеспособности, от которой производны производительность труда населения и конкурентоспособность экономики страны»[9].

Развитие и безопасность культуры России связаны с информационными ресурсами, системами и технологиями. Так, стратегическими целями обеспечения национальной безопасности в сфере культуры является расширение доступа широких слоев населения к лучшим образцам отечественной и зарубежной культуры и искусства путем создания современных территориально распределенных информационных фондов[10]. Проект федерального закона «О культуре в Российской Федерации» предусматривает возможность создания Единой государственной информационной системы в сфере культуры. Данная система будет содержать как компоненты ограниченного доступа (для уполномоченных лиц), так и компоненты общего (массового) доступа[11]. В данном же законопроекте в качестве одной из основных задач ставится необходимость создания условий для сохранения и актуализации исторического и культурного наследия, творческого развития, распространения и популяризации культуры, в том числе на основе новых информационно-коммуникационных технологий.

Достижение весьма высоких контрольных значений показателей развития информационного общества на период до 2015 г., определенных в «Стратегии развития информационного общества в Российской Федерации»[12], и соответствующих показателей государственной программы «Информационное общество (2011–2020 годы)» требуют самых серьезных усилий со стороны десятков тысяч учреждений культуры, федеральных и муниципальных органов исполнительной власти, гражданского общества. Уже созданные и создаваемые в рамках программы «Информационное общество», иных программ и проектов гигантские информационные ресурсы и информационная инфраструктура требуют адекватных мер по обеспечению информационной безопасности.

При этом не следует забывать, что угрозы в области информационной сферы «проецируются» и многократно усиливаются в сфере «цифровизации» культуры. Это порождает проблему обеспечения

информационной безопасности объектов культуры с позиций такого уровня их критичности, когда деструктивные воздействия могут вызывать непоправимый ущерб национальной безопасности, включая безопасность личности, общества и государства.

Решение ее затруднено тем, что «основная причина возможной утраты электронной информации, а часто и реальных потерь состоит в том, что отсутствует осознание проблемы на всех уровнях. Как следствие, не обеспечиваются должная организация процессов сохранения электронной информации на всех этапах ее жизненного цикла и наличие критической массы взаимозаменяемых специалистов, способных реализовать эти процессы»[13].

Среди первоочередных задач, решаемых в области информационной безопасности в сфере культуры, можно выделить следующие:

разработка концептуальных документов в области информационной безопасности культуры и ее нормативно-правовой базы;

обеспечение безопасности цифрового наследия Российской Федерации, включая его целостность и безопасность создаваемой инфраструктуры;

обеспечение доступности цифрового наследия;

обеспечение конфиденциальности информации, связанной с авторским правом;

обеспечение конфиденциальности информации, связанной с безопасностью учреждений культуры и персональными данными, которые они собирают;

научно-методическое и кадровое обеспечение.

Основными ожидаемыми результатами реализации государственной политики в области цифрового наследия в сфере культуры должно стать повышение эффективности деятельности учреждений культуры на основе современных средств раскрытия фондов, обеспечения их виртуальной целостности, унификации программно-технических решений хранения и доступа, а также повышение сохранности фондов на традиционных носителях.

3. Проблемы формирования и защиты цифрового наследия

По одному из немногочисленных определений[14], цифровое наследие характеризуется следующими признаками:

наличием критериев отнесения информации к цифровому наследию;

наличием цифровых оригиналов;

свободным доступом к цифровому наследию;

системой паспортизации, каталогизации и поиска по объектам цифрового наследия;

бессрочным хранением цифрового наследия.

Мировое сообщество осознало важность сохранения цифрового наследия и угрозы, связанные с его утратой. Это нашло отражение в «Хартии по сохранению цифрового наследия», принятой ЮНЕСКО в 2003 г.[15] Развивается система рекомендаций по оцифровке и онлайн-доступу к культурным ценностям и сохранению цифровой информации, в частности, в рамках деятельности Европейской комиссии[16].

К сожалению, понятие «цифровое наследие Российской Федерации» и вопросы обеспечения его безопасности пока не нашли должного отражения как в научно-практических исследованиях, так и в документах федерального и ведомственного уровней. Одной из основных правовых проблем цифрового наследия является то, что цифровые образы объектов, отнесенных к культурному достоянию народов России, сами не являются объектами такого достояния. Поэтому к ним и к обеспечению их безопасности относятся как к чему-то второстепенному, факультативному. Само музейное, библиотечное и архивное сообщество (за редким исключением, см., напр., работы В.И. Тихонова[17]) также пока еще недостаточно готово к обсуждению поставленных проблем, особенно в области информационной безопасности.

Кроме того, процессы оцифровки так или иначе не являются неразрушающими. Например, оцифровка ветхой магнитной ленты, требующая аналогового воспроизведения, может привести к фатальным для ленты последствиям. Кроме того, повальное увлечение «цифрой» ведет к прекращению или даже к невозможности использования хорошо зарекомендовавших себя аналоговых средств. Это осознается, например, научным сообществом, занимающимся репрографией, и немногочисленными профессиональными студиями аналоговой звуковой записи. Не рискуем ли мы получить, в конце концов, «цифру вместо музыки»?

В научно-практическом плане не решен вопрос и «разумной аутентичности» цифровых копий аналоговых оригиналов. Часто за разумный предел принимают, например, способность восприятия человеческим глазом. Но при этом никто не знает ни того, какими через несколько десятков лет будут средства визуализации, ни какими будут возможности наверняка модифицированного человеческого зрения. С другой стороны, уже сейчас мы

вплотную подошли к задаче восприятия предметов искусства компьютером, и где должен находиться «разумный» уровень разрешения и частотного спектра для изображений или частота дискретизации звука, не может ответить никто. А именно эти факторы существенно влияют и на психофизиологию восприятия, и на экономику цифрового наследия.

Объект культуры может являться сложной системой, включающей материальные и нематериальные компоненты, а также связанные с ними культурные сообщества. Такие системы могут включать ландшафты, здания, картины, музейные традиции и коллективы и т. п. Нарушение целостности и доступности такого объекта может быть связано с огромным количеством факторов, например с изменением правового статуса или даже биоразнообразия территории. В свою очередь, цифровое представление таких комплексных объектов культуры, даже в статике, представляет новую и чрезвычайно сложную задачу.

Жизненный цикл объекта культуры включает в себя процессы от замысла отдельного автора до бессрочного хранения самого объекта или его цифрового образа. Конфиденциальность процесса создания важная, а иногда и необходимая составляющая, особенно в индустрии музыки и кино. В общем плане свобода процесса творчества, гарантированная законодательством Российской Федерации, должна подкрепляться и инструментальными средствами защиты информации для, например, производства кинофильмов. Так, утечка информации на стадии замысла или создания может привести к серьезным финансовым потерям киностудии. Таким образом, требуется обеспечение конфиденциальности информации, связанной, в частности, с этапом создания произведения искусства. В действующих Основах законодательства Российской Федерации о культуре это сформулировано как весьма общее право на охрану секретов мастерства.

Проблемы конфиденциальности и доступности традиционного и цифрового наследия часто не совпадают. Так, книга может (должна) находиться в свободном доступе в публичной библиотеке, однако ее электронная верстка или отсканированный вариант являются объектами правовой и информационной защиты.

Уже отмечена «критически важная обязанность – это защита конфиденциальности пользователей при работе с цифровыми материалами. Конфиденциальность пользователей тесно связана со свободой самовыражения и доступом к информации, поскольку недостаточная защита личной неприкосновенности лишает права пользоваться этими свободами»[18].

Целостность культурного наследия пока относится к интуитивным понятиям. Цифровое наследие России плохо систематизировано и разрозненно. Отчасти это объясняется и архаичностью систем государственного учета культурных ценностей. Пока о целостности цифрового наследия приходится говорить только в порядке постановки задачи. Одним из способов решения проблемы целостности цифрового наследия России могло бы стать создание распределенного (резервируемого) катастрофоустойчивого хранилища с единой системой управления. Пока даже отдельные учреждения культуры национального уровня не всегда могут обеспечить целостность своих цифровых собраний. Однако трудности создания единого информационного хранилища связаны в значительной мере с низким уровнем доверия учреждений культуры к любому из возможных операторов данного хранилища. Вместе с тем в настоящее время подавляющее количество информационных ресурсов учреждений культуры хранится в единственном экземпляре в самих объектах культуры и их сохранность, как правило, не регламентируется никакими ведомственными или внутренними документами.

Все угрозы обычному культурному наследию следует считать и угрозами будущему цифровому наследию, поскольку еще не оцифрованные объекты в случае утраты не могут быть оцифрованы, но даже оцифрованный объект почти наверняка будет нуждаться в повторной оцифровке на технологическом оборудовании новых поколений. С другой стороны, оцифровка объекта существенно повышает сохранность и физическую безопасность, поскольку, например, для архивных документов может ограничить круг пользователей оригинала, а для картин уменьшает возможность подмены оригинала копией в силу наличия специальных методик оцифровки.

Проблемы целостности традиционного и цифрового наследия взаимосвязаны. Отдельные части произведений (например, комплекты журналов или даже фрагменты одной книги) могут быть рассредоточены по разным хранилищам, что создает серьезные проблемы для формирования полных и аутентичных цифровых копий. А виртуальная реконструкция утраченных или реформированных объектов культуры является, по сути, единственным способом воссоздания их целостности. Кроме того, говорить в современном мире о целостности и доступности культурного наследия страны, региона или учреждения культуры без наличия полного общедоступного электронного каталога (реестра) фондов практически бессмысленно.

Весьма важно, что само культурное достояние не может быть отчуждено ни в какой форме, оно привязано именно к государству – субъекту права. Часто предметом обсуждения очень жестких дискуссий является даже сама возможность трансграничного перемещения предмета культуры или даже его перемещения внутри одной страны, а иногда даже и одного комплекса зданий. Как только возникает необходимость наличия цифрового оригинала (в настоящее время это, как правило, цифровая копия аналогового оригинала с максимально существующим разрешением), возникают многочисленные организационные и правовые проблемы с его хранением, перемещением, копированием и пр. Поскольку цифровое наследие становится важным активом как учреждений культуры, так и государств (а также транснациональных компаний), вопросы его жизненного цикла становятся весьма важными для всех заинтересованных сторон. При этом «по инерции» все права и вся ответственность за цифровые оригиналы остается за владельцами («операторами») их реальных копий, т. е. учреждениями культуры, которых в нашей стране десятки тысяч. Целостность традиционного культурного наследия поддерживается на ментальном уровне (например, «русская культура»), законодательном (например, «музейный фонд Российской Федерации»), описательно-научном («книжные памятники Российской Федерации»), иногда программно-техническом (каталоги/реестры культурного наследия) и в последнее время на уровне точки доступа (порталы культурного наследия, истории и туризма). Технологически и организационно комплексная безопасность цифрового наследия не поддерживается и не обеспечивается вообще. Цифровое наследие может свободно перемещаться и управляться любыми, в том числе зарубежными, структурами (как управляется, например, архив Коминтерна или книжное наследие старообрядцев). Учитывая, что повторное создание страховых копий, скажем, гектографических старообрядческих изданий, вещь проблематичная, государство теряет управляемость цифровым наследием, включая свободный доступ российских граждан к нему. Конечно, законодатель учитывает и будет учитывать такие моменты, но мы хотим подчеркнуть именно системный характер проблемы управления цифровым наследием, а также необходимость упреждающих мер при управлении этим наследием, например, при возможном размещении в облаках транснациональных компаний.

В подавляющем большинстве, если не во всех российских учреждениях культуры, цифровые копии фондов хранятся на тех же самых площадках, что и оригиналы. Тем самым возрастают риски

одновременной потери того и другого. Отметим, что для страховых копий на микрофишах территориально распределенная система хранения существует. Такое состояние дел характерно не только для России. И такое положение сохраняется в течение уже многих лет после появления Хартии. Как считал Абдельазиз Абид, курировавший программу ЮНЕСКО «Память мира»: «Прежде всего, необходимо разработать самую настоящую стратегию охраны цифрового наследия. ... В каждой стране требуется создать организацию, ответственную за выполнение общегосударственной программы в этой области. Такая мера позволит исключить и случаи дублирования, и риск что-то забыть... Если не позаботиться о сохранности цифровых документов, то для будущих поколений они исчезнут, как в черной дыре космоса. Сохранятся глиняные таблички Шумерского царства, пергаментные свитки, китайская, арабская и европейская бумага... Но XX и XXI века не оставят ничего! Поэтому мы просто обязаны оставить память о нашей эпохе»[19]. До сих пор в мире нет организаций, которые могли бы подготовить рекомендации по стандартам сохранности. Цели и политика в области долгосрочной сохранности и безопасности должны быть разработаны каждой организацией самостоятельно, равно как и каждым институтом памяти, и на национальном уровне[20].

Тем не менее передовые, флагманские учреждения культуры развитых стран не боятся брать на себя инициативы в цифровой сфере, казалось бы, не имеющие прямого отношения к их традиционной деятельности. Так, Библиотека Конгресса США стала учреждением, обеспечивающим хранение архива сообщений Twitter. Сам Twitter начал предоставлять услуги по возможности генерации сообщений после смерти владельца аккаунта (аналог «одухотворенного аватара», см. ниже). Таким образом, государственная библиотека одного государства выступает гарантом целостности огромного массива личных сообщений, накопленных частной компанией, а сама интернет-компания, по сути, расширила и модифицировала все социокультурное поле памяти.

Часто для обеспечения сохранности и доступа необходимо поддерживать и защищать и аппаратно-программную среду существования цифрового наследия. При этом возможности поддержки необходимых версий операционных систем или баз данных выходят далеко за рамки возможностей традиционных учреждений культуры. Более того, даже ведущие учреждения могут не обладать необходимыми вычислительными мощностями, например, по простому открытию «тяжелых» файлов, таких как цифровые копии больших картин, имеющие объем, скажем,

более 500 Гб. В этом смысле для цифрового наследия характерны проблемы «больших данных». Таким образом, цифровое наследие может стать «котом в мешке».

Доступность цифрового наследия зачастую носит формальный характер, ограничиваясь сайтами учреждений культуры, размещающих цифровые изображения низкого качества, накладывающих произвольные ограничения на скорость доступа, количество скачиваний, процедуры выборки информации из баз данных и т. д.

Цифровое наследие подвержено угрозам на всех стадиях его жизненного цикла. Эти угрозы разнообразны и носят как антропогенный, так и естественный характер.

Не претендуя на должную классификацию и полноту возможных угроз цифровому наследию, выделим некоторые из них для различных этапов жизненного цикла.

Угрозы на стадии формирования цифрового наследия как системы связаны в том числе с:

недостаточными темпами формирования цифрового наследия;

неправильно обозначенными приоритетами и ошибочно выбранными объектами культуры для создания цифровых образов;

использованием устаревших или неадекватных методов и технологий для создания цифровых образов;

отсутствием регламентов по созданию цифровых образов объектов данного типа;

недостаточным контролем качества создаваемых цифровых образов;

отсутствием адекватных средств описания и самими метаописаниями;

возможностью нанесения вреда объекту оцифровки;

непроработанностью правовой базы;

возможностью утраты прав на цифровой образ или ограничениями на его использование.

Угрозы на стадии сохранения цифрового наследия связаны в том числе с:

отсутствием адекватных условий хранения;

физическими угрозами инфраструктуре хранения;

отсутствием субъекта, ответственного за сохранность цифрового наследия;

отсутствием адекватных регламентов хранения;

нарушением целостности цифрового наследия;

физическим старением носителей;

недостаточным опытом и возможностями по миграции цифрового наследия;

изменениями в условиях финансирования обеспечения сохранности;

отсутствием необходимых кадров.

Угрозы нарушения доступности цифрового наследия связаны в том числе с:

неправомерными ограничениями в доступе к цифровому наследию;

техническими ограничениями в доступности цифрового наследия;

отсутствием развитых средств навигации и поиска в цифровом наследии;

«зашумленностью» информационного пространства и недостаточными мерами по популяризации цифрового наследия.

Таким образом, в этом далеко не полном и не систематизированном списке мы видим совокупность физических, организационных и технических угроз цифровому наследию, с которыми сталкиваются как отдельные учреждения культуры, так и государство в целом.

Под «обеспечением сохранности цифрового наследия» подразумеваются действия, направленные на обеспечение долгосрочного существования контента и релевантных метаданных архивных документов, в том числе действий, направленных на воздействие на создателей информации задолго до приобретения и отбора документов[21]. При этом стандарты сохранения цифровой информации не разработаны и в большинстве стран не разрабатываются и не применяются. Целенаправленная подготовка специалистов в области сохранения цифровой информации (будущих исследователей и практиков) не ведется, задачи подготовки таких специалистов не сформулированы, методы и учебные программы их подготовки и переподготовки не разработаны и мало где разрабатываются[22]. Стоит отметить, что подобная печальная констатация фактов относится прежде всего к цифровому наследию в сфере культуры. По-видимому, много полезного для решения этих задач можно почерпнуть из опыта силовых структур, аэрокосмической отрасли, а также финансовых организаций. Весьма перспективным явилось бы и сотрудничество с крупнейшими страховщиками для проведения актуарных расчетов, связанных с утерей отдельных сегментов цифрового наследия.

В тех случаях, когда государство не может достаточно эффективно решать проблемы сохранности и доступа к цифровой информации (например, в силу причин, связанных с авторским правом), эти проблемы пытаются решить сообщества частных лиц

и сетевые структуры. Так, русскоязычные трекеры обеспечивают доступ десятков миллионов пользователей к более чем миллиону единиц хранения общим объемом около двух петабайт. Это в разы превышает объемы оцифрованной информации всех российских учреждений культуры, вместе взятых. При этом качество собственных оцифровок и метаописаний, осуществляемых по определенным регламентам, как правило, выше, чем в большинстве государственных учреждений культуры, а сохранность и доступность обеспечивается самой организацией пиринговой сети. Внешняя нестабильность, «зыбкость» статей Википедии компенсируется ее инфраструктурой и программным обеспечением, позволяющими хранить все редакции всех статей этой всемирной энциклопедии, обеспечивая жизненный цикл новой формы мирового знания, вовлекая в его формирование и использование сотни миллионов людей. Тем самым при формировании цифрового наследия следует учитывать интересы и возможности гражданского общества, в том числе и в вопросах информационной безопасности.

4. «Умный музей»: некоторые перспективы

Ни отдельные учреждения культуры, ни отдельные государства, ни транснациональные компании, ни граждане, ни мировое сообщество в целом не могут справиться с вызовами, связанными с цифровым наследием. Это касается всех этапов – от формирования до освоения цифрового наследия и связано как с ограниченностью возможностей человека как представителя биологического вида (сенсорные, ментальные и физиологические ограничения), так и с социальной природой нынешнего человека (непредсказуемость, конфликтность, деструктивность). На наш взгляд, именно «человеческий фактор» является слабым звеном, сдерживающим формирование, освоение и обеспечение безопасности цифрового наследия. На этом выводе можно было бы поставить точку и встать в позицию ожидания, когда проблема решится сама собой по мере социального, технического и институционального прогресса человеческого общества. Однако в повестке дня вырисовывается потенциальная возможность для разноформатного (на уровне отдельного или корпоративного объекта) движения вперед, а именно: проектирование и создание «умного музея», в котором интегрированы возможности современных информационных технологий, позволяющие посетителям вступать в заинтересованный, интерактивный контакт с «умными экспонатами».

Концепция и подходы к построению «умного музея» изложены в статьях Д.В. Кондратьева, А.Н. Ненашева, С.Т. Петрова[23]. Согласно высказанным в них идеям, в виртуальном пространстве мы получаем не только внешнюю сторону музея в виде выстроенной по определенному замыслу системы доступных для зрителей информационно подкрепленных «артефактов», но и внутреннюю, содержащую все необходимые приложения для обеспечения жизненного цикла учреждения культуры. «Умный музей» с данной точки зрения представляет собой масштабируемую аппаратно-программную модель защищенного информационного пространства в единстве функциональных элементов музея, хранящихся в нем предметов, посетителей, сотрудников музея, интерактивных банков информации, включающих искусствоведческие и профессиональные знания, компетенции в сферах музейной экономики, безопасности, учета, хранения, функционирования технических систем, персональных данных, информационных каталогов и архивов, авторских, смежных прав, нормативных документов и правил. Естественно, «умный музей» – это единая социотехническая система, состоящая из совокупности внутренне непротиворечивых подсистем, содержащих постоянные и переменные компоненты.

Один из важнейших элементов «умного музея» – «умный экспонат», оснащенный датчиками и средствами технического взаимодействия для решения задач мониторинга условий хранения, перемещения, безопасности, документирования действий с экспонатом, а также интерактивного диалога и взаимодействия с посетителями. Причем такой экспонат «умнеет» по-разному в зависимости от степени его материальности.

Освоение и популяризация цифрового наследия также начинает постепенно переходить к «одухотворенным аватарам»[24]. В сохранении и распространении культурного наследия заинтересованы прежде всего сами авторы как по соображениям общественного признания, так и по сугубо материальным мотивам. Никого не удивляет, что значительная часть биржевых операций осуществляется роботами. Вполне логично доверить им и управление отдельными сегментами цифрового наследия. Так, аватар живого или умершего автора вполне может отслеживать активность издателей и пользователей, связанных с его творчеством, управляя своими имущественными и неимущественными правами. В свою очередь, сам аватар становится важным элементом цифрового наследия.

Информационные технологии расширяют традиционное музейное поле в пространстве и времени. Так, например, с помощью аудиогида CitySurf, созданного на базе глобальных навигацион-

ных систем, объекты города – здания, памятники, места – превращаются в экспонаты, а весь город – в музей под открытым небом[25]. Дальнейший шаг – использование транспорта (например, железнодорожного) как «коммуникатора культуры». Имеющиеся в современных поездах средства отображения, информирования и позиционирования уже сейчас могут эффективно использоваться для передачи сведений об объектах культуры по маршруту следования. Причем не только в данный момент времени, но и в исторической динамике[26]. Таким образом, на транспортном средстве может быть интегрирован в один огромный виртуальный музей «разновременной культурный срез» как отдельного города, так и всей страны в целом, связанный с маршрутом следования железнодорожного состава.

Заключение

Информационная безопасность сферы культуры в современных условиях является проблемой, подходы к решению которой заложены в понимании таких феноменов XXI в., как глобализация, универсальность учения о ноосфере, информационное общество, цифровое наследие сферы культуры, институты информационной безопасности, доступность и самоценность сферы культуры, автоматизация процессов, защищенность человеческой личности, транснационализация источников права.

Рассмотреть эти проблемы невозможно в рамках одной статьи. Однако необходимо нащупать системные решения, без которых невозможно обеспечить представление в традиционной и цифровой форме отечественного культурного наследия для граждан нашей страны и его зарубежных почитателей. В качестве реального результата следует рассматривать также повышение степени защищенности, сохранности, доступности и притягательности для посетителей наших учреждений культуры в условиях формирующегося мирового информационного пространства и конкуренции.

В данном контексте представляется весьма своевременным концентрация интеллектуальных ресурсов страны на информационной составляющей безопасности российской культуры, всесторонняя и высокопрофессиональная подготовка будущих исследователей и практиков в области сохранения цифровой информации и продвижения наших культурных ценностей.

Примечания

[1] См.: *Зеньковский С.А.* Русское старообрядчество: В 2 т. М., 2009. 688 с.

[2] См.: *Семенова С.Г.* Философ будущего века: Николай Федоров. М., 2004. 584 с.

[3] См.: *Богданов А.А.* Вопросы социализма: Работы разных лет / Под ред. Л.И. Абалкина (отв. ред.). М.: Политиздат, 1990. С. 330.

[4] См.: *Стрельцов А.А.* Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. М.: МЦНМО, 2002. 286 с.

[5] См.: Память мира. Память России: Сб. инструкт. и метод. материалов // Науч. ред. И.В. Морозова. М., 1999. 145 с. О современном взгляде и состоянии в данной области см. также в Ванкуверской декларации «The Memory of the World in the Digital Age: Digitization and Preservation» [Электронный ресурс] // Официальный сайт ЮНЕСКО. URL: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/unesco_ubc_vancouver_declaration_en.pdf (дата обращения: 07.05.2013).

[6] См.: Проект федерального закона «О культуре в Российской Федерации» [Электронный ресурс] // Сайт «Российской газеты». URL: http://www.rg.ru/2011/10/26/kultura-site-dok.html (дата обращения: 07.05.2013).

[7] См.: Хартия ЮНЕСКО о сохранении цифрового наследия [Электронный ресурс] // Сайт МОО «Информация для всех». URL: http://www.ifap.ru/ofdocs/digit.htm (дата обращения: 07.05.2013).

[8] См.: *Петров С.Т.* Автохронные информационные системы. Народный цифровой архив // Информационное общество. 1999. № 2. С. 58–60.

[9] См.: *Генисаретский О.И.* Между выживанием и развитием: возрастные состояния, мотивации и аффекты // Культурологический альманах «Архэ». Вып. 5. Антропополитика. Томск, 2004.

[10] См.: Стратегия национальной безопасности Российской Федерации до 2020 года [Электронный ресурс] // Сайт Совета Безопасности РФ. URL: http://www.scrf.gov.ru/documents/1/99.html (дата обращения: 07.05.2013).

[11] См.: Проект федерального закона «О культуре в Российской Федерации».

[12] См.: Стратегия развития информационного общества в Российской Федерации [Электронный ресурс] // Сайт Совета Безопасности РФ. URL: http://www.scrf.gov.ru/documents/6/90.html (дата обращения: 07.05.2013).

[13] См.: *Куйбышев Л.А.* Музеи и сохранение цифрового наследия [Электронный ресурс] // Центр по проблемам информатизации сферы культуры. URL: http://www.minervaplus.ru/publish/Museums-preservation-heritage.doc (дата обращения: 07.05.2013).

[14] См.: *Петров С.Т.* Мир цифрового наследия // Цифровое наследие. 2009. № 1. С. 17.

[15] См.: Хартия ЮНЕСКО о сохранении цифрового наследия.

[16] См.: Рекомендации Европейской комиссии по оцифровке и онлайн-доступу к культурным ценностям и сохранению цифровой информации [Электронный ресурс] // Официальный сайт Европейской комиссии. URL: http://ec.europa.eu/information_society/activities/digital_libraries/doc/recommendation/recom28nov_all_versions/en.pdf (дата обращения: 07.05.2013).

[17] См.: *Тихонов В.И.* Информационные технологии и электронные документы в контексте архивного хранения. Статьи разных лет. М., 2009. 384 с.

[18] См.: Сохранение электронной информации в информационном обществе: проблемы и перспективы: Сб. мат-лов Международной конференции (Москва, 3–5 октября 2011 г.). М., 2012. 345 с.

[19] См.: *Абид А.* Документальное наследие в век информатики // Курьер ЮНЕСКО. 2007. № 5. С. 4.

[20] См.: *Вилкс А.* Доступ к цифровому контенту: стратегии, возможности и угрозы // Сохранение электронной информации в информационном обществе: проблемы и перспективы. С. 137.

[21] См.: Сохранение электронной информации в информационном обществе: проблемы и перспективы.

[22] См.: *Кузьмин Е.И.* Сохранение информации: прошлое, настоящее, будущее // Сохранение электронной информации в информационном обществе: проблемы и перспективы. С. 41.

[23] См.: Музей (научно-практический журнал). 2013. № 5 [Тема номера: Музей и технологии будущего].

[24] См.: *Расторгуев С.П., Литвиненко М.В.* Аватаризация. СПб., 2011. 310 с.

[25] См.: *Крячков С.М.* GPS/GLONASS аудиогид CitySurf – интерпретация городской среды как музейного пространства [Электронный ресурс] // Сайт международной конференции «EVA 2012 Москва: Информационное общество, культура, образование». URL: https://eva.rsl.ru/ru/2012/report/list/1088 (дата обращения: 07.05.2013).

[26] См. проект GOOGLE по доступу к картографической информации, позволяющей видеть изменения ландшафта за десятки лет: A picture of Earth through time [Электронный ресурс] // Google Maps. URL: http://google-latlong.blogspot.co.uk/2013/05/a-picture-of-earth-through-time.html (дата обращения: 07.05.2013).

Л.В. Морозова, М.Ю. Паждин

ДУХОВНО-ИНТЕЛЛЕКТУАЛЬНОЕ РАЗВИТИЕ ЛИЧНОСТИ КАК ОСНОВА ПРОТИВОДЕЙСТВИЯ ДЕСТРУКТИВНОМУ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОМУ ВОЗДЕЙСТВИЮ В УСЛОВИЯХ ВЕДЕНИЯ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

В статье приведена попытка отобразить основы информационного противоборства на плоскость учения православной церкви и противопоставить деструктивным информационно-психологическим воздействиям духовно-интеллектуальное развитие личности.

Ключевые слова: информационное противоборство, государство, личность, православие, духовно-интеллектуальное развитие.

В соответствии с определением государства[1] основу пирамиды государства составляет общество, которое состоит из множества отдельных индивидуумов – личностей. Путем целенаправленного воздействия на личность можно добиться как положительных, так и отрицательных результатов в отношении того общества, к которому принадлежит личность, что, в свою очередь, может сказаться на вышестоящем уровне иерархии – государстве в целом. Таким образом, одной из главных и важных целей при ведении комплексного информационного противоборства является человек – его личность, самосознание.

Под термином «информационное противоборство» будем понимать явные и скрытые целенаправленные воздействия систем друг на друга с целью получения определенного выигрыша[2].

Основу информационного противоборства в части воздействия на личность составляют информационно-психологические операции. Конец XX – начало XXI в. характеризуются развитием медийных и интернет-технологий, переходом от постиндустриального к информационному обществу[3]. Совокупность этих факторов в

настоящее время позволяет достигать в достаточно короткие сроки при ведении информационного противоборства гигантских масштабов последствий: от снижения темпов развития и разрушения государств до достижения суперэффектов в процессах мирового (глобального) управления.

Обозначенные в Доктрине информационной безопасности Российской Федерации[4] вопросы обеспечения безопасности духовного и интеллектуального развития личности как основы сильного государства и выделение в одно из основных направлений научных исследований в области информационной безопасности направления по обеспечению безопасности личности, общества и государства от деструктивных информационных воздействий[5] во втором десятилетии XXI в. для Российской Федерации являются весьма актуальными.

Переход общества от постиндустриального к информационному все более и более остро ставит перед государством и каждым человеком вопросы обеспечения информационно-психологической безопасности как личности, так и государства в целом. Психология и организация информационного общества является очень благоприятной средой для проведения специальных информационно-психологических операций, цели которых могут быть очень разнообразными. Психология личности человека информационного общества более уязвима и лучше «программируема». Результаты исследований пользователей глобальной сети и особенно социальных сетей показывают, что до 90% это активная молодежь от 18 до 24 лет[6], которая является наиболее уязвимой к деструктивным воздействиям и более «удобонастраиваемой» для подобных целей.

Находясь в «глобальной паутине», человек думает, что он более свободен и независим в выборе источника информации, может проверить любую информацию и выбрать для себя более «доверенный» и «достоверный». Начинает действовать принцип комплексности в получении и проверке информации. Однако в принципе комплексности и кроется одна из ошибок личности в оценке достоверности информации. За горизонтом восприятия человека остается то, что организаторами операции каждый раз планомерно сокращаются число альтернатив для получения информации и ее проверки. Целью операции как раз и является лишение личности возможности реального выбора, делание человека более предсказуемым. Применением организаторами информационной операции метода «сужения» и «расширения» горизонта информационного поля достигается эффект разрушения целостности картины восприятия информации личностью. Проследить и выявить настоя-

щего «хозяина» информации обычному человеку при этом в сети достаточно сложно.

В особую группу деструктивных воздействий в начале XXI в. необходимо выделить и широко используемый индустрией рекламы нейромаркетинг, который строится на передовых достижениях в области сетевых интернет-технологий и психологии личности[7,8]. Применение достижений этого направления в целях деструктивного воздействия на человека в условиях информационного противоборства достаточно опасно, однако в настоящее время активное изучение и противодействие данным приемам со стороны государства не наблюдается, что может повлечь за собой огромную опасность в будущем.

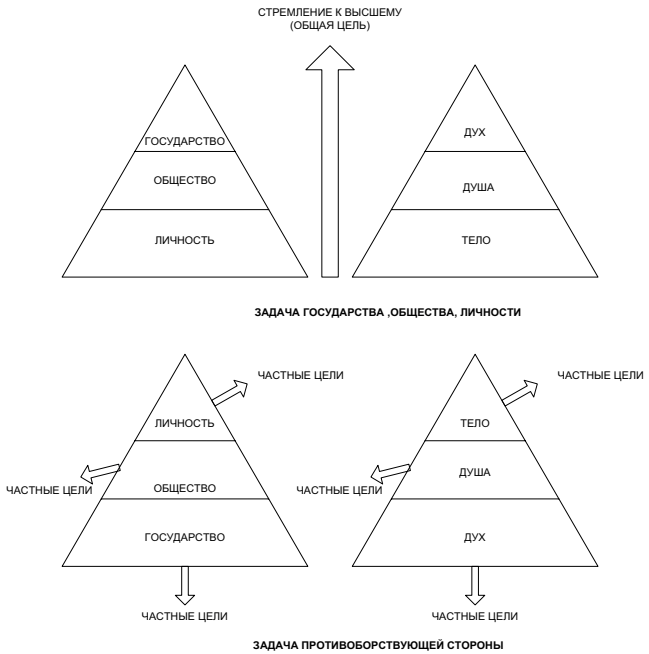
Так каким образом личности и государству в целом можно активно противостоять различного рода деструктивным информационным воздействиям? Одними организационно-техническими мерами и средствами, в первую очередь со стороны государства, полноценного эффекта добиться невозможно, необходима вторая составляющая – развитая духовная основа человека, способная на основе внутренних убеждений и знаний противостоять внешним деструктивным воздействиям.

Если отобразить основы информационного противоборства на плоскость учения православной церкви, то мы увидим, что цели противостояния «добра» и «зла» за всю историю человечества не изменились. В нашем контексте под «злом» необходимо понимать деструктивное воздействие на человека, под «добром» – противодействие личности деструктивному воздействию. Если цель «зла» – переориентация внимания личности к какому-либо предмету, информации, воззрению и т. п. (в православии – переориентация от Бога, отпадение от жизни в Боге) для осуществления деструктивного замысла, то задача «добра» – удержание внимания на главном, на истине (в православии – постоянное устремление к Богу, жизнь в Боге).

Методы, используемые в информационном противоборстве, очень схожи с учением об этапах развития греха в человеке[9]. Если отобразить суть пяти этапов развития греха (прилог, сочетание, сложение, пленение, страсть) на методы, используемые при проведении информационного противоборства, то мы увидим явную параллель (захват внимания, «информационная блокада», «информационная интервенция», принятие мнения как своего личного, «рефлексивное управление»).

Таким образом, одной из целей информационного противоборства со стороны «зла» является дезориентация и обеспечение

разнонаправленности устремлений, составляющих пирамиду государственности: личности, общества и государства (искажение и дезориентация системы ценностей). Противоположной задачей является обеспечение однонаправленности устремлений всех составляющих к высшей цели. Если пирамиду государственности сравнить с учением святых отцов православной церкви о трехсоставности человека, то проиллюстрировать все вышесказанное можно следующим рисунком.



В связи с вышесказанным основу комплексного противодействия деструктивным воздействиям в условиях информационного противоборства со стороны государства и личности должно составлять духовно-интеллектуальное развитие личности на всем протяжении жизни человека. Противостояние государства нарастающим деструктивным информационно-психологическим воздействиям, направленным на разрушение духовно-нравственных основ личности и, как следствие, подрыв устойчивости и развития государства,

особенно в условиях развития возможностей глобальной сети Интернет и перехода человечества к информационному обществу, ставит много вопросов и угроз перед всем человечеством.

Примечания

[1] См.: Малый энциклопедический словарь Брокгауза и Ефрона. СПб.: Издательское общество «Ф.А. Брокгауз – И.А. Ефрон», 1907–1909.

[2] См.: *Расторгуев С.П.* Информационная война. М.: Радио и связь, 1999. 416 с.

[3] См.: *Алиева Н.З., Ивушкина Е.Б., Лантратов О.И.* Становление информационного общества и философия образования. М.: Изд-во «Академия Естествознания», 2008. 168 с.

[4] См.: Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895) [Электронный ресурс] // Сайт Российской газеты. URL: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm html (дата обращения: 30.04.2013).

[5] См.: Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации (утверждена Исполняющим обязанности Секретаря Совета Безопасности Российской Федерации, председателя научного совета при Совете Безопасности Российской Федерации 7 марта 2008 г.) [Электронный ресурс] // Сайт Совета Безопасности РФ. URL: http://www.scrf.gov.ru/documents/94.html (дата обращения: 30.04.2013).

[6] См.: Результаты исследования, направленного на изучение контингента пользователей различных социальных сетей 05.02.2013 [Электронный ресурс] // Сайт исследовательского холдинга Ромир. URL: http://www.romir.ru/studies/431_1360008000/ (дата обращения: 30.04.2013).

[7] См.: *Фингелькурц Ан.А., Фингелькурц Ал.А.* Нейрофизиологические основы принятия решений и выбора – перспективы для нейромаркетинга [Электронный ресурс] // Сайт компании «Вселенная мозга». URL: http://www.neuro-marketing.ru/section_13.html (дата обращения: 30.04.2013).

[8] См.: *Акулич М.В.* Нейромаркетинг и... [Электронный ресурс] // Сайт «Энциклопедия маркетинга». URL: http://www.marketing.spb.ru/lib-around/science/neuro_&.htm (дата обращения: 30.04.2013).

[9] См.: *Лествичник Иоанн, преподобный.* Лествица. М.: Сибирская Благозвонница, 2009. 575 с.

О.В. Казарин, А.А. Тарасов

СОВРЕМЕННЫЕ КОНЦЕПЦИИ КИБЕРБЕЗОПАСНОСТИ ВЕДУЩИХ ЗАРУБЕЖНЫХ ГОСУДАРСТВ

Динамичное формирование глобального информационного пространства связано, с одной стороны, с предоставлением человечеству невиданных ранее информационных возможностей, а с другой – с возникновением новых угроз. Возник новый феномен – «кибербезопасность», с которым связаны такие понятия, как «киберпреступность», «кибертерроризм», «кибервойны». Организация безопасного функционирования национальных информационных инфраструктур будет, скорее всего, определяться соответствующими концепциями кибербезопасности, разработанными практически всеми развитыми странами мира и крупными международными организациями. Анализ концепций ведущих зарубежных государств – предмет настоящей статьи.

Ключевые слова: глобальное информационное пространство, информационно-коммуникационные технологии, информационное противоборство, кибербезопасность.

Глобальное информационное пространство (ГИП) можно представить как совокупность взаимосвязанных информационных инфраструктур различного уровня (межнациональных, национальных, региональных и иных). Основа ГИП – сеть Интернет. Формирование ГИП породило такие угрозы, как киберпреступность, кибертерроризм, угрозы военно-политического характера, которые проявляются в использовании информационно-коммуникационных технологий (ИКТ) для достижения политических, экономических, военных целей посредством враждебного использования этих технологий, а также такие угрозы, как[1]:

неправомерное использование информационных ресурсов другого государства без согласования с государством, в информационном пространстве которого располагаются эти ресурсы;

действия в информационном пространстве с целью подрыва политической, экономической и социальной систем другого государства, психологическая обработка населения, дестабилизирующая общество;

манипулирование информационными потоками в информационном пространстве других государств, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества, эрозия традиционных культурных, нравственных, этических и эстетических ценностей;

информационная экспансия, приобретение контроля над национальными информационными ресурсами другого государства.

Реализация данных угроз, так или иначе связанных с кибервойнами и проведением специальных операций в информационном пространстве, может привести к нарушению мира и безопасности, к подрыву доверия в международных отношениях, а также к отрицательному воздействию на целостность государственных инфраструктур и нанесению недопустимого ущерба. Это определяет необходимость соответствующего противодействия. Основой для формирования стратегического вектора в организации такого противодействия призваны стать существующие и разрабатываемые концептуальные документы в области кибербезопасности.

Концепция кибернетической мощи государства (США)

Кибернетическая мощь государства (кибермощь, cyberpower) рассматривается в США сегодня как его способность использовать киберпространство в своих интересах для создания в нем преимуществ и возможность влиять на ситуацию в других операционных средах (военной, военно-политической, экономической, информационной)[2]. Кибернетическая мощь государства в военно-политической сфере определяется в доктринальных документах США как применение стратегических и оперативно-тактических планов и концепций, которые, в свою очередь, используют инструменты киберпространства для достижения военно-политических целей и выполнения военных миссий.

Использование кибернетической мощи государства рассматривается сегодня американцами в связке с адекватным и взвешенным

(по их мнению) использованием мягкой и жесткой силы и рассматривается в шести основных фазах.

Фаза 0. Формирование стратегических и оперативно-тактических целей.

Фаза 1. Сдерживание агрессии.

Фаза 2. Захват инициативы и обеспечение свободы собственных действий.

Фаза 3. Осуществление стратегических и оперативно-тактических операций и достижение полного превосходства.

Фаза 4. Переход к операциям по установлению стабильности, безопасности и верховенства закона.

Фаза 5. Участие в восстановлении экономики и передаче управления гражданским властям.

Концепция кибернетической мощи государства предполагает, что основой будущих военных стратегических операций (американцами рассматриваются сроки 2012–2025 гг.)[3] будет реализация следующих трех видов специфических действий:

установление, расширение и обеспечение досягаемости потенциального противника, как виртуальной – через киберпространство, так и физической – обычными средствами;

приобретение, совершенствование и объединение знаний о киберпространстве;

идентификация, создание и эффективное использование различных свойств киберпространства.

В целом США считают наличие кибернетической мощи фундаментальным явлением современной жизни[4]. В политической, экономической и военной сферах ИКТ должны обеспечивать и поддерживать деятельность ключевых элементов американской инфраструктуры, в том числе и в области национальной безопасности. Считается также, что Соединенные Штаты должны создать эффективную национальную и международную стратегическую основу для развития и использования своей кибернетической мощи в качестве полномасштабного направления реализации стратегии национальной безопасности. Такая стратегическая основа будет иметь структурные и геополитические составляющие. Структурная составляющая сосредоточит свое внимание на укреплении безопасности и человеческом капитале, улучшении управления и более эффективной организации деятельности. Геополитическая составляющая сосредоточится на более традиционной сфере обеспечения национальной безопасности и обороноспособности США. Сюда включается:

- развитие концепции сетецентрических операций[5];
- интегрированное планирование компьютерных сетевых атак;

- расширение эффективных способов влияния на состояние и характеристики киберпространства;
- грамотное сочетание планирования деятельности в киберпространстве с планированием деятельности обычных вооруженных сил и учреждением при этом соответствующей доктрины;
- образование и обучение в области информационных технологий и информационной безопасности;
- международная деятельность в этих областях.

Особое место в концепции кибернетической мощи государства отводится ИКТ, которые сегодня могут значительно увеличить вероятность успеха в операциях по обеспечению устойчивости, безопасности, перехода к мирной жизни и восстановлению (операции SSTR), которые в настоящее время американские стратеги выделяют чуть ли не как основную часть любой военной миссии или кампании. В Концепции выделяется пять основных составляющих эффективного использования ИКТ: гарантированное (американским правительством) совместное использование ИКТ гражданского и военного назначения при проведении операций SSTR; обязательное использование военных ИКТ при планировании и проведении операций SSTR; предварительное планирование и установление партнерства в области ИКТ с другими регулярными участниками операций SSTR; сосредоточение внимания на стране, где проводятся операции SSTR; использование ключевых возможностей ИКТ для поддержки основной стратегии действий.

Концепция создания кибернетических войск (США)

В настоящее время в США активно прорабатывается вопрос о создании кибервойск. В Министерстве обороны США как наиболее мощной организации в области кибербезопасности уже существуют следующие подразделения, ведущие операции (как оборонительные, так и наступательные) в киберпространстве:

- сетевое командование (отвечает за безопасность домена .mil);
- подразделения ВМС США по проведению операций в компьютерных сетях;
- Cyber Task Force в структуре ВВС США;
- командование C4 (Command, Control, Communications and Computer) корпуса морской пехоты.

Создается киберкомандование как орган, координирующий деятельность всех подразделений, ответственных за вопросы ки-

бербезопасности в структуре Министерства обороны, а также осуществляющий оперативное взаимодействие с другими ведомствами (вне министерства обороны). При этом речь не идет о создании кибервойск как отдельного вида вооруженных сил.

Серьезными проблемами при разработке стратегии действий кибервойск являются:

- проблемы идентификации в сети источника нападения;
- проблемы законодательного разделения актов киберпреступлений, кибершпионажа и военного кибернападения;
- проблемы оценки эффективности и достаточности финансовых затрат при обеспечении кибербезопасности и, как следствие этого, проблемы бюджетного планирования.

Специалисты Министерства обороны США отмечают, что государственные ведомства сталкиваются ровно с теми же проблемами в области кибербезопасности, что и бизнес-структуры (при этом имеет место формула «одинаковая атака – разные последствия»). Как следствие этого, остро встает вопрос о привлечении кадров высшей квалификации (на фоне мирового уровня) для работы в области кибербезопасности в интересах государственных ведомств. Для этого разрабатывается отдельная федеральная программа, призванная решить для США вопросы кадрового обеспечения кибервойск.

При разработке стратегии ведения кибервойн специалисты США категорически отвергают использование принципа «сдерживания», сработавшего в период ракетно-ядерного противостояния времен «холодной войны». Основная причина этого в том, что в киберпространстве отсутствует абсолютная уверенность в надежном подавлении противника и использование принципа «сдерживания» может привести к опасным иллюзиям у политиков. Национальная стратегия кибербезопасности США скорее всего будет строиться на принципах «управления рисками», т. е. баланса потенциальных угроз и затрат по их нейтрализации.

В основу идеи создания кибервойск закладывается одна из составляющих концепции кибернетической мощи государства – концепция военной кибермощи (Military CyberPower)[6]. При этом военная кибермощь рассматривается как одно из состояний киберпространства применительно к выполнению военных миссий и кампаний, включая гуманитарную помощь, ликвидацию последствий (операции HA/DR), обеспечение устойчивости, безопасности, перехода к мирной жизни и восстановлению (операции SSTR), а также как собственно военная борьба, включающая военное управление, управление персоналом, военно-медицинское и материально-техническое обеспечение.

Особое значение в концепции военной мощи придается обеспечению вооруженных сил современными ИКТ и ИТКС, сбалансированному использованию мягкой (в основном с использованием элементов киберпространства) и жесткой силы при выполнении военных миссий, связи с партнерами по коалициям. Также большое значение придается эффективному управлению рисками при проведении военных операций, так как все более и более увеличивается зависимость военной инфраструктуры от «гражданских элементов» киберпространства, от их возможностей, ИКТ-продуктов и служб.

Одна из основных составляющих военной кибермощи – это операционная среда, включающая информационные операции (операции IO), операции влияния (в основном – операции с использованием «мягкой силы»), сетецентрические операции (операции NCO), разведывательные операции и операции, связанные с коммерческим и административным использованием киберпространства.

Кроме того, концепция военной кибермощи рассматривает идею интеграции сетей Министерства обороны США через объединение существующих методов, сетевых услуг и сервисов с целью создания глобальной информационной решетки (Global Information Grid, GIG) – как общей сетевой основы для реализации сетецентрических операций в киберпространстве. Такая сетевая решетка создается в рамках программы формирования объединенной корпоративной региональной системы обмена информацией (Combine Enterprise Regional Information Exchange System, CENTRIXS).

Концепция также рассматривает различные военные сценарии, заключающиеся в возможности ведения различных информационных операций, войн, в том числе сетецентрических, асимметричных и иррегулярных.

Стратегия Министерства обороны США по ведению операций в киберпространстве

В июле 2011 г. Президентом США Б. Обамой была подписана Стратегия Министерства обороны США по ведению операций в киберпространстве[7], призванная стать всеобъемлющей стратегией США по обеспечению превосходства в киберпространстве. Документ дает право США проводить все виды военных операций в киберпространстве для нанесения «поражения и разубеждения» противника, а также предотвращения угроз национальным интересам США.

Несмотря на изменения в последнее время по многим позициям, в том числе в вопросах признания военно-политических угроз в киберпространстве, новая Стратегия Министерства обороны США по ведению операций в киберпространстве предусматривает не только оборонительные, но и наступательные кибердействия в час «Х». Один из основных разделов этого документа посвящен стратегии и тактике наступательной кибервойны и вопросам практического взлома компьютерных сетей противника.

В данной Стратегии в том числе говорится, что киберпространство рассматривается в качестве одного из основных оперативных направлений ключевой организационной концепции Министерства обороны США по обеспечению государственной безопасности. Это позволяет министерству «...в расчете на проведение операций в киберпространстве вести деятельность по организации, подготовке и оснащению таким же образом, как это делается в отношении воздушных, сухопутных, морских и космических военных сил, в целях обеспечения интересов государственной безопасности».

В то же время в Стратегии говорится, что в МО США планируют изучить подходы по коренному изменению правил поведения в киберпространстве с целью усиления оборонного потенциала и повышения уровня устойчивости в случае злонамеренных действий. МО планирует следовать по пути реализации революционных технологий, которые ведут к переосмыслению непосредственно технологических основ киберпространства.

Международная стратегия США для киберпространства

Президент Соединенных Штатов Америки Б. Обама в июне 2011 г. подписал Международную стратегию для киберпространства[8]. Новый документ представляет огромный интерес для понимания современной глобальной американской политики. В опубликованной Стратегии наблюдается значительный пересмотр официальных позиций Соединенных Штатов по вопросам информационной безопасности. Новая Стратегия представляет собой результат двадцатилетней истории формирования системы государственного обеспечения информационной безопасности в США.

В Стратегии декларируется, что США готовы использовать «все необходимые средства» для защиты своих жизненно важных киберобъектов, что США будут «отвечать на враждебные действия

в киберпространстве, как и на любую другую угрозу», в том числе сохраняют за собой право отвечать военными действиями.

В целом в ключевых стратегических документах администрации Б. Обамы неоднократно говорилось о том, что формирующаяся система международных отношений носит полицентричный характер. Особую роль в новом мире играют так называемые негосударственные акторы. В силу особенностей такого специфического ресурса, как информация, государство имеет крайне ограниченные возможности управления и контроля в этой области. Однако негосударственные акторы – транснациональные корпорации, международные организации, общественные объединения, сетевые структуры – нередко обладают гораздо более мощными информационными ресурсами, чем государства. В полицентричном мире Соединенным Штатам придется конкурировать, а возможно, и противостоять различным акторам международных отношений.

Сразу бросается в глаза, что, в отличие от многочисленных «национальных стратегий», документ называется «Международная стратегия для киберпространства». Очевидно, этим администрация стремится подчеркнуть ключевое изменение в американской политике в области обеспечения информационной безопасности – упор на международное сотрудничество.

С выходом новой Стратегии кибербезопасности можно говорить о новом этапе формирования системы государственного обеспечения информационной безопасности в США. В опубликованном документе говорится о стратегическом подходе к вопросам кибербезопасности. Среди потенциальных угроз в этой сфере отмечаются как экономические, так и военные и техногенные угрозы экономике, бизнесу, обществу и национальной безопасности.

Отдельный параграф новой Стратегии посвящен проблеме информационного сдерживания. В подписанной Стратегии говорится о том, что в ответ на кибератаки США готовы использовать любые средства – дипломатические, экономические и военные. Сам факт появления дискуссий об информационном сдерживании свидетельствует о том, что Соединенные Штаты отказались от претензий на доминирование в ГИП, но в то же время стремятся не уступать своих позиций.

Таким образом, опубликованная Стратегия подтверждает стремление Соединенных Штатов адаптироваться к полицентричной системе международных отношений. В новом формирующемся мире США видят себя как центр силы, обладающий мощным информационным потенциалом. В случае применения Стратегии развития этого потенциала, направленной на дальнейшее укрепле-

ние государственно-частного партнерства, Соединенные Штаты будут обладать весьма мощным ресурсом «мягкой силы».

Стратегические документы в области кибербезопасности европейских стран

Анализируя стратегические документы в области кибербезопасности европейских стран, можно сделать следующие выводы.

В среде, где постоянно появляются и эволюционируют киберугрозы, страны – члены Евросоюза при встрече с новыми, глобальными угрозами намереваются получить большую выгоду от гибких, оперативных стратегий кибербезопасности. Трансграничный характер угроз вынуждает страны вступать в тесное международное взаимодействие. Сотрудничество на панъевропейском уровне необходимо не только для эффективной подготовки к кибератакам, но и для своевременной реакции на них. Комплексная государственная стратегия кибербезопасности – первый шаг на этом пути, считают в европейских странах.

В указанных выше документах чаще всего встречаются следующие рекомендации по решению основных вопросов в области кибербезопасности на краткосрочную и среднесрочную перспективу[9].

В краткосрочной перспективе:

спроектировать, переоценить и поддерживать государственную стратегию кибербезопасности, а также мероприятия, проводимые в рамках стратегии;

четко определить рамки действия, цели стратегии и само толкование термина «кибербезопасность»;

убедиться, что предложения и заявления министерств и других государственных органов приняты во внимание и рассматриваются;

учесть в стратегии интересы промышленности, научного сообщества и гражданских представителей;

признать, что непрекращающееся развитие киберпространства и кибербезопасности отразится в постоянном редактировании и пересмотре стратегий;

осознать, что предыдущий пункт подразумевает появление не только новых угроз и рисков, но и новых возможностей улучшения информационных систем для правительства, промышленности и общества;

убедиться, что в стратегии принимается во внимание уже проделанная работа по повышению уровня безопасности национальных и панъевропейских информационных систем. Необхо-

димо избегать дублирования мероприятий и сфокусироваться на новых проблемах;

сотрудничать с другими странами, входящими в Евросоюз, а также с комиссией Евросоюза, чтобы гарантировать согласованный характер кибербезопасности;

поддержать комиссию Евросоюза в деле создания Стратегии безопасности Интернета.

В среднесрочной перспективе:

договориться об общепринятом толковании термина «кибербезопасность» для того, чтобы в дальнейшем сформулировать общие цели для всего Евросоюза;

убедиться, что стратегии кибербезопасности Евросоюза и его членов не противоречат целям международного сообщества, а поддерживают борьбу с проблемами кибербезопасности на глобальном уровне;

для реализации стратегий кибербезопасности частный и государственный секторы должны работать в тесном сотрудничестве. Сотрудничество должно осуществляться посредством обмена информацией, передовыми практиками (например, в сфере управления инцидентами), а также учениями на государственном и панъевропейском уровнях.

Для содействия комиссии Евросоюза в миссии по созданию стратегии кибербезопасности Евросоюза Европейское агентство по сетевой и информационной безопасности (ENISA) разрабатывает специальное руководство (Good Practices Guide). В руководстве будут содержаться передовые практики и рекомендации по проектированию, внедрению и поддержке государственной стратегии кибербезопасности. Руководство должно стать полезным инструментом и практическим советом для людей, ответственных или вовлеченных в проектирование стратегии. Руководство разрабатывается в содействии с частными и государственными заинтересованными сторонами по всей Европе.

Доктринальные установки и стратегические документы в области кибербезопасности других стран (Китай, Индия, Канада, Австралия, Новая Зеландия, Япония, Израиль)

Взгляды Китая на информационное противоборство формируются преимущественно под влиянием американских концепций информационных операций. Однако в отличие от стремящихся к

глобальному доминированию США, китайская концепция носит оборонительный характер и ее главной задачей является противодействие предполагаемой военной угрозе со стороны Соединенных Штатов.

В зависимости от масштаба, характера решаемых задач, используемых сил и средств в Китае различают два вида информационного противоборства[10]:

в широком смысле – ведущееся на государственном уровне во всех сферах, скрытно или явно как в мирное, так и в военное время, предполагающее установление контроля над информационным пространством стран, представляющих угрозу национальным интересам КНР, а также в целях обеспечения собственной информационной безопасности;

в узком смысле – осуществляющееся непосредственно в ходе войн и вооруженных конфликтов и ограниченное пространственными рамками театров военных действий.

По мнению специалистов Генерального штаба Национально-освободительной армии Китая, в качестве основных мероприятий по информационному противоборству в том числе следует считать:

информационное воздействие, включающее управляемое информационное воздействие (распространение или доведение до противоборствующей стороны ложной или искаженной информации);

программно-аппаратное воздействие путем применения информационного оружия на высокотехнологичные системы поражения и автоматизированные системы управления войсками, развертываемые на базе сетевой телекоммуникационной инфраструктуры;

защиту от информационного воздействия противника;

разведывательно-аналитическое обеспечение, заключающееся в выявлении важнейших объектов информационной инфраструктуры противника, оценке их доступности, определении основных способов и продолжительности воздействия на них; оценке и прогнозировании угроз информационной безопасности; анализе результатов проведенных мероприятий информационного противоборства и в предоставлении командованию необходимых данных для принятия решений.

По мнению китайского руководства, в сфере развития ИКТ страна пока отстает от наиболее развитых в военном и экономическом отношении стран, что говорит о ее неготовности в настоящее время к ведению информационной войны и достижению информационного превосходства. В связи с этим предполагается ускорить комплексное развитие всех компонентов информационного

противоборства, прежде всего в военной области. Это касается, в частности, развития информационной инфраструктуры и технологий военного назначения, а также специальной подготовки личного состава.

Признавая свое существенное отставание от ведущих стран Запада в области создания командно-управляющих систем на базе современных ИКТ, КНР делает в настоящее время ставку на формирование возможностей для проведения нестандартных информационных атак и других асимметричных действий.

Позиция Индии изложена в проекте Государственной политики кибербезопасности «Безопасность компьютерных сред и высокий уровень надежности электронных транзакций»[11]. Суверенитет киберпространства Индии должен обеспечиваться путем его киберзащиты. «Киберзащита[12] связана с защитными действиями против активности, которая, главным образом, исходит от враждебных субъектов, имеющих политическую, квазиполитическую или экономическую мотивацию, и влияет на государственную безопасность, общественную безопасность и экономическое процветание общества».

В этом документе отмечается необходимость «защиты данных на этапе их обработки, хранения и передачи, а также защиты конфиденциальной личной информации с целью создания атмосферы доверия. Организации должны следить за тем, чтобы важные данные и записи были защищены от утраты, уничтожения или фальсификации в соответствии с законодательными, регуляторными, контрактными и бизнес-требованиями. Если для воздействия на человека или организацию требуются юридические усилия (как гражданского, так и уголовного характера), необходимо надлежащим образом собирать, сохранять и представлять электронные доказательства, соблюдая правила, действующие в соответствующей юрисдикции».

Опубликованная в 2010 г. Стратегия кибербезопасности Канады зиждется на трех основных принципах:

защита правительственных систем;

сотрудничество с целью защиты ключевых информационных и телекоммуникационных систем, находящихся вне ведения федерального правительства;

обеспечение безопасности канадских граждан в онлайн-среде.

Первый принцип подразумевает установление четких ролей и ответственности, усиление безопасности информационных и телекоммуникационных систем федерального уровня и повышение информированности правительства в области кибербезопасности.

Второй устанавливает ряд партнерских проектов государственного уровня с привлечением частного сектора и секторов критических инфраструктур. И наконец, третий – это борьба с киберпреступностью и защита канадских граждан в онлайн-среде. Здесь также затрагивается проблема защиты персональных данных.

В Стратегии кибербезопасности Австралии признается существование растущего спектра государственных и негосударственных акторов, совершающих противоправные действия в информационном пространстве. При этом указывается, что грани между этими акторами становятся все более размытыми. Угроза, по мнению австралийцев, исходит от киберпреступников, террористов и разведок недружественных государств. Аналогичные угрозы позиционируются и в Стратегии кибербезопасности Новой Зеландии.

Стратегию кибербезопасности Японии можно разбить на несколько ключевых областей действия:

усиление политик, направленных на борьбу с возможными массовыми кибератаками, и учреждение органа, ответственного за предотвращение атак;

введение политик, легко адаптирующихся к изменениям в сфере информационной безопасности;

предпочтение активных политик информационной безопасности пассивным.

Основные мероприятия, описанные в стратегии Японии, включают в себя:

управление IT-рисками для обеспечения безопасной жизни общества;

внедрение политики, которая усилит государственную безопасность, улучшит управление кризисами в киберпространстве и не будет противоречить политике использования информационно-коммуникационных систем, которая служит основой для социоэкономической деятельности;

введение трехвекторной политики, комплексно затрагивающей проблемы национальной безопасности, управление кризисами и защиту общества/личности. В особенности важна политика информационной безопасности общества/личности;

введение политики информационной безопасности, которая не противоречила бы стратегии экономического роста;

участие и развитие международных альянсов.

Руководство Израиля в условиях военно-политического противостояния с арабским миром уделяет вопросам организации информационного противоборства повышенное внимание[13]. В Израиле задачи по планированию и реализации мероприятий

по нарушению функционирования объектов информационной и телекоммуникационной инфраструктуры зарубежных государств возложены на разведывательное управление и управление связи и компьютерных систем генерального штаба национальных вооруженных сил.

В связи с возрастанием количества кибератак со стороны исламских экстремистов в ГИП Тель-Авив в июне 2010 г. принял решение о создании подразделения, специализирующегося на противоборстве кибертерроризму и проведении специальных операций в ГИП, а также в информационных сетях правительственных, силовых, финансовых и других структур потенциального противника. Его формирование осуществляется в составе специального подразделения радиоэлектронной разведки разведывательного управления генерального штаба.

Основными лицами, уполномоченными осуществлять деятельность в области планирования и реализации мероприятий по использованию ИКТ для нарушения функционирования объектов информационной и телекоммуникационной инфраструктуры зарубежных государств, являются премьер-министр, министр обороны, начальник генерального штаба ВС и начальник разведывательного управления генерального штаба ВС Израиля. Для защиты национального киберпространства в Израиле при Министерстве финансов создано и успешно функционирует специальное подразделение Tehila, на которое возложены следующие задачи:

обеспечение защищенного обмена данными через Интернет между государственными ведомствами;

создание безопасных программно-аппаратных платформ для веб-сайтов и ресурсов правительственных организаций;

пресечение распространения через Интернет противоправной информации; координация усилий заинтересованных ведомств по противодействию кибератакам.

Оперативное отражение нападения на национальные компьютерные сети, если алгоритм компьютерной атаки известен, в Tehila обеспечивает дежурная группа. В случае выявления нестандартной схемы действий противника к работе подключается группа экспертов, которая проводит всесторонний анализ ситуации и вырабатывает инструкции для дежурного персонала.

В начале 2010 г. Тель-Авивом принята концепция, допускающая кибератаки на серверы и электронные адреса, через которые предпринимаются попытки разрушения информационного пространства, компьютерных систем и электронных баз данных Израиля. В связи с этим группа Tehila наделена дополнительными

полномочиями проводить наступательные акции на зарубежные компьютерные системы.

Израильтяне считают, что отсутствие международных правовых механизмов, ограничивающих использование программно-аппаратных средств для поражения компьютерных систем, позволяет применять их без согласования с международными организациями и иностранными государствами.

Заключение

В последнее десятилетие ГИП все больше превращается в арену межгосударственного соперничества, борьбы за достижение стратегических и тактических политических целей. В 2011 г. опубликованы стратегии кибербезопасности ряда крупнейших держав мира (США, Великобритании, ФРГ и др.), в которых провозглашается курс этих стран на строительство кибервооруженных сил. Американские военные доктринально закрепили за киберпространством статус пятого театра военных действий (наряду с сушей, водой, воздухом и космосом). Большинство европейских стран, особенно входящих в блок НАТО, также разработали свои стратегии кибербезопасности, хотя, по большому счету, они являются некоторым переложением доктринальных документов своих «старших» партнеров.

Свой стратегический взгляд на решение проблем кибербезопасности имеют Китай, Индия, Израиль, ряд международных организаций (НАТО, ОБСЕ и др.).

Вместе с тем в большинстве национальных стратегий кибербезопасности, блоковых доктринах стран западного мира слабо отражается обеспокоенность международного сообщества в вопросах недопущения очередного витка гонки вооружений на качественно новом уровне развития ИКТ, снижения опасности угрозы агрессивного использования этих технологий для силового разрешения межгосударственных противоречий, а также угрозы безнаказанного совершения с использованием данных технологий преступных деяний в ГИП.

Поэтому сегодня главный вопрос, стоящий перед мировым сообществом, состоит в следующем: «Как сохранить весь позитивный потенциал ГИП и вместе с тем нейтрализовать негативные и деструктивные тенденции его использования?»

Одним из первоочередных шагов на пути к его решению должна стать разработка и принятие на уровне Организации Объ-

единенных Наций документа, закрепляющего фундаментальные принципы деятельности в ГИП и обеспечения безопасности этой деятельности.

Примечания

1 См.: Конвенция об обеспечении международной информационной безопасности (концепция). Международная встреча высоких представителей, курирующих вопросы безопасности, Екатеринбург, сентябрь 2011 года [Электронный ресурс] // Сайт центра политических исследований России. URL: http://www.pircenter.org/kosdata/page_doc/p2728_1.pdf (дата обращения: 07.05.2013).

2 См.: Cyberpower and national security / Ed. by F.D. Kramer, S.H. Starr, L.K. Wentz. Washington, D.C.: National Defense University Press; Potomac Books, 2009.

3 Ibid.

4 Ibid.

5 Концепция сетецентрических операций (сетецентрической обработки данных) связана с манипуляцией и обменом сложными данными, которые происходят в масштабах все более крупных и сложных неоднородных сетей, спонтанно расширяющихся в неконтролируемом пространстве Интернета. Эта концептуальная схема вытекает, прежде всего, из повышенных требований к живучести информационных систем, характеризующихся высокой степенью распределенности ресурсов (сервисами, программным и аппаратным обеспечением, телекоммуникациями) и практически полным отсутствием централизованного управления.

6 См.: Military perspectives on cyberpower / Ed. by L.K. Wentz, Ch.L. Darry, S.H. Starr. Washington, D.C.: Center for Technology and National Security Policy at National Defense University, 2009.

7 См.: Department of Defense Strategy for Operating in Cyberspace. Washington, D.C.: U.S. Department of Defense, 2011.

8 См.: Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington, D.C.: The White House, 2011.

9 См.: Государственные стратегии кибербезопасности года [Электронный ресурс] // Сайт SecurityLab by Positive Technologies. URL: http://www.securitylab.ru/analytics/429498.php (дата обращения: 07.05.2013).

10 См.: *Димлевич Н.Р.* Информационные войны в киберпространстве – Китай и Индия [Электронный ресурс] // Международная жизнь. 2011. 3 февраля. URL: http://interaffairs.ru/read.php?item=614 (дата обращения: 07.05.2013).

11 Discussion draft on National Cyber Security Policy [Электронный ресурс] // Government of India. Department of Electronics and Information Technology. URL: http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf (дата обращения: 07.05.2013).

[12] При этом разделяются понятия «кибербезопасность» и «киберзащита». Кибербезопасность, по индийскому документу, – это деятельность по защите информации и информационных систем (сетей, компьютеров, баз данных, центров обработки данных и приложений) с применением соответствующих процедурных и технологических мер безопасности. В этом смысле понятие кибербезопасности является довольно широким и охватывает все виды защитной деятельности. Под киберзащитой понимается более узкий вид деятельности, связанный с конкретными аспектами и организациями.

[13] См.: *Димлевич Н.Р.* Информационные войны в киберпространстве – Великобритания и Израиль [Электронный ресурс] // Фонд стратегической культуры. URL: http://www.fondsk.ru/news/2010/11/08/informacionnye-vojny-v-kiberprostranstve-velikobritanija-i-izrail-873.html (дата обращения: 07.05.2013).

В.Р. Григорьев, А.А. Новиков

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ – СТРАТЕГИЧЕСКИЙ РЕСУРС ВЕДЕНИЯ СЕТЕЦЕНТРИЧЕСКИХ ВОЙН

Создание глобальной сетевой информационной инфраструктуры привело к глубоким изменениям во взглядах политического и военного истеблишмента Запада на ведение войны в информационную эпоху. Соответствующая тенденции всеобщей сетевизации социальных ресурсов, коммуникаций и услуг концепция получила название сетецентрической войны. Появление и взаимопроникновение технологий облачных вычислений и Web 2.0 стимулировало особый интерес военно-промышленных кругов к рассмотрению их в качестве новой операционной среды для проведения будущих сетецентрических операций и боевых действий в глобальном виртуальном пространстве. По прогнозам специалистов, эти технологии и связанные с ними глобальные трансформационные процессы будут коренным образом влиять практически на все сферы цивилизационных инфраструктур общества: промышленность, образование и государственную деятельность примерно так же, как в свое время повлияли промышленная и информационная революции.

Ключевые слова: облака, облачные вычисления, виртуализация, федеральная стратегия в области облачных вычислений, сетецентрические войны.

Введение

Сегодня Россия вынуждена реализовывать свои национальные интересы в новых международных и даже цивилизационных условиях. Мир стремительно глобализируется, повсеместно складывается постиндустриальное общество, основанное на информации, эрозии подвергаются многие государственные институты, а в области безопасности появляются «новые», не-

традиционные и асимметричные угрозы (террористические сети, «цветные» революции, манипуляции общественным мнением). Ведущие западные страны во главе с США, первыми переступив порог информационной эпохи, осуществляют структурную перестройку всех сегментов своего общества, начиная с бизнеса и науки и заканчивая вооруженными силами и системой обеспечения национальной безопасности, чему строго соответствует появление новых технологий социально-политического менеджмента. Возникают постиндустриальные теории политического устройства, экономики, культуры, коллективной и индивидуальной психологии, военной стратегии, которые, будучи применены в глобальной информационной среде, дают их разработчикам неоспоримые преимущества перед оппонентами, действующими исходя из установок предыдущей фазы исторического развития.

Новые военно-политические сентенции концептуально оформлены в виде стратегии так называемой сетецентрической войны (СЦВ)[1,2] и осуществляются на практике в рамках реализации геополитической концепции окружения Евразии «кольцами анаконды».

Будущей операционной средой для ведения вооруженными силами США сетецентрических войн, по мнению военно-политического руководства, должны стать облачные вычисления, Web 2.0 и Интернет. Эти технологии подвержены быстрым изменениям и, возможно, окажут уже в ближайшее время серьезное влияние на трансформацию общества, в том числе и на качественное преобразование военной инфраструктуры, а также на мировоззрение военных. В соответствии с принятыми в последние годы нормативными документами и директивами по стратегии ведения сетецентрических операций и развитию облачных вычислений киберпространственный домен (Интернет) в качестве военной «распределенной сетевой базы» становится все более предпочтительной средой для согласованных синхронизированных действий всех элементов государственной власти, а вооруженные силы Соединенных Штатов, как ключевая составляющая этой власти, готовятся монопольно оперировать этим доменом[3,4]. Ключевой вопрос о возможности реализации стратегического военно-политического доминирования США в глобальном информпространстве состоит в том, насколько эффективно будут действовать в реальных «полевых» условиях новые сетецентрические концепции (далее в этой статье – сетецентрические войны 2.0). В зависимости от того, как быстро Россия найдет адекватный ответ на новые стратегические вызовы, будет зависеть существование ее военно-политического паритета с США и с блоком НАТО в целом.

Сетецентрические войны – стратегия мирового доминирования

Термин «сетецентризм» впервые появился в компьютерной индустрии и стал результатом прорыва в информационных технологиях, которые позволили организовать взаимодействие между компьютерами, даже несмотря на использование в них разных операционных систем. Идеи открытых систем способствовали развитию сетецентрических технологий для обеспечения распределенных вычислений на существующей информационной инфраструктуре – был пройден путь от простого удаленного вызова процедур до сложных архитектурных решений, а венцом творения в данной области стала сервисная архитектура (Service-Oriented Architecture, SOA). В приложении к военному делу сетецентризм – более широкое и насыщенное понятие, которое, по сути, определяет парадигму XXI в. и становится неотъемлемым элементом происходящей революции в военном деле (РВД). В приложении к геополитике наиболее актуальной становится главная задача вскрытия и противодействия механизму западных подрывных политических технологий, направленных на создание управляемых конфликтов в информационную эпоху.

В XXI в. главным инструментарием достижения новых боевых возможностей, то есть повышения степени реализуемости боевого потенциала, стали современные информационные технологии. И сейчас действительно можно говорить о фундаментальном сдвиге от «платформоцентрической» к «сетецентрической войне», которая, по утверждению ее разработчиков, не только определяет новые принципы управления войсками и силами, но и способствует осуществлению революции в военном деле на современном этапе.

Ключевым понятием для всей теории СЦВ является термин «сеть». В современном американском языке помимо существительного «the network» – «сеть» – появился неологизм – глагол «to network», что приблизительно переводится как «охватить сетью», «внедрить сеть в», «подключить к сети». Смысл «сети», «сетевого принципа» состоит в том, что главным элементом всей модели является «обмен информацией» – максимальное расширение форм производства этой информации, доступа к ней, ее распределения, обратной связи. «Сеть» представляет собой новое пространство – информационное пространство, в котором и развертываются основные стратегические операции – как разведывательного и военного характера, так и операции, направленные на

«мягкий» перехват власти (управления) в той или иной стране, а также их медийное, дипломатическое, экономическое и техническое обеспечение. «Сеть» в таком широком понимании включает в себя одновременно различные составляющие, которые ранее рассматривались строго раздельно. Боевые единицы, система связи, информационное обеспечение операции, формирование общественного мнения, дипломатические шаги, социальные процессы, разведка и контрразведка, этнопсихология, религиозная и коллективная психология, экономическое обеспечение, академическая наука, технические инновации и т. д. – все это отныне видится как взаимосвязанные элементы единой «сети», между которыми должен осуществляться постоянный информационный обмен. Смысл проводимой в США военной реформы в рамках «новой теории войны» информационной эпохи состоит в создании мощной и всеобъемлющей сети, которая концептуально заменяет ранее существовавшие модели и концепции военной стратегии, интегрирует их в единую систему. Регулярная армия, все виды разведок, технические открытия и высокие технологии, журналистика и дипломатия, экономические процессы и социальные трансформации, гражданское население и кадровые военные, регулярные части и отдельные слабо оформленные группы, наемники и «частные армии» – все это интегрируется в единую сеть, по которой циркулирует информация. Создание такой сети составляет сущность военной реформы ВС США[5].

Концепция сетецентрической войны естественным образом включила в себя стратегию непрямых действий, трансформацию взглядов на ноополитику и доктрину упреждающих действий (преэмпции) Буша, а также отражает место и роль технологий информационного противоборства в достижении США глобальной гегемонии во всех сферах мирового пространства и установления окончательного диктата всему мировому сообществу, включая и нынешних союзников по НАТО (рис. 1)[6].

Стратегия непрямых действий – это достижение государством-агрессором геополитической победы в процессе противоборства. Она предполагает не только физическое разрушение самого института государственности страны-жертвы, что ведет к завоеванию ее территории и ресурсов, но и изменение цивилизационной, конфессионально-культурной и национальной идентификации ее народа. При этом следует подчеркнуть, что такая победа в ходе геополитического противоборства в отличие, например, от победы в войне является абсолютной и необратимой, то есть исторически не оспариваемой, ввиду исчезновения оспаривающей стороны.

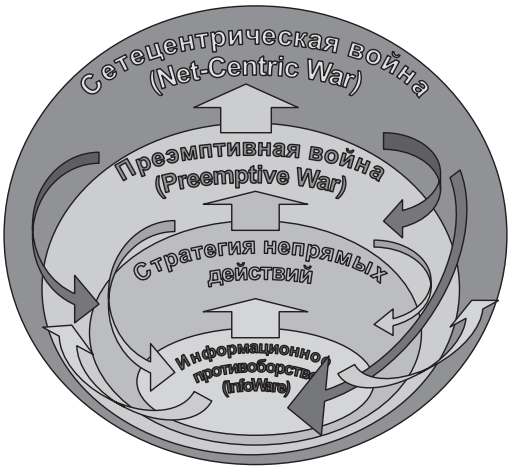


Рис. 1. Соотношение составляющих концептов действующих в США доктрин достижения стратегической униполярной гегемонии в XXI в.:

– прямые воздействия «по восходящей» траектории;

– обратные воздействия «по нисходящей» траектории

Стратегии непрямых действий и «мягкой силы» в настоящее время являются наиболее эффективными средствами ведения геополитической борьбы на международной арене, которые используются в целях ослабления реальных и потенциальных государств-противников.

Общая стратегия концентрированной атаки государства-агрессора против страны-жертвы, разработанная во многом под влиянием результатов исследований ученых-синергетиков, концептуально должна быть ориентирована на то, чтобы на достаточно длительный период полностью лишить государственно-геополитическую систему вражеского государства самой возможности устойчиво развиваться в соответствии с национальными интересами. Цель – создание социально-политического хаоса, необходимого агрессору для последующего разрушения и трансформации государственной системы в соответствии с принципами, которые полностью отвечали бы его геополитическим интересам.

Реализация стратегий непрямых действий и «мягкой силы» осуществляется на протяжении последних десятилетий в виде различных модификаций «цветных революций».

Произошедшие на постсоветском пространстве и на Ближнем Востоке «цветные революции» являются следствием разработанной в Соединенных Штатах технологии смены политических режимов, базирующейся на теории «управляемого хаоса» (или, как еще ее называют, теории «контролируемой нестабильности»), авторами которой являются Джин Шарп (автор книги «От диктатуры к демократии») и Стивен Манн (автор книги «Теория хаоса и стратегическая мысль»)[7].

Центральной задачей ведения всех сетевых войн является «совокупность действий, направленных на формирование модели поведения друзей, нейтральных сил и врагов в ситуации мира, кризиса и войны»[8]. Это означает заведомое установление полного и абсолютного контроля над всеми участниками актуальных или возможных боевых действий и тотальное манипулирование ими во всех ситуациях – и тогда, когда война ведется, и тогда, когда она назревает, и тогда, когда царит мир.

Понятие «сетецентрическая война», или «ведение боевых действий в едином информационно-коммуникационном пространстве», рассматривает боевые формирования как своеобразные устройства, подключенные к единой сети. В зависимости от выбора сетевой архитектуры и ее типа такими устройствами могут быть корабли, самолеты, средства поражения, управления, связи, разведки и наблюдения, группа военнослужащих или отдельные солдаты, а также комбинация и тех и других. В этом случае возможности боевых формирований определяются не столько индивидуальными тактико-техническими характеристиками отдельных образцов ВВТ, сколько возможностями всей группы подключенных к сети средств как единого целого.

Здесь, собственно, и проявляется эффект синергизма, когда целое представляет нечто большее, чем сумма его частей. В приложении к военному делу синергизм – это эффект от совместного действия объединенных в сеть средств вооруженной борьбы, который по совокупному результату превышает сумму эффектов от применения тех же средств по отдельности[9].

Основу информационно-коммуникационного пространства войны будущего составляет GIG – так называемая «Глобальная информационная решетка» (ГИР), представляющая собой мощную группировку разведывательных, коммуникационных и навигационных космических летательных аппаратов США на околоземной орбите (рис. 2). Именно ГИР связывает воедино все силы

и средства вооруженных сил США и их союзников по НАТО и обеспечивает их всей информацией, необходимой для ведения войны. Быстрое развитие компьютерных технологий требует создания новой концепции сетецентрических войн на базе современной интерактивной сети. В плане реализации такой концепции следующим шагом в достижении решающего информационного превосходства американским стратегам представляется слияние технологий ГИР, Web 2.0 и облачных вычислений.

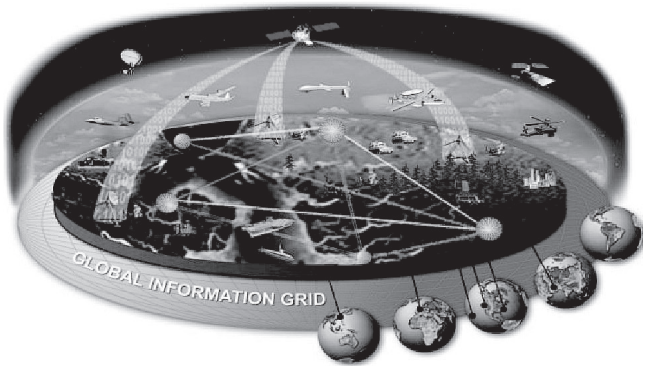


Рис. 2. Глобальная информационная решетка/сеть (The Global Information Grid (GIG)) – инструмент мирового господства

Облачные технологии стали следующим индустриальным шагом в трудном освоении сетевого пространства распределенных вычислений. Они реализуются в продвинутой сетевой архитектуре «клиент–сервер» с расширенной вычислительной интерпретацией, направленной на предоставление уже не только информационных, но и ресурсоемких алгоритмических услуг в широких диапазонах применения. Несомненно, облачные технологии позволят существенно расширить сферы применения распределенной обработки информации корпоративного уровня. В том числе способствовать достижению целей совершенствования работы вооруженных сил и спецслужб США.

Термину «cloud computing» различные поставщики решений до сих пор дают отличные друг от друга определения. «Облако» – это метафора, суть которой заключена в изображении Интернета на диаграмме компьютерной сети. Традиционно – если это слово вообще применимо в данном случае – под «облачными» вычисле-

ниями принято подразумевать технологии обработки данных, где информационные ресурсы и мощности предоставляются пользователю как сервис, базирующийся в Интернете. Вопрос наличия ИТ-инфраструктуры, ПО и операционных систем уходит для него даже не на второй, а скорее на третий план. Информация в нужный момент кэшируется на клиентской стороне и постоянно хранится на системах поставщика услуги.

Стремительные успехи таких гигантских корпораций, как Google, в ИТ-технологиях и облачных вычислениях неизбежно поставили вопрос о необходимости использования вооруженными силами Соединенных Штатов механизмов облачных вычислений в качестве практических технологий для проведения сетецентрических операций и боевых действий в будущих конфликтных ситуациях[10]. Для извлечения максимального эффекта из преимуществ облачных вычислений вооруженные силы США планируют в ближайшее время освоить Интернет в качестве сетевой базы ведения боевых действий взамен традиционных стационарных ИТ-структур, а также как можно быстрее освоить и применить в реальных «полевых» условиях новые сетецентрические концепции (далее в этой статье – сетецентрические войны 2.0), не упуская при этом из виду и другие аспекты: учет финансовых затрат, межвойсковое взаимодействие, повышение боевых качеств отдельных боевых платформ, расширение возможностей доступа к ведомственной и служебной информации, разработку методов и процедур для осуществления новых параллельных и последовательных операций, а также разработку и внедрение новых инновационных технологий для расширения возможностей анализа данных.

Облачные вычисления и Web 2.0 представляют собой фундаментальное преобразование методов доступа, хранения, трансляции и использования программного обеспечения и информации, существующих с самого начала информационной эры. Это изменение имеет потенциал для воздействия почти на все аспекты жизни общества, в том числе на военную концепцию ведения сетецентрических войн.

Опыт США по реализации федеральной госстратегии в области облачных вычислений

В настоящее время в США сформировался устойчивый тренд к целенаправленной информатизации разведывательного сообщества, вооруженных сил, да и страны в целом. И это вполне объективно, так как в современных условиях политической, экономиче-

ской и технологической обстановки информационные технологии рассматриваются в качестве инновационного инструмента повышения возможностей и конкурентоспособности государства при одновременной экономии средств. Это государственная политика, направленная на унификацию и оптимизацию всей информационной инфраструктуры в США, а также на поддержку внедрения прорывных технологических решений.

Облачные вычисления легли в основу новой Федеральной правительственной инициативы в области облачных вычислений (Federal Government's Cloud Computing Initiative), предложенной главным американским CIO (соответствует уровню федерального министра) Вивеком Кундрой в сентябре 2009 г. (к настоящему времени он уже покинул этот пост, перейдя на работу в Гарвард, но, как говорится, «процесс пошел»)[11]. В феврале 2011 г. этот же чиновник представил новую государственную стратегию в области информационных технологий страны. В соответствии с данной стратегией четверть федерального ИТ-бюджета США, который сегодня составляет 80 млрд дол., должна выделяться на облачные вычисления. Главные цели стратегии: снижение затрат, повышение прозрачности и эффективности государственных ИТ-расходов. В частности, предполагается, что ее реализация позволит добиться 30%-ной экономии на инфраструктуре дата-центров.

Стратегия в сфере облачных вычислений является самой масштабной и на сегодняшний день одной из самых результативных среди других государственных ИТ-инициатив, представляя собой по сути реформу управления ИТ на федеральном уровне США. Наиболее яркой инициативой Вивека Кундры стал проект www.data.gov, в рамках которого в течение 2010 г. было опубликовано в открытом доступе свыше 250 тыс. документов разных органов федеральной власти США. Эта инициатива стала одним из шагов реализации политики американских госорганов, направленной на раскрытие своей информации для всего общества.

В бюджетном послании президента США Барака Обамы на 2011 г. облачные вычисления были заявлены как основная часть стратегии для достижения эффективных и действенных технологий. Федеральные ведомства должны переходить на них для совершенствования оказания ИТ-услуг. Служба управления и бюджета (OMB) администрации президента США предложила всем госучреждениям при расчете основных инвестиций в ИТ в рамках исполнения финансового бюджетного процесса 2011 г. провести оценку потенциального внедрения альтернативных вариантов облаков, исходя из своих бюджетных возможностей.

Национальная стратегия облачных вычислений стала предтечей ряда других важных ведомственных документов. Среди них выделим «Стратегию облачных вычислений» МО США (DoD Cloud Computing Strategy), принятую в июле 2012 г.[12] В данном документе отражены намерения Пентагона трансформировать подходы, по которым он закупает, эксплуатирует свои информационные средства и управляет ими в интересах повышения эффективности выполнения поставленных задач, производительности, а также безопасности своих информационных систем. Таким образом, и в военном ведомстве США началась масштабная трансформация информационной структуры, предусматривающая формирование единого информационного пространства. По замыслу разработчиков, оно должно обеспечить новые возможности по сбору, обработке, обмену информацией, обеспечению ее безопасности независимо от местонахождения пользователя и аппаратных средств.

Министерство обороны США в рамках дальнейших усилий по формированию единого информационно-коммуникационного пространства (ЕИКП) вышло с инициативой подключить к нему не только свои ведомства, но и промышленность, а также другие правительственные учреждения. Уже к 2016–2020 гг. в формируемое пространство должны интегрироваться многочисленные разрозненные облака Министерства обороны США, разведывательного сообщества, военно-промышленного комплекса, правительства и др. По заявлениям представителей МО США, для успешной реализации планов главное – понять, что усилия по формированию единого информационно-коммуникационного пространства направлены не просто на развертывание сетей нового типа, их объединение и интеграцию, а на повышение эффективности применения вооруженных сил в войнах и вооруженных конфликтах будущего.

Пентагон выделяет следующие преимущества перехода в облака.

Эффективность	
Преимущества облачной среды	Текущая среда
Увеличение эффективности использования (использование серверов > 60–70%)	Низкая эффективность использования (использование серверов < 30%)
Объединенные требования и улучшенное системное взаимодействие	Фрагментированные требования и дублирующие друг друга системы
Увеличение продуктивности разработки приложений, управления приложениями, сетями и устройствами конечных пользователей	Сложность управления системами

Быстрота	
Преимущества облачной среды	Текущая среда
Приобретение сервиса у доверенных облачных провайдеров Почти мгновенное увеличение и сокращение требуемых ресурсов производительности Быстрая реакция на изменившиеся требования	Требуются годы для создания датацентра для новых систем Требуются месяцы для увеличения ресурсов производительности существующих систем
Инновации	
Преимущества облачной среды	Текущая среда
Переход от собственности (CBT) к управлению сервисом Переход к инновациям частного сектора Поощрение предпринимательства Улучшенная связь с появляющимися технологиями	Обременение управлением активами (CBT) Нет связи с инновациями частного сектора Нет склонности к риску

В то время как традиционные модели практического внедрения ИТ ориентированы на создание, внедрение и эксплуатацию компьютерного оборудования и программного обеспечения, модель облачных вычислений специализируется на предоставлении ИТ в качестве сервиса. В рамках модели облачных вычислений существуют поставщики услуг и потребители услуг. Сервис-провайдеры специализируются на выполнении конкретных задач или функций обслуживания потребителей. Поставщики услуг и потребители услуг взаимодействуют друг с другом через Интернет-протокол (IP)-сеть.

На рис. 3 представлена логическая основа предполагаемого к боевой эксплуатации облака Министерства обороны США по завершении конечного этапа его создания. Из него следует, что облако Министерства обороны представляет собой интегрированную среду, основанную на глобальной информационной сети/решетке (GIG), состоящую из компонентов Министерства обороны, коммерческих структур, федеральных организаций и партнеров.

Рис. 3. Облачная среда взаимодействия субъектов Министерства обороны США

Однако при переходе к среде облачных вычислений Министерство обороны отмечает, что испытывает определенные трудности при таком качественном переходе, в первую очередь связанные с проблемами обеспечения безопасности[13].

Проблемы при переходе к среде облачных вычислений

Несмотря на давно назревшую необходимость планируемых изменений, специалисты полагают, что они будут проходить болезненно. Большинство систем, стоящих на вооружении МО, были предназначены для работы в защищенной среде с выделенной инфраструктурой, и хотя облачные вычисления продолжают демонстрировать значительные преимущества, проблемы остаются. Так, существует определенная настороженность в плане достижения желаемых результатов по обеспечению необходимого и достаточного уровня конфиденциальности, целостности и доступности информации, чтобы не поставить под угрозу всю миссию по внедрению на боевое дежурство новых облачных технологий.

Таблица 2 определяет 5 общих категорий задач и мероприятий по смягчению последствий, которые помогут министерству решить эти проблемы. Следует отметить, что эти проблемы не являются исключительными для облачных вычислений и распространяются на все уровни управления.

Таблица 2

Проблемы перехода
к среде облачных вычислений

Изменение в управлении и культуре	
Проблемы	Смягчение последствий
Создание и поддержание руководством информационной службы МО первичного подхода к формированию облачных сервисов	Выполнение полномочий, делегированных Начальнику инф. службы МО по утверждению / использованию корпоративных сервисов по реализации возможностей JIE для всего министерства
Поддержка и управление развитием предпринимательской облачной среды для целей JIE	Установка под руководством Начальника инф. службы МО совместного управления для контроля функциональных компонентов облака
Преодоление культурных препятствий, ставших на пути МО ИТ-сообщества по принятию первичного подхода к формированию облачных сервисов	Выполнение познавательно-образовательной программы
Стимулирование предпринимательских инноваций в условиях существующей регуляторной политики МО и осуществление процесса выдачи мандатов	Внедрение гибких механизмов финансирования работ по созданию и использованию облачных сервисов
Обеспечение доступности, целостности информации; отказоустойчивость и кибербезопасность	
Проблемы	Смягчение последствий
Достижение видимости в реальном времени всех видов функционирования «облака», где потребители не имеют физического контроля над своими системами, сами системы могут изменяться динамически, а поставщики имеют возможность реагировать на возникающие требования роста вычислительных потребностей	Обеспечение регулирования, приобретения и киберзащиты политики, которой облачные услуги должны придерживаться для того, чтобы адекватно обеспечить безопасность и защиту информации Министерства обороны

Продолжение табл. 2

Реализация непрерывного мониторинга, обнаружения вторжений, обработки выявленных аномалий, последующего оповещения, а также проведение необходимой диагностики и формирование требуемых ответных реакций	Внедрение новых или изменение существующих технических возможностей для работы в облаке и, в частности, предоставление министерством сети и операционных системных центров (NOCs/SOCs)
Обеспечение коммуникационных и ИТ-возможностей для реализации IA-управления, которые обеспечивают мониторинг в реальном времени назначенных DOD IA персонала и обеспечивают методы и процедуры владельцев миссии по запросу	Поддержка критической защиты инфраструктуры, усиленная для обеспечения упругой и устойчивой среды облачных вычислений
Поддержание доступности данных, их конфиденциальности и устойчивости	Реализация IDAM, PKI и тэгирование защищенных данных по всему министерству
Поддержка судебно-медицинских, регистрирующих управлений, Закона о свободе информации (FOIA), а также двухфакторной аутентификации с общими картами доступа МО	Обеспечение эффективного приобретения коммерческих облачных услуг, используя Федеральный совет Службы информации, «Создание эффективных облачно-вычислительных контрактов для федерального правительства»
Независимость сети от линии фронта	
Проблемы	Смягчение последствий
Предоставление доступа к надежным, дистанционно устанавливаемым сервисам для войск США и вспомогательного персонала, работающих в ограниченных тактических условиях (высокая мобильность, риск отключения, неустойчивость связи, ограниченная пропускная способность и долгие задержки)	Предоставление услуг настолько широко, насколько это возможно, используя во время автономной работы наименьшее возможное значение пропускной способности
Обеспечение надлежащей защиты для обеспечения бесперебойной работы и отказоустойчивости	

Продолжение табл. 2

Служба приобретения и финансирования технического обеспечения	
Проблемы	Смягчение последствий
Переход от акцента на приобретение материальных решений и продуктов к акценту на приобретение и потребление облачных услуг	Создание политик и процедур бюджетирования, финансирования, приобретения, а также возмещения расходов, которые усиливают действие модели «плата за услуги»
Создание механизмов финансирования, которые могут быстро адаптироваться к изменениям спроса для поддержания роста широко используемых услуг	Использование функции брокера по регулированию использования, производительности и синхронизированной доставки предложения облачных сервисов
Сокращение или ликвидация инвестирования неполных и неэффективных услуг	Разработка бюджетной стратегии для финансирования первоначальных инвестиций облака через министерство
Осуществление эффективного управления изменениями в облачной среде	Сокращение или ликвидация инвестирования неполных и неэффективных услуг
Обеспечение права собственности на данные и перемещение данных одного облачного провайдера к другому	Создание и реализация критериев управления изменениями облачных вычислений МО
	Обеспечение заключения контрактов и механизмов приобретения, сохраняющих целостность данных и поддержку транспортировки данных
Перемещение данных, управление и взаимодействие данными	
Проблемы	Смягчение последствий
Обеспечение обнаружения данных и приложений, размещенных в различных облачных сервисах, доступ, хранение, использование и защита между различными компонентами МО и партнерами по миссии	Включение интеллектуальной доставки из различных источников информации в различных форматах приложений, обеспечение бесшовного в режиме реального времени обмена информацией, которая находится в безопасности, поддерживает несколько платформ и сочетает в себе новые достижения в области обработки информации и анализа данных
Оказание соответствующих услуг безопасности (мониторинга и реагирования, IA и т. д.), для обеспечения целостности, конфиденциаль-	

Окончание табл. 2

ности и доступности данных МО в среде облачных вычислений Обеспечение зависимости размещения данных МО-компонентов поставщика облачных услуг от технических и договорных условий, содействия в перемещении данных к другому провайдеру или обратно Обеспечение совместимости данных и безопасного обмена информацией с многонациональными и другими партнерами миссии с помощью облачных сервисов Обеспечение совместимости и переносимости данных Обеспечение всех категорий Контролируемой несекретной информации (CUI), включая личную информацию (PII), личную медицинскую информацию (PHI), международные правила торговли оружием (ITAR) и договорную информацию, правильно и надлежащим образом закрепленные, контролируемые и проверенные во время передачи, обработки и хранения	Принудительное использование оценки риска, которая считает воздействие на правовые, правоохранительные органы, и требования национальной безопасности принимающей страны Использование соглашения об уровне обслуживания (SLAs) для решений МО по обеспечению перемещений, конфиденциальности данных и требований к доступности Требование и обеспечение принятия предприятий обнаружения и поиска, исполнение IDAM и пометок данных, совместного управления и междоменного решения по безопасности Требование использования переносимости данных и совместимости стандартов по мере их появления Обеспечение протокольных правовых процедур соблюдения законов и правил, касающихся CUI-данных

На рис. 4 представлен переход от нынешней разнородной коммуникационной среды к консолидированным и виртуализированным приложениям и данным и, наконец, к облачной инфраструктуре, которая позволит Пентагону перейти к использованию в своих нуждах среды облачных вычислений.

Очередной этап реформирования американской разведки, направленный на повышение эффективности и оперативности информационного обмена между членами разведывательного сообщества, также связан с активным внедрением облачных технологий. Облачные технологии станут основой для формирования нового пространства, создаваемого в рамках инициативы, получившей название Intelligence Community Information Technology Enterprise (ICITE).

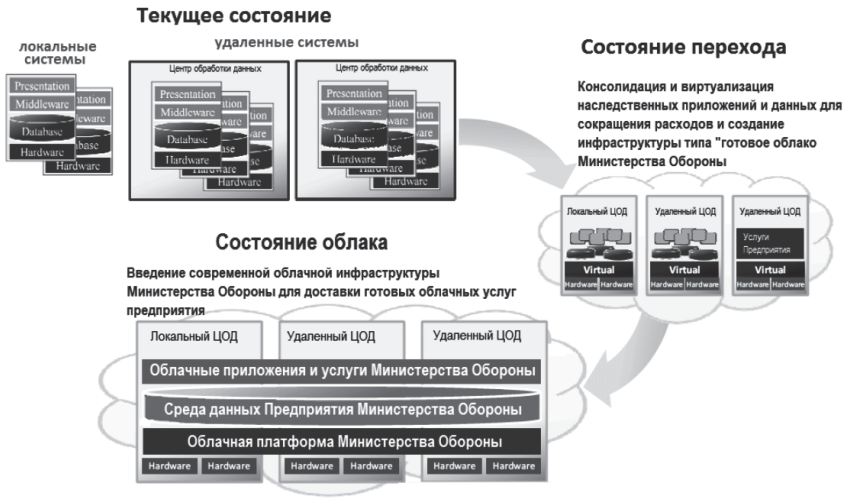


Рис. 4. Консолидированные центры обработки данных сформируют основу облачной инфраструктуры МО США

Сама инициатива была представлена широкой общественности в конце 2011 г., спустя несколько дней после того, как директор национальной разведки анонсировал планы секвестрирования бюджета разведывательного сообщества более чем на 10 млрд долл. И почти половина сэкономленной суммы сформируется как раз за счет оптимизации пунктов бюджета по информационным технологиям.

На практике планируемые изменения включают несколько инициатив, связанных с внедрением современных технологий, позволяющих в перспективе упростить и ускорить процедуры информационного обмена, а также радикально снизить сопутствующие расходы. Среди них можно выделить следующие.

• Обеспечение стандарта «тонкий клиент» для компьютеров большинства пользователей разведывательного сообщества.

• Интеграция облачных компьютерных технологий и архитектур, обеспечивающих организацию взаимодействия с другими сетями (облаками).

• Модернизация каналов передачи данных и оптимизация существующих программных приложений.

• Разработка концепции и проектирование консолидированного клиентского приложения и среды, реализующей концепцию рабочего стола для обеспечения формирования новой архитектуры.

Новый проект даже не об облачных вычислениях как таковых. По сути, его цель в объединении усилий ведомств американской разведки для создания распределенных возможностей, единых сервисов и служб. Реализация проекта позволит обеспечить доступ к необходимым базам данных и приложениям с любого компьютера разведывательного сообщества. Исчезнет сама необходимость поиска нужного компьютера или установки свитчей и хабов для организации связи между многочисленными сетями и сеточками. При этом никаких специальных секретных технологий создавать не планируется. Основу составят готовые аппаратные средства, специально адаптированные под нужды спецслужб.

По пути США в плане государственной поддержки внедрению облачных технологий пошли и другие высокоразвитые в области IT-технологий страны. Так, австралийское правительство видит следующие преимущества перехода к облачным вычислениям[14].

Таблица 3

Преимущество	Особенности
Масштабируемость	Неограниченная производительность дает возможность существования более гибким решениям, которые масштабируемы и легко меняются
Эффективность	Перераспределение ресурсов даст возможность агентствам сфокусироваться на: – исследовании и разработке новых приложений; – создании новых решений, которые технически/экономически невыполнимы без облачных сервисов; – ввод в эксплуатацию новых решений менее затратен и более быстр; – исследовании возможностей отделения приложений от существующей инфраструктуры
Уменьшение затрат	Позволяет изменить финансовую модель: – сервисы и дисковое пространство становятся доступны по требованию без серьезных финансовых вложений
Гибкость	– уменьшение времени ввода в эксплуатацию систем; – для переноса в облако нет необходимости использовать дополнительное ПО и железо; – удаленное внедрение; – возможность доступа к последним технологиям, т. к. провайдер регулярно обновляется

Окончание табл. 3

Доступность	– доступ к расширенной информации из любой точки мира; – облачное ПО разрабатывается с учетом поддержки максимальной сетевой производительности
Устойчивость	– сильно снижена вероятность отказа. Отказ одного из узлов облачной системы не несет угрозы работоспособности всей системы

Резюмируя развиваемые Минобороны США и правительственными структурами Австралии подходы к внедрению облачных систем, можно выделить следующие их преимущества по сравнению с ИТ прошлого этапа развития информатизации (табл. 4).

Таблица 4

Преимущество	Особенности
Маштабируемость	Ресурсы подстраиваются под систему
Эффективность	Высокая эффективность использования оборудования, высвобождение средств для новых проектов
Гибкость	Удаленное внедрение новых продуктов, уменьшение накладных потерь при вводе в эксплуатацию новых систем
Доступность	Доступ к информации по требованию из любой точки
Устойчивость	Снижается вероятность отказа системы. Выход из строя одного из узлов не нарушает работоспособность
Инновации	Поощрение новых разработок в этой области, переход от управления железом к управлению сервисом

Области приложений облачных систем

Таблица 5 дает представление о возможных местах использования облачных систем.

Таблица 5

Слой	Пример
Информационный и сервисный слой	
Сервисы, ориентированные на граждан	Предоставление услуг гражданам
Бизнес-процессы	Объединение разрозненных бизнес-процессов (финансовые, кадровые, планирование, управление контентом и т. п.)
Приложения	Прикладные программы, внешние услуги
Персональные данные	Индивидуальные проблемы граждан
Публичные данные	Открытые государственные данные, сайты, блоги, вики
Технологический слой	
Каналы	Государственные сайты и порталы
Технология (инфраструктура)	IT- и телекоммуникационная инфраструктура
Технология (процессы/вместимость хранилищ)	Обработка и анализ больших наборов данных Использование в качестве площадок для хранения данных

Сетецентрические войны 2.0: Перезагрузка домена киберпространства через «облака»

Учитывая тот неоспоримый факт, что двигателем прогресса в гражданских отраслях являются прорывные технологии, создаваемые в интересах вооруженных сил, целесообразно взглянуть на облачные технологии и с другой стороны. А именно: каким образом они рассматриваются представителями Пентагона в своих стратегических планах по завоеванию информационного превосходства над всеми своими потенциальными противниками и соперниками.

Поскольку нет общих стандартов для взаимодействия среди существующего на рынке изобилия доступных решений облачных вычислений, развить персонально ориентированные приложения для решения прикладных задач будет непросто и еще сложнее реализовать на их базе возможности для использования в военных применениях, особенно при проведении сетецентрических войн.

Например, как отмечают американские авторы, если персонал Министерства обороны использует Google Talk, а государственный департамент – Yahoo Instant Messenger, то эти подразделения остаются без возможности общаться между собой, используя сервисы мгновенных сообщений[15]. К тому же у них будут собственные глобальные списки электронных адресов. На рис. 5 представлен предполагаемый результат такого взаимодействия.

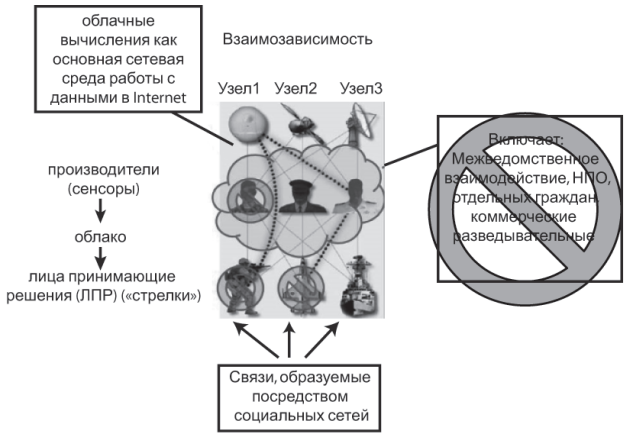


Рис. 5. Реализация концепции СЦВ 2.0 на основе использования различных федеральных облаков

Как отмечают американские специалисты, осуществление всей деятельности федерального правительства в облаке создает опасность ее компрометации. Хорошо известен факт, что сети Министерства обороны США уже давно сталкиваются с ежедневными атаками. Так, имели место несколько широко известных фактов взлома, приведших к компрометации данных: в 2007 г., например, взломщики Китайской народно-освободительной армии проникли в сеть Министерства обороны США и добыли из нее некоторые файлы[16]. Такого рода успешные атаки вызывают у специалистов по защите серьезную озабоченность по вопросу обеспечения безопасности данных в облачных вычислениях. Главное опасение связано с возможностью доступа к данным и отсутствием гарантированной защиты особо важной информации. Данные, хранимые в облаке, доступны в любой момент времени, что делает их уязвимыми для

злоумышленников, имеющих достаточно времени и ресурсов для изучения уязвимостей системы.

Если в будущем облачная система федеральных органов исполнительной власти США будет скомпрометирована, то это может привести к тому, что практически каждое постулированное достоинство использования облачных вычислений может обернуться реальным ущербом. Брешь в системе безопасности может легко подорвать все потенциальные преимущества и декларируемые возможности, предоставляемые облачными вычислениями.

Одна из возможных эффективных контрмер, предлагаемая для блокирования такой опасности, – это концентрация данных, способная обеспечить системную защиту от полномасштабного отказа систем федерального уровня. Другими словами, непораженные банки данных остаются доступными для соответствующих организаций, а подозрительные могут быть легко изолированы и зачищены. С этой точки зрения неспособность к быстрому взаимодействию между различными департаментами на самом деле может предотвратить полномасштабный отказ системы.

В общем, нерешенные проблемы безопасности добавляют ложку дегтя во все возможные преимущества облачных вычислений. Если злоумышленник/противник обладает возможностью компрометации облака, то все плюсы от его использования совершенно точно исчезнут и, что гораздо хуже, могут обернуться минусами, будучи использованы против их создателей. К тому же высокая степень взаимодействия в облачных системах делает возможным быстрое распространение угрозы по всей федеральной системе, чего можно избежать в случае эксплуатации только отдельных систем.

Полоса пропускания

Чтобы пользоваться и функционировать в облаке, необходимо обладать широкополосным каналом, так как традиционное коммутируемое соединение не справится с задачей. Таким образом, любая организация, создающая и использующая облачные системы, должна увеличить полосу пропускания для конечного пользователя, чтобы компенсировать распределенный характер облака.

Наличие достаточной пропускной способности также влияет на доступность спутниковой связи в целом и интернет-соединений в частности. Перегрузка существующей инфраструктуры всегда является серьезным испытанием для системы.

Взаимодействие

В рамках сетецентрических войн взаимодействие рассматривается как одно из наиболее весомых преимуществ сетецентричных войск, позволяющих эффективно объединять усилия для достижения успеха операции. Как бы то ни было, Web 2.0 и облачные вычисления уже сейчас предоставляют возможности по взаимодействию множества потребителей, в чем можно убедиться по предпринятым успешным попыткам организации межведомственного взаимодействия, вовлечения в информационный обмен иностранных партнеров и общественности. «Викиномика» предлагает несколько наглядных примеров взаимодействия, ставшего возможным благодаря Web 2.0.

Если партизанские войны, «мятеж-войны» или, как их определяет полковник Хэммс (автор «The Sling and the Stone»), боевые действия четвертого поколения, станут основой будущих военных конфликтов, то идея объединения масс населения страны-жертвы, на которую будут направлены «гуманитарные миротворческие» устремления ВС США, посредством использования предоставленного населению контролируемого оккупационными властями информационного ресурса, придется весьма кстати. Независимо от того, выявлен ли враг или он растворен среди населения, содействие местных жителей крайне необходимо. Для проведения соответствующих психологических операций используются специальные информационные мем-технологии в виде пандемии идей-вирусов[17]. Сегодняшние сетецентрические системы коммуникации первого поколения создают между войсками и населением цифровую пропасть: другими словами, население имеет очень ограниченный доступ к ценной информации в несекретных военных сетях либо не имеет его вообще. Создание открытой сетевой среды для кооперации с местным населением могло бы стать, по мнению американских военных, одним из решений этой проблемы.

Концепция сетецентрических войн 2.0, которую более уместно назвать концепцией социально-сетецентрических войн (Social Network-Centric Warfare), позволит, по мнению ее создателей, развивать эффективные виртуальные связи между военнослужащими и гражданами и, более того, сотрудниками государственного департамента, ЦРУ, ФБР и других служб[18].

Заключение

Бурное развитие теории, а главное – создание реально действующего инструментария эффективного ведения информационных войн в условиях локальных конфликтов последнего десятилетия позволило США на практике отработать сценарии ведения войн нового поколения и перейти к применению концепции сетецентрических войн в операциях по смещению неугодных режимов, не готовых к отражению агрессии нового типа. Проблема создания адекватного, пусть даже несимметричного ответного потенциала Россией перешла в разряд первоочередных задач сохранения ею независимости и суверенитета в XXI в.

Информационная война приобретает черты системного противоборства, так как инфосфера становится средой, через которую могут быть осуществлены реальные угрозы национальной безопасности и стабильности государств. Полем боя становится разум отдельных людей, групповое и массовое сознание, а инструментом борьбы – компьютерные социальные сети и облачные технологии.

Лидирующие позиции в сфере информационных войн позволяют ведущим странам Запада оказывать с помощью СМИ массированное информационно-психологическое воздействие на мировое сообщество с целью формирования благоприятного для них общественного мнения, необходимых взглядов и установок у населения разных стран. В связи с новыми вызовами национальной безопасности изменился подход к электронной войне в инфосфере, информационному противоборству, организации разведывательной деятельности.

Размывание традиционных ведомственных границ и переплетение сфер ответственности оборонных, разведывательных, дипломатических и правоохранительных структур (а в определенном смысле – и границ публичной и частной сфер) – ключевые следствия новых вызовов общественной и государственной безопасности в эпоху информационно-коммуникативной революции. Неизбежность данных процессов становится еще более очевидной с учетом фактора концепций ведения потенциальным противником сетецентрической войны.

«Холодная война» в новой сетевой редакции ведется на новых фронтах: культурном, цивилизационном, этническом, религиозном и т. д. Эта война является по содержанию духовноборческой, по сути – сетевой, а по организации – сетецентрической.

Разработки в области информационных технологий резко изменяют взаимодействие как народов, организаций, так и

отдельных людей. Быстрое распространение информации посредством социальных сетей и облачных технологий ставит под вопрос уместность привычных и обычных организационных и управленческих начал. Военное значение новых организационных наук, которые исследуют сетевые взаимоотношения в противоположность иерархическим моделям управления, также пока еще не полностью понято. Глобализация сетевой связи создает новые уязвимости ключевым национальным информационным инфраструктурам, и новые угрозы информационной инфраструктуре исходят именно из достижений в области глобальных телекоммуникаций. К сожалению, Россия не успела к настоящему времени перестроить свою систему безопасности под новый вид угроз.

Зная о том, какие шаги предпринимают США, России необходимо мобилизовать свой научно-технический и интеллектуальный потенциал для создания асимметричного потенциала способности ведения глобального информационного противоборства с целью обеспечения собственной информационной и, как следствие, национальной безопасности. У государства должна быть четко сформированная позиция по этому вопросу и соответствующее финансирование подобного рода программ.

Примечания

1 См.: *Cebrowski A.K., Garstka J.J.* Network-Centric War-fare: Its Origin and Future // Proceedings. 1998. January.

2 См.: *Arquilla J., Ronfeldt D.* Swarning and Future of Conflict. Santa Monica, CA: RAND National Defense Research Institute, 2000.

3 См.: *Григорьев В.Р.* Сетецентрическая парадигма информационного противоборства с позиции теории управляемого хаоса // Вестник ИКСИ. Серия «В». 2010. № 7. С. 291–321.

4 См.: *Шарп Д.* От диктатуры к демократии. Стратегия и тактика освобождения. М.: Новое издательство, 2012.

5 См.: *Arquilla J., Ronfeldt D.* Op. cit.

6 См.: *Григорьев В.Р.* Указ. соч.

7 См.: *Шарп Д.* Указ. соч.

8 См.: *Arquilla J., Ronfeldt D.* Op. cit.

9 См.: *Григорьев В.Р.* Указ. соч.

10 См.: *Кондратьев А.Е., Затуливер Ю.С.* Облачное будущее по-американски. Независимое военное обозрение от 11.02.2013. [Электронный ресурс] // Сайт Академии Военных Наук Российской Федерации. URL: http://www.avnrf.ru/

index.php/vse-novosti-sajta/500-oblachnoe-budushchee-po-amerikanski (дата обращения: 30.04.2013).

[11] См.: *Kundra V.* Federal Cloud Computing Strategy // U.S. Chief Information Officers Council. 2011. February 8.

[12] См.: Cloud Computing Strategy // Department of Defense. Chief Information Officer. 2012. July.

[13] См.: Cloud Computing Strategic Direction Paper // Australian Government Department of Finance and Deregulation. 2011. April. Version 1.0.

[14] Ibid.

[15] См.: *Spalding R.S.* Net-Centric Warfare 2.0: Cloud Computing and the New Age of War // USAF. A Research Report Submitted to the Faculty. In Partial Fulfillment of the Graduation Requirements. Air war college air universitu. 2009. 22 February.

[16] Ibid.

[17] См.: *Григорьев В.Р.* Информационные вирусы – новое оружие массового поражения // Информационные войны. 2008. № 3. С. 2–29.

[18] См.: *Spalding R.S.* Op. cit.

А.Е. Баранович

УПРАВЛЕНИЕ ЭВОЛЮЦИЕЙ МУЛЬТИМОДАЛЬНОГО КОНТЕНТА В ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СЕТЯХ*

В отношении вполне определенного класса угроз информационно-психологической безопасности открытого киберпространства, характеризуемого интенсивным развитием массовых информационно-коммуникационных технологий, формулируется перспективная стратегическая концепция управляемой эволюции мультимодального контента в открытых информационных сетях. Концепция основана на постнеклассическом информационно-эволюционном подходе к системному анализу и моделированию объективной реальности, атрибутивно-ингредиентной теории информации, аппарате управляемой эволюции естественного языка и методологических основаниях криптосемантики.

Ключевые слова: концентрация знаний, атрибутивно-ингредиентная теория информации, угрозы кибербезопасности, открытое киберпространство, криптосемантика, подход информационно-эволюционный, фильтры семантико-аксиологические, эволюция управляемая.

Введение

Организация социальной коммуникации в открытых информационных сетях (ОИС) РФ в настоящее время носит фактически стихийный, неуправляемый характер. До настоящего времени управление эволюцией контента осуществляется на уров-

* Статья подготовлена в рамках реализации Программы стратегического развития РГГУ, проект 2.1.1 «Решение комплексных проблем в области общественных и информационных наук» в Центре системного анализа и моделирования мышления Института информационных наук и технологий безопасности.

не «постусловия», т. е. реакции органов управления на изменения в социальной среде, происшедшие естественным, неуправляемым образом. Опережающее интеллектуальное управление коммуникацией на практике фактически отсутствует, как отсутствует и общая концепция управляемой эволюции сетевого контента. Что, в общем, нельзя сказать о действиях оппонентов РФ в контексте информационного противоборства в глобальном киберпространстве.

Заметим, что и сам Интернет как открытая информационная система включен в перечень реальных угроз человечеству в XXI в.[1] Вышеупомянутые угрозы реализуются в условиях фактически неограниченной (по ст. 29 Главы 2 Конституции РФ 1993 г.[2]) свободы производства и распространения информации (за исключением лишь нескольких пунктов), вне ее прагматических качеств истинности и социальной ценности для индивидуума[3].

Универсальных моделей, методов и средств управления эволюцией мультимодального контекста в информационных сетях общего назначения в открытых источниках ни за рубежом, ни в отечественной практике не представлено. Косвенные механизмы представлены (в иной предметной феноменологии) прежде всего логико-лингвистическими конструкциями поиска («отсеивания») необходимой информации во внешних источниках знаний, интегрированными в сетевые поисковые системы, средствами контроля за вредоносными программами (вирусами и транзакциями злоумышленников) и адресными блокираторами отторгаемых источников (например, защита от спама).

Аналитический обзор применяемых в настоящее время методик анализа сетевого контента, генерируемого антропными субъектами и киберботами сети, позволяет заключить, что в их основе лежат не универсальные механизмы глубинного семантико-аксиологического анализа, а совокупность элементарных структурно-статистических методов «поверхностной» семантики. То есть методов, опирающихся не на семантические (содержательные) атрибуты информации, а на поверхностные частотно-морфологические признаки мультимодальной лексики сети.

Таким образом, настоящий уровень развития аппарата системного анализа, управляемого синтеза и эволюции мультимодального контекста в ОИС, опирающегося на развитый аппарат информационного моделирования процессов семантико-прагматической коммуникации антропоморфных интеллектуальных систем, существенно отстает от общего уровня развития коммуникационных технологий.

Полученные к настоящему времени новые фундаментальные и прикладные научные результаты, частично отраженные в би-

блиографическом перечне основных публикаций по направлению исследований, наряду с появлением новых средств исследований и развитием междисциплинарных связей в новой информационной среде, создают принципиально новые возможности решения актуальных проблем мониторинга и управления контентом в социально значимых ОИС. Последнее предполагает реализацию возможности перехода в информационной среде от этапа эмпирического контроля и управления, классификации и систематизации открытого контента к этапу его интеллектуального целенаправленного мониторинга и управления, включая конструктивный синтез эффективных искусственных интеллектуальных механизмов преобразования социальной действительности.

В гуманитарной интерпретации проблема управления эволюцией мультимодального контента в ОИС очевидным образом пересекается (взаимодействует) со стратегией внутреннего и внешнего использования «мягкой силы РФ (2.0)»[4], в естественно-научной, информационной интерпретации – с фундаментально-прикладными результатами обеспечения локальной и глобальной информационной безопасности эволюционирующего социума как симбиотического коллектива автономных интеллектуальных систем.

I. Основания концепции управляемой эволюции сетевого контента и методологический базис ее реализации

Основным объектом, предметом и результатом деятельности в ОИС является мультимодальный контент, т. е. непосредственное информационное наполнение сети (в отличие от средств преобразования информации, также относящихся к информационным продуктам), представленное самыми различными форматами представления данных, ориентированными на эффективное взаимодействие с существующим расширенным сенсориумом индивидуумов социума.

В феврале 2013 г. Президент РФ отметил в своем выступлении на Коллегии ФСБ следующее: «Нужно блокировать попытки радикалов использовать для своей пропаганды возможности информационных технологий, ресурсы Интернета и социальных сетей <...> ни у кого нет монополии на право говорить от имени всего российского общества, тем более у структур, управляемых и финансируемых из-за рубежа <...> необходимо как можно скорее сформировать единую систему обнаружения, предупреждения

и отражения компьютерных атак на информационные ресурсы России»[5].

Основание концепции управляемой эволюции (КУЭ) мультимодального контента (МК) в открытых информационных сетях составляет положение о необходимости и возможности[6] целенаправленного управления генерацией (созданием), трансляцией (распространением), интерпретацией, преобразованием и использованием (уничтожением) социальной информации в открытых информационных сетях, основанного на конструктивном синтезе и использовании эффективных искусственных интеллектуальных механизмов создания, преобразования и эволюции социальной действительности[7]. В абстракции потенциальной осуществимости данный этап соответствует этапу синтеза искусственных виртуальных сред («миров») в теории интеллектуальных систем (ИнС) и современных информационно-коммуникационных технологиях (ИКТ), отвечая постнеклассической фазе современного естествознания[8].

Методологический базис разрешения проблемы управляемой эволюции сетевого контента представлен общей теорией систем и системного анализа, теорией эволюционного моделирования, атрибутивно-ингредиентной теорией информации, теорией интеллектуальных систем, теорией категорий, обобщениями аксиоматической теории множеств, теорией многоосновных алгебраических метасистем и обобщениями теории графов, теорией конечных метаавтоматов, теорией нейроподобных сетевых структур, исследованием операций, неархимедовым анализом, теорией самоорганизующихся систем, специальными разделами криптологии (криптосемантика), основами аксиологии и телеологии.

С точки зрения перспективных тенденций в создании современных интеллектуальных (информационных) систем, объединенных понятием «архитектура, обусловленная моделированием» («Model Driven Architecture» – MDA, «Meta Object Facility» – MOF), в методологическом базисе концепции целесообразно задействовать общую (единую) для всех ее компонент модель, определяющую основные принципы синтеза и эволюции информационной базы ИнС и интеграции ее различных приложений[9]. В качестве модели-универсума семантико-прагматической информации произвольных сложных макросистем (мультимодального контента) предполагается использовать апробированную модель множества семиотико-хроматических гипертопографов (СХ-ητ-графов) произвольного порядка топологизации множества-носителя k, редуцируемого в измеримое метрическое хроматическое k-гиперпространство

над GF(2) и поглощающего все известные модели представления декларативных знаний. Динамика процесса функционирования макросистемы и исчисления семантико-прагматических атрибутов информации в зависимости от уровня абстрагирования и постановки решаемой задачи моделируется конечной метаалгебраической системой, конечным метаавтоматом или семиотико-хроматической гипертопосетью, в качестве элементов основных множеств входа и внутренних состояний которого задействованы элементы измеримого метрического k-гиперпространства СХ-ητ-графов.

II. Основные направления, задачи и механизмы реализации КУЭ МК в ОИС

В приведенном библиографическом перечне авторских работ[10] представлены три основных класса угроз информационной и информационно-психологической безопасности социума, кратко характеризуемых общими понятиями: «защита информации», «защита от информации» и «защита информационно-вычислительных ресурсов».

Стратегической целью КУЭ МК в ОИС является создание системы воздействия на объекты ОИС в направлении ориентации сетевого контента (его субъектов-генераторов) на созидательную эволюционную деятельность, отвечающую системе цивилизационных геополитических ценностей и целей многонационального народа РФ, ее глобальных союзников и единомышленников, единого и многополярного в своем культурном разнообразии мира в целом, непосредственно содействующую гармоническому развитию всех и каждого.

С позиции стороннего наблюдателя, КУЭ МК в ОИС представлена как внутренними, так и внешними составляющими, отражающими задачи внутренней эволюции социума и его симбиотическое взаимодействие с социальными системами внешнего мира в общесоциальной геобиологической эволюции. Вследствие существенного различия целевых установок внутренней и глобальной эволюции вышеупомянутые составляющие могут быть представлены весьма различающимися направлениями, задачами и механизмами их реализации. В частности, в области цивилизационного информационного противоборства механизмы пассивной защиты (в вышеприведенных классах угроз) могут быть использованы наиболее эффективным образом в активном (наступательном) варианте.

В парадигме универсального эволюционизма последовательные этапы реализации КУЭ МК в ОИС представлены следующими обобщенными задачами.

1. Обеспечение многоуровневого доступа в ОИС, включая все уровни модели ISO.

2. Реализация комплексного и всестороннего мониторинга ОИС.

3. Обеспечение свободного доступа к информационным источникам.

4. Разработка и внедрение эффективных средств системного (контент-, ивент-, коннект-) анализа информации из ОИС, включая выявление, идентификацию и классификацию источников.

5. Комплексная характеризация семантико-прагматических атрибутов информации. Извлечение знаний из МК.

6. Управление доступом к МК в ОИС.

7. Управление конкретными составляющими МК (объекты, субъекты, инфраструктура).

8. Управление эволюцией контента, что в самой общей постановке может быть интерпретировано как увеличение «прагматического потенциала»[11] полезной информации в МК ОИС и деструкция или «смещение» вредной (бесполезной) информации в направлении снижения значения «прагматического потенциала» последней.

В рамках стратегии парирования вышеупомянутых классов угроз в контексте разрабатываемой КУЭ МК в ОИС по материалам работ[12] могут быть предложены следующие механизмы ее реализации.

1. Семантико-аксиологическая фильтрация.
2. «ε-концентрация» семантики информации.
3. Концентрация знаний.
4. Скрытое управление контентом посредством:
   – «экстралингвистического»* использования национального языка в качестве языка международного общения (ЯМО)[13] и, соответственно, навязывания «чужой» ментальной (семантико-аксиологической) среды посредством использования неофициального ЯМО;
   – навязывание модели контента информационного наполнения социальной коммуникации посредством информационно-вещественных продуктов иной ментальности, все механизмы управления которыми сосредоточены в руках производителя;

* Не имеющего лингвистического обоснования для использования в качестве наиболее эффективного средства международной коммуникации.

– различной семантической интерпретации контента (внутри генерирующей страты и вне ее).

5. Искусственное «смещение» прагматических характеристик социальной информации[14].

6. Управляемая «диффузия информации» как антиномия «концентрации знаний».

7. «Смещение» («замещение») семантики информации[15], формирующее в совокупности с п. 4–6 «управляемый хаос» семантической коммуникации социума*.

8. Автоматический выбор и формирование виртуальной комплементарной информационной среды существования (коммуникации) в ОИС (расширенный семантико-аксиологический и семантико-теологический поиск).

9. Формирование и управление первичными информационно-вычислительными ресурсами ОИС.

10. Управляемое формирование пространства знаний ОИС.

11. Формирование иллюзорных субъективных миров (активная подмена информационных прообразов сенсориума).

12. Персонализация и индивидуальная ответственность источников информации. Публичное игнорирование (дискредитация, ликвидация) анонимных источников.

13. Ограничение (ликвидация) уровней трансляции информации: первоисточник–транслятор–получатель. Разрешение контролируемых упорядоченных ссылок на первоисточники.

14. Ограничение интерпретации информационных прообразов.

15. Управляемое формирование телеологического пространства страт социума.

16. Формирование (выбор, синтез) и навязывание собственных системы ценностей и телеологического пространства социума.

---

* В качестве примера «смещенной» семантики общеупотребительного понятия можно привести уже сформировавшуюся в обыденном сознании своеобразную интерпретацию семантики термина «Апокалипсис» (греч. – Αποκάλυψης), свободно интерпретируемую в СМИ и общественном сознании как «Страшный суд» (религиоз.), и никак иначе. Автор был весьма удивлен, услышав последнее из уст официального представителя уважаемого Министерства иностранных дел РФ на одном из представительных международных форумов 2013 г. В то время как реальная семантика понятия есть «откровение, раскрытие». Соответственно, выражения «грядет Апокалипсис» или «нас ожидает Апокалипсис» в контексте наступления Страшного суда не имеют смысла (семантика – пуста).

Из системы ценностей следуют (–>) цели эволюции –> понятие прогресса –> показатели качества эволюции (развития) –> критерии оценки[16]. Таким образом, в разных системах ценностей «работают» различные критерии оценки и «не работают» унифицированные. Что касается системы ценностей исторической эволюции геополитического пространства России, то в его отношении необходимо отметить следующее.

Есть общечеловеческие (альтруистические) ценности (знания), способствующие эволюции всех и каждого (человечества)*, есть стратифицированные (эгоистические) ценности (знания), способствующие эволюции (прогрессу) отдельных страт и деградации иных (в рамках универсальных законов биологического эволюционизма).

И какие бы властные метаморфозы ни происходили на историческом пути России, страна со времен выбора в качестве духовной скрепы социума православного христианства (в противовес его биологизации) вкупе с общинным характером языческого бытия народа всегда тяготела к первым, обретая действительное могущество и привлекательность (в рамках собственной «мягкой силы») именно в моменты реального воплощения в жизнь данной системы (включая период реализации собственной социалистической модели развития)**, когда общее дело, общие цели, общий прогресс социума превалировали над индивидуальными. Но никогда – наоборот. В противовес антагонистическому антиподу – реальному сверхэгоизму индивидуальной свободы, усиленному заимствованной моделью западноевропейского капитализма.

III. О стратегии «опережающего действия» в КУЭ МК ОИС

Еще на пороге 2000 г. в контексте формирования концепции создания, использования и эволюции информационных технологий 2-го порядка, включающих подкласс интеллектуальных, отмечалось[17], что «...реализация концепции ... предполагает отказ от стратегии

---

* По И. Ефремову, такие универсальные ценности могут существовать и в отношении иных, неантропных ИнС.

** Не следует заблуждаться в абсолютном характере «мягкой силы». Симбиоз «жесткой» и «мягкой силы» носит выраженный мультипликативный характер. И существуют духовно не развитые страты, обреченные в историческом контексте, для которых принуждение (в их иллюзорном восприятии) есть единственный достойный эволюционный аргумент.

“догнать и перегнать” в рамках программы “устойчивого развития” и переход к стратегии “опережающего развития” как единственно возможной для сохранения державного статуса РФ в XXI веке».

Там же подчеркивалось, что наряду с прямым социально-экономическим эффектом от использования в конкретных приложениях интеллектуальные информационные технологии (ИИТ) позволяют получить весьма важный вторичный эффект от их внедрения в мировую информационную инфраструктуру. В случае включения в коллектив интеллектуальных систем естественных систем антропоморфного типа процедуры прямой и обратной редукции используемых моделей знаний в последовательные семиотико-лингвистические коммуникационные модели непосредственным образом связаны с использованием конкретного естественного языка (ЕЯ). При этом особенности реализации устойчивой несмещенной семантической коммуникации ИнС[18] оказываются неразрывно связаны с конкретными особенностями функционирования как подсистем знаний антропных систем, так и с особенностями их вербально-лингвистического аппарата, т. е. фактически с моделью менталитета нации* – создателя ИИТ. Дополнительным аргументом, подтверждающим вышеупомянутую связь, является то обстоятельство, что любая техническая антропогенная ИнС, включая системы «сильного искусственного интеллекта», так или иначе отражает особенности менталитета ее создателей, от авторов абстрактных антропных моделей ИнС до практических инженеров по знаниям.

Таким образом, в результате разработки в условиях информационной глобализации национальных ИИТ наряду с их основным социально-экономическим предназначением решаются и следующие, весьма важные для сохранения информационного гомеостаза ИнС, задачи:

а) монополизации интеллектуального полисенсорного интерфейса;
б) виртуального распространения национального языка;
в) внедрения национального менталитета создателей ИИТ в глобальные информационные (интеллектуальные) сети;
г) отображения особенностей национального менталитета на пользователей ИИТ;
д) обеспечения информационной и информационно-психологической безопасности социума (информационного противоборства) и т. п.

---

* Его интеллектуальной, культурной, психологической и даже эмоциональной составляющих (информационная характеризация).

В развитие положения «опережающего развития» ИИТ реализация концепции управляемой эволюции мультимодального контента в ОИС предполагает задействование стратегии «опережающего воздействия», в противовес настоящей запаздывающей управляющей реакции (... управление эволюцией ... на уровне «постусловия») на динамические процессы эволюции контента*. В классе ИИТ, предназначенных для использования в информационном противоборстве, данная стратегия реализуется посредством наступательных ИИТ, формирующих управленческое решение, путем информационного воздействия на динамическую среду функционирования ИИТ (ОИС)**.

---

* Управление путем реакции на происходящие изменения в динамической системе вполне допустимо, однако результаты запаздывающего воздействия могут быть неэффективны и, более того, непредсказуемы в общей постановке. В частности, проигрыш в информационной войне в Ираке привел к вооруженной интервенции, в результате которой истинные причины развязывания войны оказались весьма далеки от декларируемого инициаторами агрессии «наличия оружия массового уничтожения». Далее, в близком ключе, последовали Сербия, Ливия, Египет, Сирия. В историческом контексте правда в итоге может восторжествовать, однако отложенное управляющее воздействие на результаты войны вряд ли окажется эффективным для регрессирующего социума побежденной стороны. Результаты агрессии достигнуты. И «последействие» носит чаще всего лишь морально-этический характер. Несмотря на потенциальную истинность суждений Сунь Цзы о диалектическом круговороте «побед и поражений» (см.: *Сунь Цзы*. Искусство войны / Пер. с англ. / Пер. с кит., комм., прим. Л. Джайлса. Ростов н/Д: Феникс, 2002).

Следует заметить, что в информационной сфере «кристаллизация» оценок и позиций по ключевым вопросам развития социума реализуется в историческом контексте, завершаясь зачастую «полюсной» мифологизацией феноменов. В качестве примера можно привести формирование сонма святых христианской церкви или пантеонов выдающихся светских исторических личностей. Попытки игнорировать оправданно запаздывающую на несколько поколений историческую оценку деяний того или иного субъекта социума (в ложно интерпретируемом и политически мотивированном опережающем управляющем воздействии) приведут в итоге к противоположному в отношении планируемого результату.

** Управление воздействием на компоненты информационной инфраструктуры посредством целенаправленной семантической информации, в отличие от воздействия посредством изменения ресурсов (данных и программно-аппаратных элементов), есть принципиальное характеристическое свойство ИТ порядка 2.

Основу механизмов «опережающего воздействия» составляют эффективные модели предсказания (прогностические модели будущей эволюции), представляющие собой важнейший элемент подсистем знаний высокоразвитых интеллектуальных систем (с абстрактным мышлением)[19]. Причем в контексте информационно-эволюционного подхода к системному анализу и моделированию объективной реальности (ОР) этапы реальной («овеществленной») эволюции социума предваряются этапами «конструирования» (синтеза) идей (моделей эволюции). По любым направлениям: гуманитарным, естественно-научным, техническим.

Возникает интересный вопрос. Является ли конструирование идей* («генерация знаний») в процессе творчества (научного, художественного, религиозного) следствием «привлекательности» самой предметной области, т. е. ее «мягкой силы»? А если «генерация знаний» осуществляется путем конкретного экономического договора с непосредственной предоплатой процесса творчества? Имеем ли мы здесь пример «жесткой силы», т. е. принуждения к исполнению обязанностей творчества? Из практики хорошо известно, что предложение сколь угодно больших материальных благ за решение задач творческого характера вообще-то не является условием достаточным. И существуют задачи, разрешимые лишь в условиях свободного выражения воли творца. Из чего следует тезис о принципиальной невозможности (условие необходимости) реализации вполне определенных деяний субъекта под давлением обстоятельств (принуждением).

И далее, относится ли ветхозаветный «золотой телец» к мягкой («привлекательность») или «жесткой» (выживание, социальная конкуренция, механизм противоборства) силе? Из исторической практики хорошо известно, что для большинства представителей геосоциума (филистер-обыватель) стремление к максимизации наличия материальных средств (денег как универсального экономического эквивалента) в обыденном сознании биологической эволюции отождествляется с мифологической «свободой и демократией» «по-американски», вне ее очевидной, в последующем, неразрывной связи со всеми «семью смертными грехами» христианской (коммунистической) морали[20].

---

* Как предтечи прогностических моделей эволюции.

IV. Фальшивые фетиши в системах ценностей и целей

В разделе 2 в качестве одного из базисных механизмов реализации КУЭ МК определено формирование собственных системы ценностей и «пространства» целей социума. Именно на платформе сформированных ценностей и целей могут быть реализованы модели, методы и технологии КУЭ МК. Здесь необходимо отметить, что открытые информационные сети – не более чем новая коммуникационная среда на поле битвы вечных идей за души людей, представленная лишь в новой, «привлекательной» HiTec-упаковке, ориентированной зачастую на обман сенсориума и некритического интеллекта массового потребителя, но обладающая при этом рядом принципиальных особенностей, ранее недоступных иным коммуникационным средствам. В частности, к характеристическим свойствам ОИС можно отнести:

- высокую скорость активизации и реализации коммуникации;
- ее актуальную многовекторность;
- высокую эмоциональную нагрузку на участника коммуникации («коммуникационно-психологическая» конкуренция);
- гомоморфную проекцию психологических особенностей функционирования «толпы» на сетевые технологии;
- ограниченные возможности интеллектуальной деятельности индивидуума в ОИС;
- мощный поток информационных заявок, зачастую превышающий способность индивидуума по их осмысленной обработке (коэффициент загрузки системы $\rho > 1$).

Управляемо формируемый транснациональными корпорациями рынок мобильных гаджетов, наряду с их вполне определенной положительной ролью в эволюции социума, оказывает и весьма существенное отрицательное влияние на индивидуума, трансформируя его в ограниченный придаток будущей техногенно-сетевой цивилизации[21]. Таким образом, на сегодня не существует окончательного ответа на вопрос – являются ли ОИС аппаратом эффективной эволюции социума и источником истинной и достоверной информации (знаний) или нет.

В авторской работе 2007 г.[22] отмечено следующее: «С общих позиций, энтропия ... характеризует меру неопределенности, неупорядоченности (хаотичности), допустимого разнообразия системы в динамике ее существования. Негэнтропия характеризует меру упорядоченности, т. е. ограничений разнообразия или «ограничений, налагаемых на хаос». «Суть упорядочения состоит в ограничении

свободы ... хаос – ... полная свобода ... порядок – ограничение свободы ... Пойти по пути порядка – ... ставить ограничения, уменьшать число степеней свободы. Высший порядок ... когда нет выбора, есть только одна возможность»*. «В основе биологической эволюции (от неорганических соединений к человеку разумному) ... лежит механизм ограничения свободы». Причем не телеологический, а скорее синергетический, когда происходит упорядочение (рост негэнтропии), но без цели[23].

Более того, в антропоцентрической парадигме («...появление жизни на Земле предопределено ... природой, тем, как она устроена ... в ... природе был только один путь для возникновения жизни... и где бы жизнь ни возникла в нашей Вселенной, молекулярно она должна быть построена сходным образом...» [24]) человек как закономерный результат эволюции ОР сам включился в процесс ее упорядочивания, выступая уже в качестве синтезированного инструмента ускорения хода естественной эволюции. «...С появлением генетического кода завершился этап предбиологической эволюции /ОР/ и начался собственно этап эволюции жизни»[25] (сравн. с хаотической «предысторией человеческого общества» и его историей как познаваемым и управляемым процессом развития в социологических, политэкономических и философских доктринах от марксизма до «либеральной демократии» Ф. Фукуямы с его «концом истории»[26]).

Практическая реализация глобальных национальных и интернациональных проектов построения, в частности, информационного общества (post-post-industrial) или создания экономики знаний подтвердила невозможность их реализации без целенаправленного управления социумом (государством). Из вышесказанного следует, что разработка (и последующая реализация) КУЭ МК в ОИС необходимым образом отражает настоящее состояние современной науки в области синтеза перспективных интегрированных социальных информационных систем, а отсутствие постоянно действующих активных регуляторов МК делает весьма проблематичным его эффективное использование.

Из вышеприведенного утверждения о том, что «...в основе биологической эволюции ... лежит механизм ограничения свободы», вытекает элементарное для представителя естественной науки следствие. Религиозно-атеистическое «камлание» об абсолютном общечеловеческом характере «свободы» личности западноевро-

---

* Сравн. «свобода» как «осознанная необходимость» у Бенедикта Спинозы.

пейского («заокеанского») образца есть не что иное, как хорошо продуманный демагогический механизм завоевания информационного превосходства в борьбе с «традиционными» обществами за тотальное управление миром*, сформированный в период «рациональных» масонских революций (от Великой французской до Американской). Именно здесь сосредоточено их антагонистическое противоречие с миром «традиционных» цивилизаций, apriori признающим абсолютный характер не свободы, а системы ее ограничений (ответственности) в интересах социума в целом. Сами буржуазные конституционные принципы «прав и свобод» XVIII в., синтезированные по принципу «Богу – богово, кесарю – кесарево»[27], значимо отделенные, в частности, в Конституции РФ от ответственностей и обязанностей, в контексте их постнеклассической симбиотической взаимосвязи – устарели, неадекватны действительности, ограниченны и ущербны, представляя при этом элемент скрытого внешнего управления страной. Следовать им в полной мере в III тысячелетии – весьма неосмотрительно.

Перефразируя благоверного князя Александра Невского «Не в силе Бог, а в Правде» (т. е. истине), смеем утверждать, что «Бог не в свободе, а в Истине», и какова естественно-научная истина** – такова и норма свободы / ограничений. И множественные формы демократии – лишь ограниченное подмножество моделей формирования единой (совокупной, интегрированной) воли («общее дело») дееспособных субъектов социума – объединенного вектора его эволюции. Отсюда и эффективность демократии, связанная непосредственно с уровнем индивидуального развития знаний индивидуума (знаний, а не свободы). Ибо «ограниченные умы» видят демократию в одном свете, а мудрые – совершенно в ином.

Обратим также внимание и на конструктивно-имманентный антагонизм в системе управления европейской бюрократии, характеризуемый массовыми декларациями о «свободе» и реальными европейскими стандартами жизни, цементирующими виртуально свободных граждан в единое европейское социально-экономическое пространство. Конечно, в двойственной постановке тезис «стакан наполовину полон или наполовину пуст» по массе воды тождественен. Однако с метафизической позиции «наполовину полон» отражает эволюцию в сторону развития, а «наполовину пуст» – в сторону стагнации (деградации). Отсюда и пока не оформившиеся окончательно ответы на вопросы о механизмах моральной де-

---

* Сл. неумолкающее «Радио “Свобода”» (http://www.svoboda.org).

** Возможно, отождествленная и с религиозным догматом.

градации бывшего оплота христианства, а именно Европы – имеем ли мы дело с футурологической эволюцией самоорганизующейся системы или запланированной программой детерминированного хаоса. И в пока еще не окончательно разрушенной системе отношений «христианство–эволюция» – что лежит или должно лежать в основе социальной эволюции современной Европы – исторический опыт, научные знания или «свободный» полет фантазии «взбесившегося»* филистера (неопределенной национальной, культурной и гендерной ориентации) XIX–XXI вв.? И более существенно – является ли христианство тупиковой ветвью эволюции антропного социума, или отторжение христианства есть тупик его эволюции?

С прагматической точки зрения мы имеем дело с жестким столкновением на пороге III тысячелетия двух симбиотически связанных, но активно противоборствующих тенденций в процессе эволюции антропного социума – его «социологизацией» или «биологизацией». А также продолжающимся поиском ответа на вопрос – что является определяющим в направленном процессе эволюции коллектива антропных субъектов[28]: «дух» или тело (вещественное) – тело или «дух», биологический носитель или информационный контент личности (знания и мировоззрение)? В реальных условиях демагогически декларируемой социологизации и подспудно реализуемой биологизации.

В связи с этим, а также накануне приближающейся годовщины последней Российской Конституции 1993 г. хотелось бы отметить следующее. С одной стороны, официальные представители государственной власти говорят о значении и незыблемости основных положений Конституции. С другой стороны, они же уже неоднократно упоминали о непосредственном и массовом участии в организации политической жизни страны в 90-х годах XX в., в том числе и подготовке основных законодательных актов, иностранных советников, более того, кадровых сотрудников (агентов) Центрального разведывательного управления США. Действительно, что может быть эффективнее в управлении социумом, чем непосредственная подготовка законодательной основы его существования. В частности, в материалах телекомпании РенТВ утверждается[29], что «...бывший руководитель Ельцинской администрации уверен – без помощи американских политиков и ученых они бы не придумали ни одного закона»**. И далее, «... официальный сайт

---

* Озверевшего («звереющего»).

** С.А. Филатов, руководитель Администрации Президента Б.Н. Ельцина: «Это была осознанная политика Бориса Николаевича. С тем чтобы

Американского агентства по международному развитию в разделе своих достижений ... с гордостью сообщает, что за годы своей работы на территории нашей страны она (организация) разработала Конституцию России, Земельный кодекс Российской Федерации и, наконец, судебную реформу Российской Федерации...».

Обратимся же к тексту действующей Конституции РФ, а именно к статье 29 Главы 2. Права и свободы человека и гражданина. Уже с конца 90-х годов XX в. нами отмечались существенные угрозы информационной безопасности РФ, связанные с использованием в социальной практике указанной статьи, а именно ее п. 4 «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом...». Подробное изложение конкретных угроз безопасности, связанное с правом «каждого ... производить и распространять информацию...» вне оценки прагматических свойств ее истинности, ценности, достоверности, непротиворечивости и т. п., приведено в целом ряде ранее упомянутых авторских работ[30].

Обратим теперь внимание на существующие международные акты в области информационных прав и свобод.

Статья 19 Международного пакта о гражданских и политических правах 1966 г. гласит: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи* любыми средствами и независимо от государственных границ»[31].

На 102-й сессии Комитета по правам человека ООН (Женева, 11–29 июля 2011 г.) в Замечании общего порядка № 34 к Международному пакту о гражданских и политических правах в отношении ст. 19 (Свобода мнений и их выражения) еще раз подчеркнуто: «11. В соответствии с пунктом 2 государства-участники обязаны гарантировать право на свободу выражения мнений, в том числе право искать, получать и распространять всякого рода информацию и идеи независимо от государственных границ»[32].

с Соединенными Штатами проводить дальше такую конструктивную и дружескую, так сказать, политику... Естественно, они делали все для того, чтобы там этих ошибок не повторять ... И мы увезли от них богатейший материал, после чего были все эти законы приняты. Приняты почти в той редакции, которые мы состряпали, так сказать, после наших встреч ... да ... с американцами...»

* Налицо тавтология. Идеи, со времен Платона, есть информационный (невещественный) продукт.

О свободном производстве (создании, генерации) информации в документах не упоминается.

В сентябре 2011 г. Российской Федерацией, Китаем и рядом их союзников по Шанхайской организации сотрудничества на рассмотрение Генеральной Ассамблеи ООН внесены «Правила поведения в области обеспечения международной информационной безопасности», в которых о праве на свободное производство информации не говорится вовсе: «... f) в полной мере уважать права и свободы в информационном пространстве, в том числе на поиск, получение, передачу и распространение информации в соответствии с национальным законодательством каждого государства...» И это в целом уже положительный синдром[33].

Лишь только Конституция РФ, в написании которой так охотно принимали участие геополитические соперники России, в ст. 29 содержит прямое указание о праве каждого «производить и распространять информацию любым законным способом...».

Заключение

Изложенная в работе концепция управляемой эволюции мультимодального контента в открытых информационных сетях и основные направления и задачи ее реализации предполагают развертывание целого фронта работ по исследованию, анализу и синтезу эффективных механизмов мониторинга и управления сетевым контентом, опирающихся на фундаментальные результаты развития современной постнеклассической науки, упомянутые в разд. 1. Имеющиеся и формируемые ответы на сформулированные в разд. 3–4 актуальные вопросы исследования открытых информационных сетей и их информационного контента как естественно-научного, так и гуманитарного характера требуют, в свою очередь, отдельного изложения.

Список аббревиатур

ЕЯ – естественный язык
ИИТ – интеллектуальные информационные технологии
ИКТ – информационно-коммуникационные технологии
ИнС – интеллектуальная система
КУЭ – концепция управляемой эволюции
МК – мультимодальный контент

ОИС – открытая информационная сеть
ОР – объективная реальность
УЭ – управляемая эволюция
ЯМО – язык международного общения

Примечания

1 См.: *Brahic C.* 25 environmental threats of the future // [Электронный ресурс] NewScientist.com news service. URL: http://environment.newscientist.com/article/dn13505-named-25-environmental-threats-of-the-future.html (дата обращения: 30.04.2013).

2 См.: Конституция Российской Федерации: принята всенар. голосованием 12 дек. 1993 г. // Собр. законодательства РФ. 1994. № 1.

3 См.: *Баранович А.Е.* Введение в информациологию и ее специальные приложения: дидактические материалы к специальному курсу. М.: РГГУ, 2011.

4 См.: *Смирнов А.И., Кохтюлина И.Н.* Глобальная безопасность и «мягкая сила 2.0»: вызовы и возможности для России. М.: ВНИИ геосистем, 2012.

5 См.: *Латухина К.* Экстремизм не пройдет: Владимир Путин поставил задачи перед ФСБ // Российская газета. 2013. Федер. вып. № 6009. 15 февр.

6 См.: *Баранович А.Е.* Введение в предметно ориентированные анализ, синтез и оптимизацию элементов архитектур потоковых систем обработки данных. М.: НТЦ «Информрегистр», 2010.

7 См.: *Баранович А.Е.* О феноменологическом словаре теории интеллектуальных систем // Интеллектуальные системы. М., 2013. Т. 17. Вып. 1–4 (в печ.); см.: *Baranovich A.E.* Concept of operated evolution of a natural language: problem statement // Proc. of the 12th intern. conf. «Speech and Computer» SPECOM'2007. Moscow; Moscow State Linguistic University, 2007. P. 823–832.

8 См.: *Степин В.С.* Становление идеалов и норм постнеклассической науки // Проблемы методологии постнеклассической науки: [Сб. ст.] / РАН, Ин-т философии; [Отв. ред. Е.А. Мамчур]. М., 1992. С. 3–16; см.: *Аршинов В.И.* Синергетика как феномен постнеклассической науки / РАН, Ин-т философии. М., 1999.

9 См.: *Kleppe A.G., Warmer J.B., Bast W.* MDA Explained, the Model Driven Architecture: Practice and Promise. Addison-Wesley Professional Publishing Company Incorporated, 2003; см.: *Mellor S.J.* MDA Distilled, Principles of Model Driven Architecture. Addison-Wesley Professional Publishing Company Incorporated, 2004; см.: The Architecture of Choice for a Changing World™ [Электронный ресурс] // Сайт организации OMG. URL: http://www.omg.org/mda (дата обращения: 30.04.2013); см.: *Baranovich A.A., Kuznetsova I.A., Merzlikin V.G.* Modeling of the process of information accompani-ment of the life cycle of a biological system. Proc. of the VIII Intern. Conf. «Cybernetics and high technologies of XXI centuries» C&T-2007. Voronezsh, 2007. Vol. 1. P. 129–143.

[10] См.: *Баранович А.Е.* Защита «от информации» как компонент информационной безопасности интеллектуальных систем: аксиологические WEB-фильтры // Тр. VIII Междунар. научн.-техн. конф. «Интеллектуальные системы» (AIS'08). М.: Физматлит, 2008. Т. 3. С. 316–321; см.: *Он же.* Прагматические аспекты информационной безопасности интеллектуальных систем // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2009. № 10. С. 56–70; см.: *Он же.* О некоторых семантико-прагматических механизмах информационной безопасности // Системы высокой доступности. 2011. Т. 7. № 2. С. 84–89; см.: *Он же.* Семантические аспекты информационной безопасности: концентрация знаний // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2011. № 13. С. 38–58.

[11] См.: *Baranovich A.E.* Pragmatic Potential of Verbal Information: Aspects of Mathematical Modeling // Proc. of the 12th Intern. Conf. «Speech and Computer» SPECOM'2007. P. 844–852.

[12] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах. М.: МО РФ, 2002; см.: *Баранович А.Е., Баранович А.А., Лишин Н.А.* Исчисление ценности прагматической информации в интеллектуальной программной среде «АКСИОН» // Тр. XI национ. конф. по искусственному интеллекту с междунар. участ. КИИ-2008. М.: ЛЕНАНД, 2008. Т. 2. С. 364–372; см.: *Баранович А.Е.* Защита «от информации» как компонент информационной безопасности интеллектуальных систем: аксиологические WEB-фильтры...; см.: *Он же.* Прагматические аспекты информационной безопасности интеллектуальных систем...; см.: *Он же.* Введение в информациологию и ее специальные приложения: дидактические материалы к специальному курсу...; см.: *Он же.* О некоторых семантико-прагматических механизмах информационной безопасности...; см.: *Он же.* Семантические аспекты информационной безопасности: концентрация...

[13] См.: *Baranovich A.E.* Concept of operated evolution of a natural language: problem statement.

[14] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах...; см.: *Он же.* Введение в информациологию и ее специальные приложения: дидактические материалы к специальному курсу...; см.: *Грушо А.А., Грушо Н.А., Тимонина Е.Е.* Искусственная недостоверность информации как средство ее защиты // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2011. № 13. С. 123–127.

[15] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах...; см.: *Он же.* Семантические аспекты информационной безопасности: криптосемантика // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2012. № 14. С. 92–113.

[16] См.: *Смирнов А.И., Кохтюлина И.Н.* Глобальная безопасность и «мягкая сила 2.0»: вызовы и возможности для России...

[17] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах...

[18] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах...; см.: *Он же.* Введение в информациологию и ее специальные приложения: дидактические материалы к специальному курсу....

[19] См.: *Баранович А.Е.* О систематизации аксиоматического аппарата предметной области «Искусственный интеллект» // Интеллектуальные системы. 2010. Т. 14. Вып. 1–4. С. 5–34. см.: *Он же.* Информационно-эволюционный подход в теории интеллектуальных систем // Интеллектуальные системы. 2011. Т. 15. Вып. 1–4. С. 15–52; см.: *Он же.* О феноменологическом словаре теории интеллектуальных систем...; см.: Центр системного анализа и моделирования мышления [Электронный ресурс]. URL: http://www.samtcenter.ru/ (дата обращения: 30.04.2013).

[20] См.: *Данте Алигьери.* Божественная комедия / Данте Алигьери; [Пер. с итал., вступ. ст. и коммент. М. Лозинского]. М.: ЭКСМО, 2002.

[21] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах...; см.: *Brahic C.* Op. cit.; см.: *Баранович А.Е., Желтов С.А.* Гетерогенные архитектуры массовых вычислений и новые угрозы кибербезопасности // Системы высокой доступности. 2012. Т. 8. № 2. С. 16–22; см.: *Баранович А.Е., Сабо А.Р.* О некоторых возможностях внешнего управления мобильными устройствами // Тр. V Междунар. конгресса по интеллект. системам и информ. технол. / XIII Междунар. научн.-техн. конф. «Интеллектуальные системы» (AIS'13). М.: Физматлит, 2013 (в печ.).

[22] См.: *Baranovich A.E.* Concept of operated evolution of a natural language: problem statement.

[23] См.: *Галимов Э.М.* Общая судьба сложных соединений в нашей Вселенной // Эксперт. 2007. № 8 (549). С. 38–46.

[24] Там же.

[25] Там же.

[26] См.: *Fukuyama F.* The End of History // The National Interest (USA). 1989. № 16. P. 3–18; см.: *Он же.* The End of History and the Last Man. N.Y.: The Free Press, 1992.

[27] См.: Biblia. Novum IESU Christi D.N. Testamentum. Geneve: R. Estienne, 1551; см.: Библия. Книги священного писания Ветхого и Нового завета / Юбил. изд-е, посвященное тысячелетию Крещения Руси. М.: Изд. Московской патриархии, 1988.

[28] См.: *Баранович А.Е.* Информационно-эволюционный подход в теории интеллектуальных систем...; см.: *Он же.* О феноменологическом словаре теории интеллектуальных систем...

[29] См.: *Прокопенко И.С.* Русские тайны американских разведчиков [Электронный ресурс] // Сайт телекомпании REN TV. URL: http://ren-tv.com (дата обращения: 30.04.2013).

[30] См.: *Баранович А.Е.* Специальные курсы «Основы информациологии и ее специальные приложения» и «Современные информационные технологии» [Электронный ресурс] учеб. пособие. Ред. 1.0. М.: МГЛУ, 2003. 1 электрон. опт. диск (CD-ROM); см.: *Он же*. Прагматические аспекты информационной безопасности интеллектуальных систем...; см.: *Он же*. Введение в информациологию и ее специальные приложения: дидактические материалы к специальному курсу...

[31] См.: Международный Пакт о гражданских и политических правах. [Электронный ресурс] // Организация Объединенных Наций. URL: http://www.un.org/ru/documents/decl_conv/conventions/ pactpol.shtml.

[32] См.: Международный пакт о гражданских и политических правах [Электронный ресурс] // Организация Объединенных Наций. URL: http://www2. ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34_ru.doc (дата обращения: 30.04.2013).

[33] См.: Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Пункт 93 повестки дня 66-й сессии Генеральной Ассамблеи Организации Объединенных Наций. A/66/359. 14 September 2011 [Электронный ресурс] // Организация Объединенных Наций. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement (дата обращения: 30.04.2013); см.: *Смирнов А.И., Кохтюлина И.Н.* Глобальная безопасность и «мягкая сила 2.0»: вызовы и возможности для России...

Д.А. Ларин

О ВКЛАДЕ СОВЕТСКИХ КРИПТОГРАФОВ, ДЕШИФРОВАЛЬЩИКОВ, РАДИОРАЗВЕДЧИКОВ И СВЯЗИСТОВ В ПОБЕДУ В СРАЖЕНИИ ПОД КУРСКОМ. КРИПТОГРАФИЧЕСКИЕ АСПЕКТЫ БИТВЫ ПОД КУРСКОМ

Летом 2013 г. исполняется 70 лет сражения на Курской дуге (05.07.1943 – 23.08.1943) . После побед под Москвой и Сталинградом победа на Курской дуге была достигнута беспримерным героизмом советских солдат и стала очередной вершиной триумфального военного гения советских полководцев, поражение в этой битве привело фашистскую Германию к утрате стратегической инициативы. Советская армия начала активные наступательные действия с целью освобождения оккупированных территорий и полного разгрома агрессоров. Большой вклад в победу под Курском внесли советские криптографы, радиоразведчики, связисты, сотрудники разведки и контрразведки. Радиоразведчики и дешифровальщики успешно перехватывали и дешифровывали вражескую шифрпереписку. Ценнейшая криптографическая информация поступала из-за рубежа по линии разведки. В то же время связисты и работники шифровальной службы сумели обеспечить безопасность наших коммуникаций, при помощи которых осуществлялось управление войсками. Контрразведке при помощи криптографов удалось провести с немцами ряд радиоигр с целью дезинформации противника.

Ключевые слова: Курская битва, криптография, шифрование, дешифрование, шифр, шифратор, связь.

Весенние месяцы 1943 г. на советско-германском фронте были относительно спокойными. К началу апреля 1943 г. фронт представлял собой почти прямую линию от Ленинграда до берегов Черного моря. И лишь в районе Орла, Курска и Белгорода образовался огромный выступ, вошедший в историю под названием

Курской дуги, где закрепились войска Центрального и Воронежского фронтов. Наши и немецко-фашистские войска готовились к решающим летним сражениям. Имея достаточно объективную информацию от нашей радиоразведки и дешифровальной службы, а также военной разведки и контрразведки о намерении противника провести летом 1943 г. операцию «Цитадель», Ставка Верховного Главнокомандующего (ВГК) в течение апреля–июня развернула работу по созданию в районе Курского выступа мощной, глубоко эшелонированной обороны.

Значительную роль в выявлении планов врага и разгроме противника в Курской битве сыграли наши радиоразведчики из радиодивизионов особого назначения (ОСНАЗ)[1], криптоаналитики и сотрудники разведки. Накануне Курской битвы, буквально за сутки до начала сражения наши криптоаналитики вскрыли шифрованный приказ Адольфа Гитлера о наступлении в районе Курска[2]. Перехватив радиограмму, радиоразведчики опознали почерк радиста ставки противника и сделали вывод, что она содержит очень важный приказ. Дешифровальщики знали, что речь может идти о крупном наступлении фашистов, и предположили, что в конце документа находится подпись Гитлера. С помощью атаки «открытый-шифрованный текст» криптограмма была раскрыта. Она подтвердила информацию из других источников, в том числе и сообщения от нашего знаменитого разведчика Героя Советского Союза Н.И. Кузнецова, назвавшего дату наступления немецких войск под Курском. Приказ Гитлера войскам гласил: «Этому наступлению придается решающее значение. Оно должно завершиться быстрым и решающим успехом...»[3].

Советские радиоразведчики продолжали свою успешную работу и непосредственно в ходе сражения под Курском. Бывший в то время начальником отделения радиоразведки разведотдела Брянского фронта А.Ф. Соловьянов (впоследствии генерал-майор, начальник одного из военно-учебных заведений, кандидат военных наук) вспоминал, как в апреле 1943 г. в условиях строжайшего радиомолчания, введенного немцами в сухопутных войсках, нашей радиоразведке все же удалось установить создание на Орловском направлении ударной группировки за счет переброски туда целой полевой армии. Такой вывод наши радиоразведчики смогли сделать в результате наблюдения за радиообменом немецкой разведывательной авиации в УКВ-диапазоне. Люфтваффе (ВВС Германии) обеспечивали каждую полевую армию одной разведывательной группой, самолеты которой регулярно вели воздушную разведку переднего края нашей армии, докладывая с борта информацию о

положении наших войск. Так было и на Орловском направлении, где дислоцировалась 2-я полевая армия немцев. Но в апреле здесь появилась новая разведывательная авиационная группа, самолеты которой вели разведку исключительно южнее Орла в узкой полосе. Был выявлен еще ряд признаков, позволивших утверждать, что южнее Орла сосредоточена новая полевая армия, переброшенная для удара на Курск. Удалось установить количество корпусов и дивизий первого эшелона этой армии, определить разграничительные линии между ними. Спустя некоторое время данные радиоразведки получили дополнительное подтверждение воздушной и войсковой разведок[4].

В кульминационный момент Курской битвы 313-й радиодивизион ОСНАЗ, которым командовал подполковник П.Т. Костин, добыл важные данные об изменении направления главного танкового удара фашистов с Обояни на Прохоровку. Поворот немецких дивизий на Прохоровку обнаружила также воздушная разведка. Командующий Воронежским фронтом генерал армии Н.Ф. Ватутин, убедившись в достоверности этих данных, отменил переброску 5-й гвардейской танковой армии на Обоянское направление. Эта армия встретила противника под Прохоровкой и сорвала его планы. Впоследствии упомянутый выше радиодивизион был награжден орденами Красного Знамени и Богдана Хмельницкого. После войны его командир П.Т. Костин стал генерал-лейтенантом, лауреатом Ленинской премии, организатором одного из важнейших направлений военной разведки – радиоэлектронной разведки[5].

Для проведения операции на флангах Курского выступа были сосредоточены 50 дивизий противника (в их составе было 10 000 орудий и 2700 танков) и свыше 2000 самолетов 4-го и 6-го воздушных флотов. В дешифрованном приказе Гитлера указывалось, что наступление начнется в 5 часов утра. Советским командованием было принято решение нанести упреждающий удар. В 2 часа 20 минут наши войска начали артиллерийскую контрподготовку, которая нанесла немцам, сосредоточенным на исходных рубежах, значительные потери и оказала на них глубокое психологическое воздействие.

Кстати отметим, что для передачи информации немцы использовали не только радио, так, например, применялись цветные дымы. Вот что об этом вспоминает один из немецких солдат: «Стена фиолетового дыма поднялась в воздух, это были дымовые снаряды. Это означало: внимание, танки!»[6].

В ходе грандиозного сражения на Курской дуге враг был разгромлен, потеряв большое количество живой силы и техники. Так, например, из-за больших потерь ВВС, понесенных под Курском,

Германия вынуждена была впредь почти полностью отказаться от действий своей авиации по объектам нашего глубокого тыла. При этом источник ценнейшей для нашего командования информации очень сильно скрывался. Успех радиоразведчиков и криптографов стал одним из весьма важных факторов, приведших к победе под Курском. Однако о роли наших дешифровальщиков в победе под Курском до сих пор говорили лишь в очень туманных выражениях. Так, Маршал Советского Союза А.М. Василевский, бывший в период Курской битвы первым заместителем начальника Генерального штаба и координировавший действия фронтов в ходе крупных стратегических операций[7], в своей статье «Историческое сражение», написанной для газеты «Правда» от 04.07.1968 г., отметил роль неких «важнейших разведывательных данных»[8]. А вот еще одна оценка А.М. Василевского роли разведки перед Курской битвой: «В этот ответственный момент советское командование предъявляло особые требования к органам разведки. И, нужно сказать, она была на высоте и неплохо помогала нам. В первые два года войны мы, руководители Генштаба, не раз выслушивали справедливые упреки Верховного Главнокомандующего в адрес Разведывательного управления. В 1943 г. таких замечаний почти не было. Как ни стремился враг держать в тайне планы своего наступления, как ни старался отвлечь внимание советской разведки от районов сосредоточения своих ударных группировок, нашей разведке удалось определить не только общий замысел врага на летний период 1943 года, направление ударов, состав ударных группировок и резервов, но и установить время начала решительного наступления»[9]. Другой участник подготовки битвы под Курском, Маршал Советского Союза Г.К. Жуков, в то время заместитель Верховного Главнокомандующего[10], в своих мемуарах привел блестящий пример того, как можно делиться воспоминаниями, ничего, по сути дела, не рассказывая: «Стало известно, что сведения, полученные в тот день от захваченного пленного солдата 168-й пехотной дивизии, о переходе противника в наступление на рассвете 5 июля, подтверждаются...»[11]. Ну, вот так, просто стало известно[12].

Впоследствии высоко оценили работу наших радиоразведчиков и криптоаналитиков под Курском и немцы. Вот что позднее было написано одним из офицеров 19-й танковой дивизии вермахта: «Как выяснилось позже, противнику задолго до начала был известен X-день, а также Y-время наступления, вплоть до последнего изменения в 10 минут»[13].

Значительное количество информации о планах и намерениях немцев поступило по линии внешней разведки из Великобрита-

нии. Большой вклад в добывание английской криптографической информации внес член знаменитой «кембриджской пятерки»[14], сотрудник МИД этой страны Джон Кернкросс. Он начал работать на советскую разведку в 1935 г. Наиболее ценными разведывательными материалами, переданными Кернкроссом, были сведения, связанные с операцией «Ультра» (дешифрованием английскими специалистами немецкого шифратора «Энигма»). Кернкросс имел к ним доступ с 1942 по 1944 г., когда работал в дешифровальной службе Великобритании, располагавшейся в поместье Блетчли-парк. Название поместья стало неофициальным названием английской дешифровальной службы. Весной 1943 г. от Кернкросса поступила информация о намерениях немцев начать наступление в районе Курска (операция «Цитадель»). При этом сообщались подробности предстоящей операции, число и номера дивизий, которые должны принять участие в операции, данные по укомплектованности немецких частей вооружением, боеприпасами, средствами материально-технического обеспечения, направления ударов немцев. Эта информация имела особую ценность, так как советское командование предполагало, что немцы нанесут удар в направлении Великих Лук, а не Курска. В дальнейшем информацию Кернкросса подтвердили другие источники советской разведки. Сам Кернкросс особенно гордился тем, что ключи к шифрам люфтваффе, которые он передал советскому командованию, позволили перед Курской битвой разбомбить значительную часть немецких самолетов на земле, и это стало предпосылкой господства советских ВВС в небе над Курском. Он также информировал о расположении аэродромов люфтваффе, самолеты с которых должны были принять участие в операции «Цитадель». За два месяца до ее начала советская авиация нанесла по ним три упреждающих удара. Были уничтожены 17 аэродромов, люфтваффе потеряли около 500 самолетов. За свою работу он был награжден орденом Красного Знамени. Когда передавать информацию стало почти невозможно, Кернкросс ушел из Блетчли-парка в 1944 г. Впоследствии в связи с возникшими у английских спецслужб подозрениями Кернкросс покинул Великобританию[15].

Материалы «Ультра», переданные Кернкроссом, заметно дополнялись сведениями от сотрудника британской разведки Лео Лонга. С декабря 1940 г. он работал в британском Министерстве обороны в отделе MI-14, в котором занимались сопоставлением и анализом разведывательной информации, полученной в результате дешифрования немецких шифров, в первую очередь шифрмашины «Энигма». Лонг регулярно имел доступ к дешифрованным документам. Через некоторое время Лонг уволился с военной службы

и прекратил сотрудничество с советской разведкой. С секретными материалами британской дешифровальной службы, которая за время войны перехватила и дешифровала свыше 15 000 немецких криптограмм, советская разведка имела возможность знакомиться через своего агента Тони, еще одного члена «кембриджской пятерки» Энтони Бланта[16].

В мае 1943 г. НКГБ СССР направил в Государственный комитет обороны следующее сообщение: «Наш резидент в Лондоне передал текст телеграммы, отправленной 25 апреля 1943 г. из южной группы германских войск за подписью генерал-фельдмаршала фон Вейхса в адрес оперативного отдела Верховного командования армии; в телеграмме говорится о подготовке немцами операции "Цитадель" (прорыв нашего фронта в районе Курск–Белгород)»[17]. Скорее всего, текст этой телеграммы англичане получили в результате дешифрования «Энигмы», и он был передан в СССР Кернкроссом.

Ценный источник информации в британском военном ведомстве имела и советская военная разведка. Ее агент обладал доступом к материалам английской дешифровальной службы и передавал их советскому разведчику. В Москве этому агенту был дан оперативный псевдоним Долли. В Лондоне его работой руководил разведчик Билтон. В 1942 г. Долли передал Билтону множество (порциями по 25–38 штук) дешифрованных англичанами немецких, японских и турецких радиограмм[18].

Важнейшим видом боевых действий в эфире является радиоэлектронная борьба (РЭБ) – постановка помех вражеским линиям связи. В период Сталинградской битвы для ведения РЭБ были созданы радиобатальоны специального назначения (РБСН)[19]. Первое свое боевое крещение эти части получили во время Курской битвы. Их успеху также способствовала низкая радиодисциплина немецких связистов. Инициатором создания новой службы был заместитель начальника отдела радиоразведки Разведывательного управления Генерального штаба подполковник Михаил Иванович Рогаткин, и ему вместе с небольшим коллективом, составившим ее ядро, принадлежит разработка тактики действия дивизионов радиопомех, вооружение их необходимой техникой, организация подготовки и обучения кадров и многое другое, что необходимо для становления нового дела. М.И. Рогаткин был назначен начальником отдела радиопомех советской военной разведки. Уже после войны, до конца 1960-х годов, М.И. Рогаткин служил в центральном аппарате Министерства обороны, стал генералом, лауреатом Ленинской премии. Он – инициатор многих перспективных направлений развития радиоэлектронной разведки. Применение новой техники,

прежде всего средств УКВ-диапазона, в ходе Великой Отечественной войны значительно усилило не только тактическую, но и оперативную радиоразведку[20].

Все крупные наступательные операции, проводимые вооруженными силами СССР в годы Великой Отечественной войны, сопровождались дезинформированием врага при помощи радиоигр. Так, при подготовке к Курской битве и в ее ходе дезинформация поступала к противнику в ходе 17 радиоигр, проводившихся одновременно. Благодаря радиоиграм и работе наших дешифровальщиков советской контрразведке удалось практически парализовать агентурную деятельность в СССР Абвера (военной разведки фашистов) и СД (германской службы безопасности).

Рассмотрим одну из радиоигр подробнее. В ходе битвы под Курском сотрудники военной контрразведки «Смерш» из района Щигры–Курск–Брянск с 17 мая 1943 по август 1944 г. провели успешную радиоигру «Опыт». Работа радиостанции проводилась от имени группы немецких агентов из 3 человек, которые имели псевдонимы Шадрин – радист, Юденич и Суриков – разведчики. Немецкие агенты были выброшены на парашютах в нашем тылу в ночь на 8 мая 1943 г. В задачи агентов входило изучение дислокации воинских частей по маршруту Касторное–Курск–Льгов, мест сосредоточения техники и расположения штабов, оценка состояния железнодорожных путей и мостов, движения воинских и других грузов по этому маршруту, получение сведений о том, минируется ли Курск и какие оборонительные работы проводятся вокруг него. Донесения агенты должны были передавать немцам в зашифрованном виде при помощи портативной радиостанции КВ-диапазона. После приземления немецкие агенты направились в Курск и добровольно явились с повинной в штаб советской воинской части, после чего были доставлены в управление контрразведки «Смерш» Центрального фронта. В ходе следствия они дали подробные показания о характере их задания, известной им немецкой агентуре, выброшенной и подготовленной к выброске в тыловые районы Советского Союза, а также сообщили технические данные используемых немецкими агентами радиостанций, установленные немцами правила радиосвязи и шифры. Впоследствии радист группы Шадрин был перевербован и включен в радиоигру.

Главной задачей радиоигры является передача немцам дезинформации военного характера по указанию специалистов Генерального штаба наших вооруженных сил и проведение мероприятий по вызову к нам немецкой агентуры. Первый сеанс связи с немецким разведцентром был установлен 17 мая 1943 г., затем

каждые два-три дня легендированная радиостанция выходила в эфир и передавала дезинформацию, преследовавшую цель скрыть от германского командования готовившееся наступление советских войск в районе Курска. В соответствии с планом радиоигры в шифрованных радиограммах, направляемых к немцам, сообщалось, что в сторону линии фронта проходят эшелоны со строительными материалами, бронеколпаками, колючей проволокой и другими средствами, необходимыми для обороны, а в тылу фронта местные жители и саперы роют окопы, противотанковые рвы, строят блиндажи, доты и другие оборонительные объекты. Относительно сосредоточения войск и военной техники передавались незначительные данные. 12 июля 1943 г. от немцев было получено задание: сообщить сведения о наличии артиллерийских позиций в районе слияния рек Неруч–Зуша. Воспользовавшись этим обстоятельством, чекисты решили вывести из радиоигры сообщников радиста, а затем пролегендировать серьезные проблемы, возникшие у радиста при работе в одиночку; в связи с этим предполагалось вызвать еще одного немецкого агента ему в помощь. Одновременно решалась и другая задача – снижение активности работы данной группы агентов противника. Немцам сообщили, что оба разведчика отправились на задание и не вернулись. Таким образом, противник был поставлен перед необходимостью срочного оказания помощи оставшемуся радисту. 9 августа 1943 г. немцы прислали еще одного агента, который явился на встречу и был арестован. В связи с тем, что в этот период на фронте проходила операция по разгрому немецко-фашистских войск на Курской дуге и на фронт перебрасывалось много людей и боевой техники, наши контрразведчики, чтобы не поставить радиоигру на грань срыва, посчитали целесообразным умышленно притормозить работу легендированной радиостанции. Немцам сообщили, что встреча с их курьером не состоялась, и по-прежнему ссылались на сложные условия работы радиста, при этом поменяв место дислокации радиостанции. Из поступавших от противника шифрованных радиограмм было видно, что немцы крайне заинтересованы в срочном получении разведывательных сведений. После того как была перехвачена радиограмма немецкой разведки о прибытии курьеров в район ранее назначенной встречи, для их задержания была выслана опергруппа. Планом по оперативной разработке вновь прибывших вражеских агентов предусматривалось перед задержанием ведение наружного наблюдения для выявления интересующих нашу контрразведку сведений об их задании, инструкциях и условиях передачи радиограммы об успешном прибытии. В роли якобы немецкого радиста выступил сотруд-

ник «Смерш» Центрального фронта капитан Мурзин. В результате немцы на встречу с ним прислали своего агента. В ходе беседы с прибывшим агентом было установлено, что он и еще один агент, который скрывался и ожидал результатов контакта, были сброшены на парашютах в ночь на 23 августа. В задачу агентов входила встреча с радистом, передача ему пакета с деньгами, продуктами и элементами питания для радиостанции. Продолжая разыгрывать роль немецкого радиста, Мурзин вместе с немецким агентом и бойцом, выступившим в роли напарника радиста, встретился с другим немецким агентом. После продолжительной беседы с прибывшими немецкими курьерами, в ходе которой чекисты занимались выяснением всех интересовавших их сведений, вновь немецких агентов по одному направили на разные квартиры и там арестовали. Врагу же сообщили о благополучном прибытии их посланцев, но при этом отметили факт потери груза. Впоследствии немцам передали, что один из их агентов ушел в сторону линии фронта. При этом противнику продолжали посылать шифрованные радиограммы с дезинформацией, в подготовке которой принимал участие лично начальник военной разведки наших вооруженных сил, генерал-полковник Ф.Ф. Кузнецов.

Немцев просили прислать батареи для рации, фиктивные документы и продукты питания. Эти пожелания нашли отклик у вражеской разведки 27 февраля 1944 г., когда с самолета был выброшен контейнер с документами, деньгами в сумме 100 000 рублей, питанием для рации и обмундированием. В дальнейшем легендировалось создание разветвленной немецкой агентурной сети в городе Брянске, однако развить эту операцию в полной мере не удалось по ряду технических причин.

Всего за период проведения радиоигры противнику было передано 92 шифрованные радиограммы, получено в ответ – 51. Была инициирована переброска в нашу сторону трех немецких агентов, которые были обезврежены. Перевербованный чекистами немецкий агент Шадрин за успешную работу еще в ходе радиоигры был освобожден из-под стражи и указом Президиума Верховного Совета СССР от 28 октября 1943 г. награжден орденом Отечественной войны II степени[21].

Получение информации о противнике методами криптоанализа, а также дезинформирование немецкого командования в ходе радиоигр оказало существенное влияние на наш успех под Курском. С одной стороны, советские дешифровальщики представили руководству СССР информацию о планах и намерениях врага, с другой – контрразведчики сумели не только скрыть наши

планы, но и навязать противнику ложную информацию стратегического уровня[22].

Не менее важной задачей в ходе сражения на Курской дуге стала организация защищенной связи в полосе боевых действий и с тыловыми районами, в том числе руководством страны. Опыт оборонительных и наступательных операций Красной Армии в первом периоде Великой Отечественной войны подтвердил необходимость укрепления структур правительственной связи в действующей армии. Эта задача была возложена на НКВД СССР. Фактически был сформирован новый род войск НКВД – войска правительственной связи[23]. В первой половине 1943 г. был проведен ряд организационных мероприятий и изданы нормативные документы по улучшению функционирования правительственной связи, что положительно сказалось на организации управления войсками по линии Ставка ВГК – штабы фронтов и армий, ведущих боевые действия, и послужило импульсом к дальнейшему совершенствованию системы правительственной связи[24]. Одной из особенностей второго периода Великой Отечественной войны стало значительное возрастание роли высших штабов в управлении вооруженными силами. Большое значение в улучшении управления войсками приобрели оперативное и разведывательное обеспечение командования фронтов и армий, а также скрытность подготовки войск к предстоящим операциям, для чего к разработке планов их проведения привлекалось ограниченное количество должностных лиц. Достижению скрытности военного управления в звене Ставка–фронт–армия во многом способствовали органы и войска правительственной связи, деятельность которых постоянно совершенствовалась. Так, второй период войны характеризовался дальнейшим совершенствованием организации управления войсками в наступательных операциях. Пункты управления стали располагаться ближе к линии фронта; в обороне, кроме командных пунктов во фронтах и армиях, создавались запасные командные пункты и вспомогательные пункты управления; при подготовке пунктов управления к перемещению новые места их дислокации предварительно готовились в инженерном отношении и частично в отношении связи; большое внимание уделялось организации взаимодействия между родами войск и соседями, проведению оперативного ориентирования и т. п.[25] Все вышесказанное напрямую относится к организации связи в полосе действия фронтов, принимавших участие в Курской битве. Так, в марте 1943 г. было создано 8 новых линейных участков и увеличены штаты отделов правительственной связи ОПС ряда фронтов, в том числе принявших участие в Курской битве: Брянского, Воронеж-

ского, Юго-Западного. Это мероприятие имело целью обеспечить бесперебойное действие высокочастотной (ВЧ) связи от Москвы до штабов фронтов. В течение первой половины 1943 г. количество сил и средств, выделяемых для организации службы на армейских направлениях ВЧ-связи, неуклонно возрастало. Число отдельных рот войск правительственной связи на начальном этапе (февраль–март) составило 135, а к началу Курской битвы их было уже 207[26].

Важным моментом в поддержании бесперебойной связи была организация своевременного ремонта линий связи. Необходимость в проведении ремонтных работ возникала как в результате нарушения эксплуатационных норм, так и – в значительно большей степени – по причине повреждений на линиях ввиду воздействия авиации противника, передвижения танковых и механизированных частей, осколочных и пулевых повреждений, которых на магистралях от Ставки ВГК к штабам фронтов в апреле–октябре 1943 г. было зафиксировано более 2700. Поэтому масштаб ремонтных работ был колоссальным, в период Курской битвы были отремонтированы и проложены вновь десятки тысяч километров линий правительственной связи. Штабам Центрального и Воронежского фронтов были организованы две линии: основная и обходная к магистрали связи с Москвой. Линейная служба ВЧ-связи внутри фронтов планировалась таким образом, чтобы она могла обеспечить управление армиями как в оборонительном сражении, так и при переходе в наступление[27].

В середине 1943 г. был утвержден новый штат фронтового ОПС, предусматривавший наличие специальных должностей и подразделений для координации действий частей правительственной связи. Почти одновременно с изменением организационно-штатной структуры фронтового ОПС было утверждено новое «Положение о работе отделов правительственной ВЧ-связи фронтов, начальников отделений, начальников станций и инженерно-технического персонала» (приказ НКВД № 372 от 17.07.1943 г.). В соответствии с «Положением» фронтовым ОПС организовывались основная (фронтовая) станция правительственной связи и станции при каждой из армий, входивших в состав фронта. Задача станции, организуемой при штабе фронта, состояла в обеспечении засекреченной телефонной ВЧ-связи командования фронта с Москвой, а армейской станции – в обеспечении ВЧ-связи командующего армией со штабом фронта и с Москвой. Для обеспечения командующего фронтом ВЧ-связью на наблюдательном пункте (НП) формировалась выездная группа фронтовой станции в составе старшего техника и техника, оснащенная засекречивающей аппаратурой

телефонной связи типа «Снегирь», несколькими телефонными аппаратами и двумя-тремя комплектами щелочных аккумуляторов[28]. Еще одним типом аппаратуры засекречивания телефонных переговоров, впервые в массовом порядке примененной в ходе решающих боев на Курской дуге, стала аппаратура повышенной стойкости «Соболь», созданная под руководством знаменитого ученого В.А. Котельникова[29].

Для шифрования текстовых сообщений советские связисты применяли шифрмашины М-100, М-101 (наложение гаммы) и К-37 (дисковый шифратор многоалфавитной замены), а также ручные шифры. Наиболее распространенной системой шифрования советских вооруженных сил во время Великой Отечественной войны были коды с перешифровкой. При этом была установлена следующая иерархия: пятизначные коды для шифрования стратегической информации; четырехзначные для оперативного звена (уровень армия–фронт), трехзначные для тактического звена до уровня бригады и, наконец, двухзначные предназначались для низшего звена советских вооруженных сил. Свои кодовые системы (как правило, четырехзначные, хотя встречаются и пятизначные) использовали пограничники, внутренние и железнодорожные войска, которые тогда относились к НКВД. Советские дипломаты в основном использовали пятизначные коды. Полученный с помощью кодовой книги промежуточный шифртекст затем, как правило (в высших звеньях обязательно), перешифровывался одноразовой гаммой[30].

При этом также использовались и весьма простые, но эффективные методы защиты информации. Так, все военачальники даже при ведении переговоров по зашифрованным каналам связи использовали псевдонимы: И.В. Сталин представлялся Ивановым, у А.М. Василевского был псевдоним Александров, у И.С. Конева – Степной, у Н.Ф. Ватутина – Николаев и т. д.[31] Также применялся режим радиомолчания: так, 5-я гвардейская танковая армия генерал-лейтенанта П.А. Ротмистрова выдвигалась в район Прохоровки, соблюдая полное радиомолчание, что не позволило вычислить ее прибытие радиоразведке противника, и только после сосредоточения для контрудара было разрешено использовать радио: «...2. Начало атаки в 8.30 12.07.43 г. Начало артподготовки с 8.00. 3. Разрешаю пользоваться радио с 7.00 12.07.43 г. Командующий 5 гв. ТА генерал-лейтенант Ротмистров»[32].

Командующий фронтом и посещающие фронт представители Ставки ВГК пользовались при разговорах по ВЧ паролем «Молния» (дающим право прерывать переговоры абонентов низших категорий), а при выходе на связь Верховного Главнокомандующе-

го – паролем «Большая молния», предусматривавшим немедленное соединение и наличие двух каналов – основного и дополнительного (организованного через соседние фронты). В интересах оперативного и качественного обеспечения правительственной связью приоритетных абонентов наличие связей с соседними фронтами постоянно контролировалось сменными инженерами Московской ВЧ-станции[33].

В период, предшествовавший Курской битве, перед НКВД была поставлена задача организации устойчивой засекреченной связи штабов фронтов со Ставкой и штабами армий. К началу сражения в районе Курского выступа были сосредоточены войска Брянского, Центрального, Воронежского и Степного фронтов, а также левого крыла Западного и правого крыла Юго-Западного фронтов. Для обеспечения правительственной связи командование каждого из фронтов располагало отдельным полком правительственной связи (ОППС), это были 2, 3, 4, 11, 13 и 16-й ОППС (соответственно Западный, Воронежский, Юго-Западный, Центральный, Брянский и Степной фронты).

В ходе подготовки наших войск к летним операциям в районе Курской дуги для обеспечения устойчивого управления войсками фронтов и армий была развернута сеть командных, запасных и наблюдательных, а также вспомогательных пунктов управления: каждый фронт имел командный, 2–3 запасных командных и 1–2 вспомогательных пункта управления. Армии, в свою очередь, кроме командных пунктов, имели по 1–2 запасных командных, по 1–2 вспомогательных и по 3–4 наблюдательных пункта управления. Поэтому фронтовые ОППС готовились организовать для каждого из штабов фронтов и армий ВЧ-связь на нескольких пунктах управления: основном, запасном, а иногда и на передовом (КП, ЗКП, ПКП). Кроме того, при оперативных выездах командующих фронтами в войска с ними должен был направляться офицер правительственной связи с подвижным комплектом засекречивающей аппаратуры связи, позволяющим обеспечить связь со Ставкой ВГК. И.В. Сталин всегда должен был иметь возможность связаться с командующим любым фронтом, если последний не находился в это время в движении[34].

Достаточно продолжительная оперативная пауза, предшествовавшая Курской битве, предоставила фронтовым ОППС и частям войск связи возможность (пожалуй, впервые за все время войны) создания опорной сети правительственной связи в тылу оборонявшихся, а впоследствии наступавших фронтов. Эта сеть, построенная с учетом особенностей предполагаемого развития

боевых действий, позволила в наиболее тяжелый период перехода войск в контрнаступление не только обеспечить связь с пунктами управления, но и успешно наращивать ее при достаточно высоких темпах передвижения штабов. Накануне Курской битвы фронты располагали достаточно разветвленными сетями проводной связи. Так, проводная связь Центрального фронта со штабами армий обеспечивалась по 2–3 направлениям, разнесенным на местности, что значительно повышало их живучесть. Кроме того, для повышения устойчивости работы и получения обходных направлений в полосе действий войск фронта были построены кольцевые проводные линии вокруг Курска, Льгова, Фатежа, Золотухино и узла связи командного пункта фронта. К началу оборонительного периода сражения была организована устойчивая ВЧ-связь КП фронта с Генеральным штабом и оперативной группой представителей Ставки ВГК[35].

Следует отметить, что работа советских связистов и шифровальщиков во время Курской битвы стала боевой проверкой новой структуры организации войск правительственной связи, с формированием которых система ВЧ-связи Ставки ВГК обрела черты единой инфраструктуры и быстро стала завоевывать авторитет в высших военных кругах. Командующий 3-й гвардейской армией генерал-лейтенант Д.Д. Лелюшенко писал: «В самый разгар боя за Мценск мне сообщили: “Товарищ генерал, вас срочно просят к ВЧ”. Высокочастотный телефон в то время был новинкой. Его устанавливали для поддержания надежной связи между Ставкой и штабами крупных войсковых соединений. По ВЧ велись особо важные переговоры, передавались директивы Верховного Главнокомандования. Для нас, командиров крупных соединений, вызов к ВЧ почти всегда означал новый приказ или серьезный разговор»[36]. В свою очередь, начальник управления войск правительственной связи НКВД генерал-майор П.Ф. Угловский в одной из докладных записок на имя наркома внутренних дел Л.П. Берия констатировал: «Командование фронтов считает большим достижением в области войсковой связи наличие ВЧ-связи в звене фронт–армия. Эту связь они используют как основное и самое лучшее средство управления войсками»[37].

Делая выводы о работе службы правительственной полевой связи в летних наступательных операциях 1943 г., начальник УВПС П.Ф. Угловский в письме заместителю наркома внутренних дел И.А. Серову от 13.08.1943 г. отмечал: «Опыт последних боевых операций показал, что правительственная ВЧ-связь стала основным средством связи для командования фронтов в звене фронт–

армия... Ввиду явных преимуществ ВЧ-связь (связь телефонная, ведение секретных переговоров) в сравнении со связью, организуемой Управлением связи Красной Армии (радио, телеграф без засекречивающих устройств), командующие фронтами, члены военных советов и начальники служб фронтов справедливо оценили этот вид связи... По телефону ВЧ практически разрешено вести не только секретные, но и сов. секретные переговоры. Одно уже это обстоятельство делает ВЧ-связь в глазах командования фронтов и армий **САМЫМ ЦЕННЫМ И НЕЗАМЕНИМЫМ СРЕДСТВОМ УПРАВЛЕНИЯ ВОЙСКАМИ**» (выделено авт. цитаты)[38].

Подводя итог анализа деятельности советской криптографической службы в период подготовки и проведения Курской битвы, необходимо подчеркнуть, что на своем участке борьбы с противником она выполнила все стоящие перед ней задачи, а по ряду важнейших направлений его превосходила и тем самым внесла свой неоценимый вклад в общую победу Советской армии.

Примечания

1 Подробнее о создании дивизионов ОСНАЗ можно прочитать в книге: *Бутырский Л.С., Ларин Д.А., Шанкин Г.П.* Криптографический фронт Великой Отечественной. М.: Гелиос АРВ, 2012 и статье: *Ларин Д.А.* Защита информации и криптоанализ в СССР во время Сталинградской битвы // Вестник РГГУ Сер. «Информатика. Защита информации. Математика». 2012. № 14. С. 11–28.

2 Таким образом была подтверждена информация разведки, предоставившей этот приказ (по другим данным директиву (http://ru.wikipedia.org), правда, документ еще не был подписан Гитлером, советскому руководству весной 1943 г. (http://www.militera.lib.ru/memo/russian/mykoyan/04.html). Предположительно эта информация была получена из Германии через советскую разведсеть в Швейцарии «Люси» (http://ru.wikipedia.org), подробнее о работе этих разведчиков, в том числе о криптографических аспектах их деятельности, можно прочитать в главе 6 книги: *Бутырский Л.С., Ларин Д.А., Шанкин Г.П.* Указ. соч.

3 См.: *Жельников В.* Криптография от папируса до компьютера. М.: ABF, 1996. 335 с.

4 См.: *Шмырев П.* Часовые эфира (об истории радиоразведки) [Электронный ресурс] // Сайт журнала Computerra. URL: http://offline.computerra.ru. (дата обращения: 30.04.2013).

5 Там же.

6 См.: *Мощанский И.Б.* Крупнейшие танковые сражения Второй мировой войны. Аналитический обзор. М.: Вече, 2011. С. 297.

[7] См.: Советский энциклопедический словарь. М.: Советская энциклопедия, 1984. 1600 с. (далее – Словарь 1984).

[8] Цит. по: *Жельников В.* Указ. соч.

[9] См.: *Василевский А.М.* Дело всей жизни. М.: Политиздат, 1978. 552 с. [Электронный ресурс] // Военная литература. URL: http://www.militera.lib.ru/memo/russian/vasilevsky/index.html (дата обращения: 30.04.2013).

[10] Словарь 1984.

[11] См.: *Жуков Г.К.* Воспоминания и размышления. М.: Олма-Пресс, 2002 [Электронный ресурс]. URL: http://www.militera.lib.ru/memo/russian/zhukov1/index.html (дата обращения: 30.04.2013).

[12] Подробнее об этом можно прочитать в статьях; *Коровин В.* Курская битва: реванш советской разведки // Диалог. 1993. № 5/6. С. 46–50; *Сладков С.* Откуда после Курской дуги Сталин знал все гитлеровские планы? Взлом немецкой шифровальной техники во время Второй мировой войны // Открытая электронная газета Forum.msk.ru. URL: http://forum-msk.org/material/power/684315.html

[13] См.: *Ащеулов О.Е.* Остановившие «тигров» и «пантер»: артиллеристы Воронежского фронта в оборонительных боях Курской битвы // Военно-исторический архив. 2012. № 7 (151). С. 60.

[14] «Кембриджской пятеркой» называют созданную в середине 1930-х годов советским резидентом в Великобритании А.Г. Дейчем разведсеть из выпускников Кембриджского университета. В нее входили Гай Берджесс, Энтони Блант, Джон Кернкросс, Дональд Маклин и Ким Филби. Подробнее о работе этой сети можно прочитать, в частности, в работе: Очерки истории российской внешней разведки: В 6 т. / Под ред. Е.М. Примакова, С.Н. Лебедева. М.: Международные отношения, 1997.

[15] Более подробную информацию о добывании английских криптографических секретов Д. Кернкроссом и другими членами «кембриджской пятерки» можно получить, в частности, из книги: *Бутырский Л.С., Ларин Д.А., Шанкин Г.П.* Указ. соч. Гл. 6.

[16] *Лекарев С., Порк В.* Радиоэлектронный щит и меч // Независимое военное обозрение. 2002. № 2. С. 7.

[17] См.: Разведдаты мая // Независимое военное обозрение. 2003. № 15. С. 7.

[18] См.: *Лота В.* Секретный фронт Генерального штаба // Красная звезда. 2002. 2 нояб. *Серов Е., Волгин В.* Тайны военной разведки (1918–1945) // Армия. 1993. № 20. С. 53–56; № 21. С. 49–55; 1994. № 7. С. 52–55.

[19] Подробнее об этом рассказано в статье: *Ларин. Д.А.* Указ. соч.

[20] См.: *Болтунов М.Е.* «Золотое ухо» военной разведки [Электронный ресурс] // Онлайн-библиотека. URL: http://read24.ru/fb2/mihail-boltunov-zolotoe-uho-voennoy-razvedki/ (дата обращения: 30.04.2013).

[21] Более подробную информацию о радиоиграх с немецкой разведкой можно получить, в частности, из следующих источников: *Бутырский Л.С.,*

Ларин Д.А., Шанкин Г.П. Указ. соч. Гл. 7; *Макаров В., Тюрин А.* Как появился «Опыт». Радиоигры «Смерша» в годы Великой Отечественной войны // Военно-промышленный курьер. 2007. № 37; *Макаров В., Тюрин А.* Лучшие операции СМЕРША. Война в эфире. М.: Яуза; Эксмо, 2009.

22 Следует отметить, что к подготовке сообщений с дезинформацией, отправляемых немцам в ходе радиоигр, в том числе во время Курской битвы, привлекалось руководство Генерального штаба РККА в лице А.М. Василевского, А.И. Антонова, С.М. Штеменко, а также начальника Разведывательного управления Красной Армии Ф.Ф. Кузнецова, и другие руководители СССР, в частности нарком путей сообщения Л.М. Каганович. Обобщенные сводки по переданной немцам дезинформации периодически докладывались лично И.В. Сталину. Передача в эфир дезинформации проводилась только после утверждения Генштабом текстов радиограмм, подготовленных контрразведчиками с учетом почерка каждого агента и легенды о его разведывательных возможностях. *Макаров В., Тюрин А.* Указ. соч.

23 *Астрахан В.И., Павлов В.В., Чернега В.Г., Чернявский Б.Г.* Правительственная электросвязь в истории России. Часть I (1917–1945). М.: Наука, 2001. С. 205.

24 Там же. С. 220–221.

25 Там же. С. 223–224.

26 Там же. С. 226.

27 Там же. С. 231, 250–251.

28 Там же. С. 237.

29 Подробнее об этой аппаратуре можно прочитать в книге: *Бутырский Л.С.* Указ. соч. Гл. 4 и статье: *Ларин Д.А.* Указ. соч.

30 Подробнее о советских системах шифрования и организации шифрованной связи можно прочитать в гл. 4 книги: *Бутырский Л.С., Ларин Д.А., Шанкин Г.П.* Указ. соч.

31 *Мощанский И.Б.* Указ. соч. С. 271–272.

32 Там же. С. 286.

33 *Астрахан В.И., Павлов В.В., Чернега В.Г., Чернявский Б.Г.* Указ. соч. С. 237–238.

34 Там же. С. 250.

35 Там же. С. 252.

36 Там же. С. 256.

37 Там же.

38 Там же. С. 260.

С.А. Желтов

АДАПТАЦИЯ ρ-МЕТОДА ПОЛЛАРДА РЕШЕНИЯ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ К ВЫЧИСЛИТЕЛЬНОЙ АРХИТЕКТУРЕ CUDA

Статья посвящена некоторым аспектам организации параллельных вычислений и использования технологии GPGPU для решения задач дискретного логарифмирования в конечном поле. Основные разделы посвящены обзору адаптации ρ-метода Полларда к параллельным вычислениям на устройствах с гетерогенной архитектурой.

Ключевые слова: параллельные вычисления, дискретное логарифмирование, архитектура CUDA.

Введение

Одной из задач, сложность решения которой определяет стойкость целого ряда асимметричных систем защиты[1], является задача дискретного логарифмирования во вполне определенных алгебраических структурах.

Формально задачу дискретного логарифмирования в конечном поле можно сформулировать следующим образом.

Пусть F_p – кольцо вычетов по простому модулю p.

Для заданных $a, b \in F_p$ требуется найти $x \in F_p$:

$$a^x \equiv b (\mathrm{mod}\, p). \qquad (1)$$

Целое число x, удовлетворяющее (1), называется дискретным логарифмом числа b по основанию a.

Задача относится к классу NP, и на сегодняшний день неизвестны методы ее решения полиномиальной сложности.

Появление полиномиального алгоритма решения рассматриваемой задачи, так же как интенсивное развитие информационных технологий, в частности разработка новых вычислительных архитектур и устройств, могут представлять угрозу информационной безопасности, так как организация эффективных вычислений и их применение может повлечь снижение фактических временны́х затрат на решение задачи и снизить уровень стойкости систем защиты. Риски реализации описанных угроз безопасности можно оценить только по результатам численных экспериментов.

Одним из способов снижения практических временны́х затрат на решение указанного класса вычислительных задач является выбор эффективной модели вычислений на существующих классах архитектур (в том числе и специализированных) вычислительных систем, что требует соответствующей адаптации методов и алгоритмов к выбранной модели вычислений[2]. При использовании вычислительных архитектур в рамках классической модели вычислений А. Тьюринга–Дж. Неймана основным направлением снижения фактических временны́х затрат является организация параллельных вычислений[3].

В настоящее время все большее развитие получает параллельное программирование на графических процессорах (GPU).

I. Технология GPGPU. Архитектура CUDA

GPGPU (General-purpose graphics processing units) – технология использования графического процессора для выполнения расчетов в приложениях для общих вычислений. Это стало возможным благодаря добавлению программируемых шейдерных блоков и более высокой арифметической точности растровых контейнеров, что позволяет использовать потоковые процессоры для неграфических вычислений.

На сегодняшний день технология GPGPU реализована несколькими производителями.

Khronos Group: OpenCL – язык программирования задач общего назначения, связанных с вычислениями на различных графических и центральных процессорах.

Microsoft: DirectCompute – интерфейс программирования приложений, который входит в состав DirectX.

Advanced Micro Devices: AMD FireStream – технология GPGPU, позволяющая реализовывать вычислительные алгоритмы, выполняемые на графических процессорах ускорителей ATI.

Компания Nvidia: CUDA – технология GPGPU, позволяющая реализовывать на языке Си вычислительные алгоритмы, выполняемые на графических процессорах ускорителей GeForce восьмого поколения и старше.

Наиболее удобные средства для организации параллельных вычислений на графических ускорителях предлагает последняя технология.

Nvidia CUDA (Compute Unified Device Architecture) – это архитектура, т. е. совокупность программных и аппаратных средств, которые позволяют производить на графических процессорах компании Nvidia, поддерживающих технологию GPGPU, вычисления общего назначения[4].

Особенностью архитектуры CUDA является блочно-сеточная организация, необычная для многопоточных приложений. Она основана на концепции «одна команда на множество данных» (Single Instruction Multiple Data) или SIMT (Single Instruction, Multiple Thread).

Стоит отметить следующие особенности использования архитектуры CUDA:

- GPU (device) выступает в роли сопроцессора для CPU (host) и представляет собой массив из отдельных вычислительных ядер;
- GPU обладает собственной памятью (device memory);
- GPU способен одновременно обрабатывать множество процессов данных (threads) одним и тем же алгоритмом;
- интерфейс программирования приложений CUDA основан на стандартном языке программирования, например Си, с расширениями;
- масштабируемость CUDA – код запускается на всех устройствах, поддерживающих технологию CUDA.

Основные преимущества CUDA по сравнению с другими реализациями GPGPU обусловлены тем, что эта архитектура спроектирована для эффективного использования неграфических вычислений на GPU и использует язык программирования Си, не требуя переноса алгоритмов в удобный для концепции графического конвейера вид. Данная технология использует разделяемую память, недоступную из графических API (Application Programming Interface), и оптимизированный обмен данными между CPU и GPU.

Рассматриваемая архитектура не использует графические API и лишена недостатков, характерных для других технологий GPGPU.

II. Адаптация ρ-метода Полларда к вычислительной архитектуре CUDA

Проанализируем каждый шаг алгоритма ρ-метода Полларда[5] на возможность применения параллельных вычислений и последующего сокращения фактических затрат на время работы алгоритма при использовании архитектуры CUDA. Наиболее удобным для распараллеливания является шаг 2, который следует разбить на независимые подзадачи, которые возможно было бы выполнить в параллельном режиме. За одну такую подзадачу возьмем задачу генерации наборов (x_i, α_i, β_i) и $(x_{2i}, \alpha_{2i}, \beta_{2i})$ для фиксированного значения индекса i. Так как алгоритм не требует хранения и использования значений, вычисленных на предыдущих этапах шага 2 алгоритма, то нет необходимости обмена данными между различными подзадачами, что также положительно скажется на сокращении времени работы.

С учетом особенностей архитектуры CUDA, модифицированный для параллельной реализации алгоритм ρ-метода Полларда будет выглядеть следующим образом:

Входные данные:

$a, b \in F_p$, p – простое число.

Выход: $x \in F_p$, такое, что $a^x \equiv b (\mathrm{mod}\, p)$, если он существует.

Шаг 1: (выполняется на CPU).

Определение значения N, задание начального параметра $i = 1$.

Шаг 2: (выполняется для значений i, $i + 1$, $i + 2$, ..., $i + N$ параллельно на GPU).

Задание начальных параметров $\alpha_0 = 0, \beta_0 = 0, x_0 = 1$.

Генерация последовательности наборов (x_j, α_j, β_j), где $j = \overline{1, 2i}$ по правилу:

Если $0 < x_i \le \frac{1}{3} p$, то $\alpha_{i+1} = \alpha_i, \beta_i + 1, x_{i+1} = b x_i$.

Если $\frac{1}{3} p < x_i \le \frac{2}{3} p$, то $\alpha_{i+1} = 2\alpha_i, \beta_{i+1} = 2\beta_i, x_{i+1} = x_i^2$.

Если $\frac{2}{3} p < x_i < p$, то $\alpha_{i+1} = \alpha_i + 1, \beta_{i+1} = \beta_i, x_{i+1} = \mathrm{a} x_i$.

Положить: $u \equiv \alpha_{2i} - \alpha_i (\mathrm{mod}\, p - 1)$, $v \equiv \beta_i - \beta_{2i} (\mathrm{mod}\, p - 1)$.

Шаг 3: (выполняется на CPU).

Сравнить полученные в результате шага 2 значения x_i и x_{2i} для значений i, i+1, i+2, ..., i+N.

Если $x_i = x_{2i}$, то перейти к шагу 4.

Если $x_i \neq x_{2i}$, то перейти к шагу 1 и положить $i = i+N$.

Шаг 4: (выполняется на CPU).

Если $v = 0$, то алгоритм завершает работу.

Если $v \neq 0$, то вычислить НОД $d = (v, p-1) = vv + (p-1)\mu$.

Шаг 5: (выполняется на CPU).

Вычислить x:

Если $d = 1$, то $x = uv \pmod{p-1}$.

Если $d \neq 1$, то $x = \dfrac{uv + \omega\,(p-1)}{d}$, $\omega = \overline{1, d}$.

Число N – это количество параллельно выполняющихся подзадач. Это число зависит от конкретного графического ускорителя и определяется на начальном этапе работы программы.

Количество вычисляемых наборов на каждом последующем этапе второго шага алгоритма увеличивается. В параллельной реализации все операции выполняются одновременно, и шаг 2 будет завершен, когда вычислится набор с наибольшим индексом. В силу вышесказанного время выполнения второго шага алгоритма равно времени генерации набора с максимальным индексом, т. е. для параллельного вычисления k штук наборов с индексами 1, 2, ..., k будет затрачено то же время, что и на генерацию одного набора с индексом k при последовательных вычислениях. При реализации на CPU необходимо вычислить $k + k^2$ штук наборов.

III. Экспериментальная апробация

Для проведения численных экспериментов ρ-метод Полларда был программно реализован в классическом варианте для последовательного исполнения на CPU, на стандартном языке Си и выполнялся на центральных процессорах различных мощностей. Модифицированный к архитектуре CUDA, параллельный алгоритм ρ-метода Полларда программно реализован на расширении языка Си для CUDA и выполнялся на различных графических ускорителях компании Nvidia.

Для проведения численных экспериментов были задействованы следующие технологические платформы CPU:

- Intel core i5-2400;
- Intel Core 2 Duo E7500.

И GPU компании Nvidia:
- GeForce GTX 560;
- GeForce 9600

под управлением операционной системы Windows 7. Результаты приведены в табл. 1.

Таблица 1

Результаты вычислительных экспериментов

p	бит	Время работы, с.			
		Nvidia GeForce 9600	Nvidia GeForce GTX 560	Intel Core 2 Duo	Intel core i5-2400
7	3	0,032	0,041	0,028	0,016
13	4	0,031	0,040	0,028	0,014
41	5	0,032	0,047	0,030	0,016
61	6	0,032	0,042	0,031	0,016
113	7	0,031	0,042	0,029	0,015
197	8	0,030	0,041	0,031	0,016
379	9	0,033	0,038	0,032	0,015
659	10	0,032	0,045	0,035	0,016
1153	11	0,032	0,039	0,031	0,016
2551	12	0,032	0,042	0,046	0,019
6961	13	0,034	0,040	0,047	0,031
11719	14	0,033	0,043	0,031	0,031
23159	15	0,034	0,041	0,047	0,047
61001	16	0,033	0,045	0,141	0,078
67651	17	0,032	0,047	0,156	0,109
921637	20	0,066	0,047	1,453	0,936
6878407	23	0,132	0,094	11,047	7,110
88004533	27	0,288	0,203	84,343	50,716
926403853	30	0,349	0,282	109,265	56,320

Зависимость времени работы программных реализаций для центрального и графических процессоров от размерности модуля p представлены на следующих графиках (рис. 1, 2).

Стоит отметить, что при использовании более мощных GPU устройств или специализированных решений Nvidia (Quadro и Tesla) следует ожидать дальнейшего роста производительности в несколько раз и снижения временны́х затрат еще на несколько порядков.

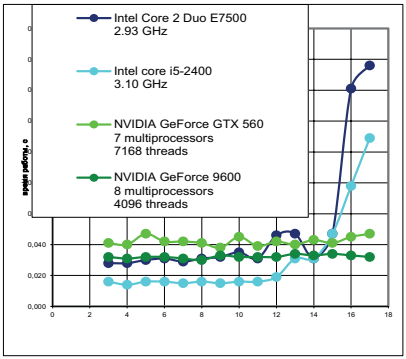


Рис. 1. Зависимость времени работы от размерности модуля ($p<17$)

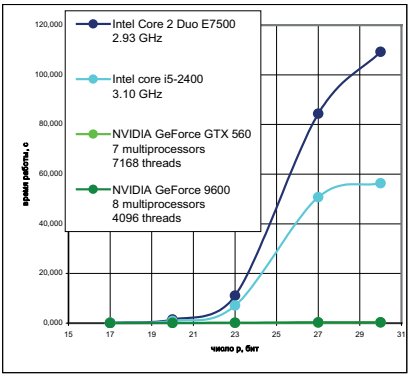


Рис. 2. Зависимость времени работы от размерности модуля ($p\geqslant 17$)

Выводы

Анализ вычислительных операций ρ-метода Полларда показал, что алгоритм обладает выраженным свойством параллелизма данных, так как одни и те же операции могут выполняться сразу над несколькими элементами из различных наборов (x_i, α_i, β_i), эти значения могут обрабатываться независимо на разных вычислительных устройствах, что подходит для эффективной параллельной реализации на архитектуре CUDA и позволяет сократить время вычислений.

Результаты числовых экспериментов показали, что ρ-метод Полларда допускает эффективную параллельную реализацию с использованием вычислений на GPGPU компании Nvidia. Распараллеливание вычислений при решении задачи дискретного логарифмирования ρ-методом Полларда дает сокращение фактических временны́х затрат до двух порядков относительно последовательной реализации.

Стоит отметить, что на практике в системах защиты используются ключи не менее 512 бит, а программные средства CUDA не имеют реализации библиотеки для работы с «большими» числами. Один из способов организации вычислений с «длинными» числами, которые выходят за диапазон значений стандартных типов данных современных языков программирования, описан автором в одной из работ[6].

Автор выражает глубокую благодарность проф. А.Е. Барановичу за ценные рекомендации и помощь при проведении исследований.

Примечания

1 См: *Смарт Н.* Криптография. М.: Техносфера, 2006. 528 с.

2 См.: *Баранович А.Е.* Введение в предметно ориентированные анализ, синтез и оптимизацию элементов архитектур потоковых систем обработки данных (Introduction in the object-oriented analysis, synthesis and optimization of elements of architecture data flow processing systems) [Электронный ресурс] 3-е изд., стереотип., испр. Электрон. дан. [М., НТЦ «Информрегистр», 2010].

3 См.: *Воеводин В.В., Воеводин Вл.В.* Параллельные вычисления. СПб.: БХВ-Петербург, 2002. 600 с.

4 См.: *Боресков А.В., Харламов А.А.* Основы работы с технологией CUDA. М.: ДМК Пресс, 2010. 232 с.

5 См.: *Guan D. J.* Pollard's Algorithm for Discrete Logarithm [Электронный ресурс] URL: http://guan.cse.nsysu.edu.tw/note/pollard.pdf (дата обращения: 30.04.2013).

6 *Желтов С.А.* Реализация арифметических операций с «длинными» числами на устройствах GPGPU // Вопросы защиты информации. 2012. № 3. С. 2–4.

В.Р. Григорьев, В.С. Кузнецов

АДАПТАЦИЯ РОЛЕВОЙ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА В СИСТЕМАХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Предложен подход к адаптации ролевой модели разграничения доступа применительно к системам облачных вычислений. Рассмотрены 3 модели развертывания облачной инфраструктуры: частное облако, публичное облако и гибридное облако. Расширение возможности распространения базовой модели разграничения доступа на облачные вычисления строится на основе предложенной модели угроз облачной системы.

Ключевые слова: ролевая модель разграничения доступа, частное облако, публичное облако, гибридное облако, облачные вычисления, модель угроз.

Введение

Актуальность облачных вычислений связана со снижением затрат, масштабируемостью и гибкостью архитектуры информационных технологий.

Облачные вычисления – это смена парадигмы, которая обеспечивает поддержку вычислений с использованием Интернета. Сервис облачных вычислений состоит из высокооптимизированных и виртуализированных центров обработки данных, обеспечивающих предоставление различных программных, аппаратных и информационных ресурсов, когда их использование оказывается необходимым. Широкое практическое внедрение облачных вычислений в настоящее время во многом связано с отсутствием механизмов гарантированной защиты информации, обрабатываемой в облаках.

На нынешнем этапе развития облачных вычислений выявлен ряд уязвимостей, связанных не только и не столько с классически-

ми угрозами для распределенных информационных систем, но и с принципиально новыми угрозами, порожденными спецификой виртуализации[1]. Организация вычислительных процессов в информационной системе на основе механизмов виртуализации предоставляет нарушителю больше возможностей, чем в классической распределенной архитектуре информационной системы предыдущего поколения. Отсюда возникает необходимость разработки новых подходов к анализу уязвимостей виртуальных сред, которые, в свою очередь, во многом опираются на выбранную для защиты политику безопасности. Возникает вопрос о выборе такой политики безопасности, которая бы наиболее адекватно соответствовала характеру обработки информации в виртуализированных ресурсах облачных вычислений.

Ролевая модель безопасности: особенности и преимущества

Следует отметить, что существующие теоретические модели политик безопасности слабо приспособлены к формализации проблем защиты, которые возникают в облачных вычислениях.

В настоящее время появляются некоторые формализованные подходы построения политик безопасности применительно к области облачных вычислений на основе имеющихся наработок для традиционных моделей разграничения доступа[2,3]. Так, например, в статье[4] предложен вариант адаптации для облачных систем наиболее распространенной теоретической модели мандатного доступа Белла–ЛаПадула (МБЛ). Однако известно, что при использовании МБЛ в контексте практического проектирования и разработки реальных компьютерных систем возникает ряд технических вопросов при построении политик безопасности для конкретных типов систем, т. е. на менее абстрактном уровне рассмотрения.

Так, например, функционирование системного администратора подразумевает выполнение в системе таких критических операций, как добавление и удаление пользователей, восстановление системы после аварий, установка программного обеспечения, устранение ошибок и т. п. Очевидно, что такие операции не вписываются в МБЛ, что означает невозможность осуществления правильного администрирования без нарушения правил данной модели.

Одним из потенциальных кандидатов для создания политики безопасности для разграничения доступа к ресурсам облачных вычислений является модель контроля доступа, базирующаяся на ролях[5].

Ролевая модель безопасности (также называемая ролевым контролем доступа) построена на условии аутентификации пользователей, то есть на процессе идентификации пользователей. Когда пользователь идентифицирован, ему назначаются роли и разрешения.

Модель контроля доступа, базирующаяся на ролях, наиболее естественным образом соответствует политикам безопасности, принятым в различных организациях, позволяет организовать такие особенности политик безопасности, как иерархия ролей (статических, динамических) и операционное разделение обязанностей[6].

Известно, что при применении дискреционного или мандатного контроля доступа информация принадлежит создавшему ее пользователю (принципиальным является то, кто имеет доступ по чтению и по записи к информации). Напротив, контроль доступа, базирующийся на ролях (role based access control, КДБР), рассматривает всю информацию, обрабатывающуюся в вычислительной системе организации, как принадлежащую данной организации.

В системе КДБР пользователи не могут передавать права на доступ к информации другим пользователям, что является фундаментальным отличием КДБР от дискреционного и мандатного доступа. Таким образом, КДБР основывается на принятии решения о доступе на основе информации о функции, которую пользователь выполняет внутри данной организации на основании своей роли.

Определение членства и распределение полномочий роли в КДБР (в отличие от дискреционного доступа) зависит не от системного администратора, а от политики безопасности, принятой в системе. Роль можно понимать как множество действий, которые пользователь или группа пользователей может использовать в контексте организации. Понятие роли включает описание обязанностей, ответственности и квалификации. Функции распределяются по ролям администратором системы. Доступ к роли также определяется администратором системы.

Ролевую политику безопасности нельзя отнести ни к дискреционным, ни к мандатным, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов.

Поэтому ролевая модель представляет собой совершенно особый тип политики, основанной на компромиссе между гибкостью управления доступом, характерной для дискреционных моделей, и жесткостью правил контроля доступа, присущей мандатным моделям.

В ролевой модели классическое понятие «субъект» замещается понятиями «пользователь» и «роль». Пользователь – это человек, работающий с системой и выполняющий определенные служебные обязанности. Роль – это активно действующая в системе абстрактная сущность, с которой связан ограниченный, логически связанный набор полномочий, необходимых для осуществления определенной деятельности. Самым распространенным примером роли является присутствующий почти в каждой системе административный бюджет, который обладает специальными полномочиями и может использоваться несколькими пользователями.

Ролевая политика распространена очень широко, потому что она, в отличие от других более строгих и формальных политик, очень близка к реальной жизни. Ведь на самом деле работающие в системе пользователи действуют не от своего личного имени – они всегда осуществляют определенные служебные обязанности, т. е. выполняют некоторые роли, которые никак не связаны с их личностью.

Ролевая политика позволяет распределить полномочия между этими ролями в соответствии с их служебными обязанностями: роль администратора наполняется специальными полномочиями, которые позволяют ему контролировать работу системы и управлять ее конфигурацией, роль менеджера баз данных позволяет осуществлять управление сервером баз данных, а права простых пользователей ограничиваются минимумом, необходимым для запуска прикладных программ.

Кроме того, количество ролей в системе может не соответствовать количеству реальных пользователей – один пользователь, если на нем лежат различные обязанности, требующие различных полномочий, может выполнять (одновременно или последовательно) несколько ролей, а несколько пользователей могут пользоваться одной и той же ролью, если они выполняют одинаковую работу.

При использовании ролевой политики управление доступом осуществляется в две стадии: во-первых, для каждой роли указывается набор полномочий, представляющий набор прав доступа к объектам, и, во-вторых, каждому пользователю назначается список доступных ему ролей.

Полномочия назначаются ролям в соответствии с принципом наименьших привилегий, из которого следует, что каждый пользователь должен обладать только минимально необходимым для выполнения своей работы набором полномочий.

В отличие от других политик ролевая политика управления доступом практически не гарантирует безопасность с помощью

формального доказательства, а только определяет характер ограничений, соблюдение которых и служит критерием безопасности системы. Такой подход позволяет получать простые и понятные правила контроля доступа, которые легко могут быть применены на практике, но лишает систему теоретической доказательной базы. Далее предлагается рассмотреть принципы составления простых правил ролевого управления доступом, которые могут быть использованы в качестве основы формирования политики безопасности для некоторых типов облачных вычислений.

Модель ролевого разграничения доступа для облачных вычислений

В качестве отправной точки для исследования вопроса возможности расширения применимости модели ролевого разграничения доступа к облачным вычислениям выберем 3 модели развертывания «облаков»[7]:

- *Частные облака.* Предназначены для исключительного использования одной организацией и обычно контролируются, управляются и хостируются частными центрами данных. Хостинг и управление частными облаками могут быть переданы на аутсорсинг внешнему сервис-провайдеру, но частное облако остается в исключительном пользовании одной организации.
- *Публичные облака.* Используются многими организациями (пользователями) совместно, обслуживаются и управляются внешними сервис-провайдерами.
- *Гибридные облака.* Появляются, когда организация использует и частное, и публичное облака для одного и того же приложения, чтобы воспользоваться преимуществами обоих. Например, при «ливневом» сценарии организация в случае стандартной нагрузки на приложение пользуется частным облаком, а когда нагрузка пиковая, например, в конце квартала или в праздничный сезон, задействует потенциал публичного облака, впоследствии возвращая эти ресурсы в общий пул, когда они больше не нужны.

1. Модель ролевого разграничения доступа

Классическая ролевая модель[8] разграничения доступа имеет следующие основные элементы:

U – множество пользователей;
R – множество ролей;
P – множество полномочий на доступ к объектам, представленное, например, в виде матрицы прав доступа;
S – множество сеансов работы пользователей с системой.

В качестве критерия безопасности ролевой модели используется следующее правило: система считается безопасной, если любой пользователь системы, работающий в сеансе S, может осуществлять действия, требующие полномочия p_1 только в том случае, если они ему разрешены.

PA: R – > 2^P – функция, задающая для каждой роли множество прав доступа, при этом для каждого права доступа p∈P существует роль r∈R такая, что p∈PA(r);

UA: S – >2^R – функция, задающая для каждого пользователя множество ролей, на которые он может быть авторизован;

user: S – >U – функция, задающая для каждой сессии пользователя, от имени которого она активизирована;

roles: S – >2^R – функция, задающая для пользователя множество ролей, на которые он авторизован в данной сессии, при этом в каждый момент времени для каждой сессии s∈S выполняется условие roles(s) < UA(user(s)).

Возможно существование ролей, на которые не авторизован ни один пользователь.

В базовой модели ролевого управления доступом предполагается, что множества U, R, P и функции PA, UA не изменяются с течением времени.

Множество ролей, на которые авторизуется пользователь в течение одной сессии, модифицируется самим пользователем. При этом отсутствуют механизмы, позволяющие одной сессии активизировать другую сессию. Все сессии активизируются только пользователем.

Следующим шагом построим модель угроз, которая позволит нам расширить, с учетом специфики систем облачных вычислений, классический набор элементов модели ролевого разграничения доступа.

2. Модель угроз

При построении модели угроз системы облачных вычислений становится ясно, что точки приложения угроз выходят за рамки классической тройки: конфиденциальность, целостность и доступность. Формализуем модель угроз для облачной системы.

1. *Конфиденциальность*. Классический элемент модели угроз, угроза конфиденциальности данных, может принять множество форм, например, *внутренние нарушители*: данная угроза очевидна для большинства организаций. В качестве иллюстрации: провайдер может не скрывать способы предоставления доступа к физическим и виртуальным объектам, способы реализации контроля сотрудников или специфику анализа сообщений безопасности. Наиболее актуальной угрозой в условиях распределенной облачной системы являются *неизвестные риски*, проще говоря, пользователь не имеет представления о том, каким образом обрабатываются его данные в облаке.

2. *Целостность*. Очевидным примером может послужить уничтожение данных при отсутствии актуального бэкапа. Потеря нескольких записей из большого массива данных может привести к его полной нечитаемости. Потеря ключа шифрования равносильна утрате данных, зашифрованных на нем. Проще говоря, неавторизованные элементы системы не должны иметь никакого доступа к критичным участкам данных.

3. *Доступность*. Угроза доступности может быть реализована посредством атаки, эксплуатирующей *небезопасные интерфейсы и API*. Провайдеры облачных вычислений предоставляют набор программных интерфейсов для взаимодействия с их продуктом. Посредством таких интерфейсов реализуется настройка, управление, мониторинг, синхронизация. В итоге доступность облачных сервисов упирается в безопасность базовых API.

4. *Функциональная устойчивость*. В ситуации с облачными вычислениями данный термин приобретает несколько иной смысл. Например, возможны такие атаки, как *кража аккаунта или сервиса*[9]. Идея не нова. Атаки наподобие фишинга, фрода или эксплойтов используемого ПО не теряют актуальности. В условиях облачной системы злоумышленник разом получает доступ ко всем данным/ресурсам, находящимся в облаке.

5. *Управление*. Атаки, эксплуатирующие недочеты в данной части системы, могут принять такую форму, как *некорректное или незаконное использование облачных систем*. IaaS-провайдеры предлагают потребителям иллюзию неограниченных ресурсов, часто сопровождаемую «упрощенной» процедурой регистрации, когда любой человек с валидной кредитной карточкой имеет возможность зарегистрироваться в системе и мгновенно получить доступ к предлагаемым услугам. Некоторые провайдеры предоставляют бесплатный тривиальный период использования своих услуг. Вышесказанное в сочетании с анонимным доступом к сер-

висам «развязывает руки» спамерам, разработчикам вредоносного кода и остальным криминальным элементам. PaaS-провайдеры также страдают от большинства перечисленных проблем. Таким образом, под некорректным или незаконным использованием облачных сервисов подразумевается использование их с целью DDOS, взлома паролей, реализации распределенных атак, создания ботнетов, взлома CAPTCHA. Также в данном пункте следует учитывать управление гипервизорами, жизненным циклом виртуальных объектов, а также *проблемы общедоступной среды*, потому как IaaS-вендоры предоставляют свои сервисы как динамически изменяемую инфраструктуру. Очень часто базовые компоненты, составляющие эту инфраструктуру (CPU кэш, GPU и т. п.), не приспособлены для реализации требований строгой изоляции, которые актуальны в многозадачной среде.

Построенная модель угроз позволяет выделить участки системы облачных вычислений, не охваченные классическими положениями модели ролевого разграничения доступа. Наличие подобных участков объясняется спецификой облачных вычислений как распределенной системы.

3. Расширение модели ролевого разграничения доступа

Построим расширение базовой ролевой модели для использования ее в условиях облака с учетом построенной выше модели угроз.

Во-первых, введем параметр *атрибут*, целесообразность которого может быть понятна из следующего примера: пользователю делегирована роль «загрузить данные» в облако. Данное действие возможно и логично для всех пользователей, но размеры вносимой информации могут быть различны. Можно ввести несколько ролей: «загрузить 1 Гб», «загрузить 2 Гб» и т. д. При подобном подходе задача администрирования системы будет значительно усложняться с течением времени. Таким образом, *атрибут* есть свойство пользователя либо роли. При передаче прав делегирования роли субъекту требуется указать, какие из атрибутов этой роли субъект имеет право изменять и как. *Атрибут* есть некое уникальное свойство роли или пользователя, являющееся численным значением. Из соображений безопасности при делегировании он либо остается неизменным, либо уменьшается. Данный параметр актуален в условиях всех моделей развертывания из п. 1. Таким образом, наш пример может выглядеть так:

C – облако, Sec – контроллер безопасности системы, C.user1 – обычный пользователь, C.user2 – привилегированный пользователь, C.upload – роль на право загрузки, C.size – атрибут облака, накладывающий ограничение на объем загрузки;

- присвоим право пользователю загружать ограниченный объем информации: (C.user1 → C.upload with C.size=1)Sec (операцию делегирования контролирует наш контроллер безопасности системы);
- присвоим право привилегированному пользователю загружать неограниченный объем информации: (C.user1 → C.upload with C.size=0)Sec (0 – значит, что ограничений нет).

Во-вторых, введем понятие «*период делегирования*», т. е. на какой срок делегируются те или иные полномочия. В качестве иллюстрации необходимости подобного понятия выступает идея облака, которая подразумевает частую смену и большое число пользователей. Также периодическое обновление полномочий имеет смысл для усиления безопасности. Данный параметр актуален в условиях всех моделей развертывания. Таким образом, наш пример может выглядеть так:

C – облако, Sec – контроллер безопасности системы, C.user1 – обычный пользователь, C.user2 – привилегированный пользователь, C.upload – роль на право загрузки, C.size – атрибут облака, накладывающий ограничение на объем загрузки;

- присвоим право пользователю загружать ограниченный объем информации: (C.user1 → C.upload<дата истечения полномочий> with C.size=1)Sec;
- присвоим право привилегированному пользователю загружать неограниченный объем информации: (C.user1 → C.upload<дата истечения полномочий> with C.size=0)Sec.

В-третьих, поскольку наше облако может быть в ведении организации, чьи филиалы распределены по большой территории, а доступ к ресурсам одного филиала необходимо предоставить другому, то при работе с элементами облака системе необходимо знать, какому филиалу они принадлежат. Для этого каждый элемент облака должен нести информацию о том, какому филиалу он принадлежит и как это проверить. Набор следующих параметров элемента облака, используемых при работе с ним, назовем *облачными параметрами*:

- сервер филиала, регулирующий доступ;
- дополнительные правила, налагаемые данным узлом облака.

Данный параметр актуален в условиях *гибридного облака*, в котором происходит смешивание узлов с различной степенью доверия. Таким образом, наш пример может выглядеть так:

C – облако, Sec – контроллер безопасности системы, C.user1 – обычный пользователь, C.user2 – привилегированный пользователь, C.upload – роль на право загрузки, C.size – атрибут облака, накладывающий ограничение на объем загрузки, C.cp – облачные параметры;

- даем право пользователю загружать ограниченный объем информации: ((C.user1 → C.upload<дата истечения полномочий> with C.size=1)<C.cp>)Sec;
- даем право привилегированному пользователю загружать неограниченный объем информации: ((C.user1 → C.upload<дата истечения полномочий> with C.size=0)<C.cp>)Sec.

4. Заключение

В данной статье для построения формализованных процедур разграничения доступа в облачных вычислениях предложено использовать модель ролевого разграничения доступа. С учетом введенных параметров наиболее интересным объектом для реализации адаптированной модели ролевого разграничения доступа представляется гибридное облако, которое образуют узлы, обрабатывающие информацию с различными грифами конфиденциальности. Также показано, что технология управления доступом на основе ролей обладает значительным потенциалом в плане адаптации и гибкости перестройки, чтобы смоделировать любую другую модель управления доступом. Предложенная модель, безусловно, не претендует на решение всех проблем в виртуализированной среде облачных вычислений, однако обладает достаточно универсальными механизмами разграничения доступа, которые требуют дальнейших теоретических и прикладных исследований.

Примечания

[1] См.: *Fang Liu, Jin Tong, Jian Mao, Bohn R.B., Messina J.V., Badger M.L., Leaf D.M.* NIST Cloud Computing Reference Architecture [Электронный ресурс] // National Institute of Standards and Technology. URL: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505; *Hogan M.D., Fang Liu, Sokol A.W., Tong Jin.* NIST Cloud Computing Standards Roadmap [Электронный ресурс] // National Institute of Standards and Technology. URL: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024.

[2] См.: *Сергеев Ю.К.* Использование технологий виртуализации для защиты информации // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2009. № 10.

[3] См.: *Качко А.К.* Формализованная модель безопасности процесса обработки данных в условиях среды облачных вычислений // Проблемы информационной безопасности. Компьютерные системы. 2012. № 2. С. 14–20.

[4] Там же.

[5] *Девянин П.Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учеб. пособие для вузов. М.: Горячая линия-Телеком, 2011. С. 227–282.

[6] См.: *Баранов А.П., Зегжда Д.П., Зегжда П.Д., Ивашко А.М., Корт С.С.* Теоретические основы информационной безопасности (дополнительные главы): Учеб. пособие. СПб.: Санкт-Петербургский ГТУ, 1998.

[7] См.: *Fang Liu, Jin Tong, Jian Mao, Bohn R.B., Messina J.V., Badger M.L., Leaf D.M.* Op. cit.

[8] См.: *Качко А.К.* Указ. соч.

[9] См.: *Баранов А.П., Зегжда Д.П., Зегжда П.Д., Ивашко А.М., Корт С.С.* Указ. соч.

А.С. Платонова

МАТЕМАТИЧЕСКАЯ И ПРОЦЕДУРНАЯ МОДЕЛИ ФОРМИРОВАНИЯ МНОГОПАРАМЕТРИЧЕСКОЙ ОЦЕНКИ УЧАЩЕГОСЯ

Статья посвящена разработке математической модели многопараметрической оценки учащегося и процедурной модели ее формирования в рамках проектирования информационной системы многопараметрического контроля образовательной деятельности на примере среднего образования. Предлагаемые модели отличаются от существующих тем, что позволяют автоматизировать контроль достижений учащихся с учетом 12 групп контролируемых параметров и 80 результатов контроля по этим параметрам. Построение моделей является одним из шагов для совершенствования методологии проектирования информационного обеспечения информационных систем контроля образовательной деятельности в соответствии с современными требованиями.

Ключевые слова: многопараметрическая оценка учащегося, математическая модель, процедурная модель.

Задача повышения качества функционирования информационных систем контроля образовательной деятельности в рамках субъекта РФ является актуальной на сегодняшний день. Одна сторона этого вопроса, связанная с предметной областью, была актуализирована премьером РФ Д.А. Медведевым, Министерством образования РФ, усилия которых в сфере общего образования были направлены на воплощение в жизнь национальной образовательной инициативы «Наша новая школа». Вторая сторона – с необходимостью информационным системам данного класса отвечать одновременно двум современным требованиям.

1. К содержанию контроля. Задается федеральными государственными образовательными стандартами. В соответствии с ними

контролю подлежат несколько групп результатов образовательной деятельности, а именно: предметные, надпредметные и личностные. В свою очередь, каждая группа параметров – с точки зрения морфологии и иерархической соподчиненности – имеет сложную структуру. Увеличение контролируемых параметров и важность мониторинга в рамках субъекта РФ приводят к необходимости увеличивать количество автоматизируемых функций, то есть повышать функциональную полноту информационной системы[1].

2. К качеству функционирования самих систем. Одной из характеристик качества функционирования информационной системы является ее производительность: реактивность, как время между предъявлением системе входных данных и появлением соответствующей выходной информации, либо продуктивность, как объем информации, обрабатываемой системой в единицу времени[2]. С точки зрения реактивности информационная система контроля образовательной деятельности должна обрабатывать информацию о результатах контроля по всем учащимся области и предоставлять итоговый результат (в данном случае здесь имеется в виду многопараметрическая оценка учащегося) в срок, не больший, чем предоставление результатов единого государственного экзамена по области, а именно не более 8–10 дней. Возрастание числа контролируемых параметров неизбежно приводит к росту количества записей в базе данных и увеличению времени их обработки до неприемлемого значения. Для уменьшения времени формирования оценки была оптимизирована структура хранения результатов контроля. Выявлены и введены в структуру базы данных дополнительные семь таблиц[3].

В рамках проектирования информационной системы многопараметрического контроля образовательной деятельности были построены: информационная модель контроля образовательной деятельности по многим параметрам, модели описания информационных процессов в системе многопараметрического контроля образовательной деятельности, концептуальная модель информационного обеспечения информационной системы. На следующем этапе потребовалось математически описать многопараметрическую оценку учащегося и разработать алгоритм ее формирования.

Для формализованного описания многопараметрической оценки учащегося выделены и обозначены входные данные, получаемые по итогам того или иного этапа контроля (от X_1 до X_{12}). Определены промежуточные данные, получаемые в результате первичной обработки результатов контроля и хранящиеся в дополнительных таблицах (от Z_1 до Z_7) (табл. 1). Определены выходные данные,

являющиеся элементами многопараметрической оценки (от Y_1 до Y_{80}). Между входными, промежуточными и выходными данными выявлены аналитические зависимости.

Таблица 1

Промежуточные результаты многопараметрического контроля (суммарные баллы)

Обозначение	Расшифровка	Расчетная формула
1	2	3
Z_1	Тестовые задания	$Z_1 = \sum_{i=1}^{n} X_{1i}$, где X_{1i} – балл за i-й вопрос тестового задания; n – количество вопросов в тестовых заданиях
Z_2	Задачи	$Z_2 = k_s \sum_{i=1}^{n} X_{2i}$, где X_{2i} – балл за i-й этап задачи; k_s – поправочный коэффициент, учитывающий сложность задачи, $k_s \in [0{,}5; 1; 2]$; n – количество этапов в задачах
Z_3	Контрольные работы	$Z_3 = \sum_{i=1}^{n} Z_{2i}$, где Z_{2i}– балл за i-ю задачу в контрольной работе; n – количество задач в контрольных работах
Z_4	Лабораторные работы	$Z_4 = \sum_{i=1}^{n} X_{4i}$, где X_{4i} – балл за i-й этап лабораторной работы; n – количество этапов в лабораторных работах
Z_5	Критерии лабораторных работ	$Z_5 = \sum_{i,j=1}^{n,m} X_{4ij}$, где X_{4ij} – балл за i-й этап лабораторной работы по j-му критерию; n, m – количество этапов и критериев в лабораторных работах соответственно

Окончание табл. 1

1	2	3
Z_6	Компоненты структурных единиц	$Z_6 = \sum_{i,j=1}^{n,m} X_{1ij}$, где X_{1ij} – балл за i-й вопрос в тестовых заданиях по j-й структурной единице; n – количество вопросов и структурных единиц в тестовых заданиях соответственно
Z_7	Этапы решения контрольных работ	$Z_7 = \sum_{i,j=1}^{n,m} X_{2ij}$, где X_{2ij} – балл за i-й этап задачи j-го типа этапа; n – количество этапов и типов этапов в задачах соответственно

Многопараметрическая оценка учащегося представляет собой множество, включающее в себя следующие элементы – группы результатов многопараметрического контроля:

$$MPM = \{Y_{11}, Y_{12}, ..., Y_{1p}; Y_{21}, Y_{22}, ..., Y_{2s}; Y_{31}, Y_{32}, ..., Y_{3l}; Y_{41}, Y_{42}, ..., Y_{4v}\}.$$

Здесь 1, 2, 3, 4 – номера групп результатов контроля; p, s, l, ν – количество результатов контроля в группе: $p = 47$, $s = 6$, $l = 18$, $v = 9$. Y_{11} – коэффициент усвоения теоретического материала: $Y_{11} = Z_1/B_1$, где Z_1 – суммарный балл, набранный учащимся за выполнение тестовых заданий; B_1 – максимально возможный балл, который учащийся мог набрать за выполнение тестовых заданий; $Y_{11} \in [0; 1]$; Y_{12} – уровень усвоения теоретического материала, зависящий от соответствующего коэффициента:

$$Y_{12} = \begin{cases} \text{низкий}, 0{,}00 \leqslant Y_{11} \leqslant 0{,}20, \\ \text{ниже среднего}, 0{,}21 \leqslant Y_{11} \leqslant 0{,}40, \\ \text{средний}, 0{,}41 \leqslant Y_{11} \leqslant 0{,}60, \\ \text{выше среднего}, 0{,}61 \leqslant Y_{11} \leqslant 0{,}80, \\ \text{высокий}, 0{,}81 \leqslant Y_{11} \leqslant 1{,}00; \end{cases}$$

Y_{13} – коэффициент усвоения физических понятий:

$$Y_{13} = \left(\sum_{i=1}^{n} X_{11i} + \sum_{i=1}^{n} X_{12i} \right) \Big/ (B_1 + B_2),$$

где X_{11i}, X_{12i} – баллы за i-е ответы на вопросы по определению физических понятий и по обоснованию необходимости введения физического понятия соответственно; B_1 и B_2 – максимально возможные баллы, которые мог набрать учащийся за ответы на вопросы по компонентам первой и второй структурных единиц соответственно; n, m – количество вопросов по первой и второй структурным единицам.

Y_{14}, Y_{15} – результаты ответа на вопросы по определению физических понятий и по обоснованию необходимости введения физического понятия соответственно, например,

$$Y_{14} = \{Y_{141}, Y_{142}, ..., Y_{14N}\}.$$

Элементы вектора могут принимать значения 0 или 1 в зависимости от того, ответил ученик на вопрос или нет:

$$Y_{14i} = \begin{cases} 0, X_{11i} = 0 \\ 1, X_{11i} > 0 \end{cases}.$$

В завершение процесса математического моделирования был выделен последний элемент многопараметрической оценки, а именно Y_{49} – уровень воспитанности, зависящий от общего балла по воспитанности Y_{48}:

$$Y_{49} = \begin{cases} \text{низкий}, 0{,}00 \leqslant Y_{48} \leqslant 1{,}00, \\ \text{ниже среднего}, 1{,}01 \leqslant Y_{48} \leqslant 2{,}00, \\ \text{средний}, 2{,}01 \leqslant Y_{48} \leqslant 3{,}00, \\ \text{выше среднего}, 3{,}01 \leqslant Y_{48} \leqslant 4{,}00, \\ \text{высокий}, 4{,}01 \leqslant Y_{48} \leqslant 5{,}00. \end{cases}$$

Выделенные результаты многопараметрического контроля сведены в иерархическом шаблоне, являющемся формой представления МПОУ (рис. 1).

Многопараметрическая оценка состоит из четырех частей, каждая из которых посвящена подробному описанию результатов контроля по учебным предметам, общеучебным умениям и навыкам, развития и воспитания соответственно. Часть 1 включает в себя несколько разделов, например раздел 1 – «Физика»: в каждом из параграфов описываются результаты усвоения учебного материала по предмету на ученическом, алгоритмическом и творческом уровнях.

Многопараметрическая оценка учащегося

Ф.И.О.: <_____>
Класс: <_____>
Школа: <_____>

Часть 1 Знания и умения по предметам
Раздел 1 Знания и умения по <*ФИЗИКА*>
Обученность О учащегося равна <Y_{46}> – уровень – <Y_{47}>
Параграф 1 Усвоение основных компонентов структуры физических знаний

Коэффициент усвоения теоретического материала $К_{ум}$ равен <Y_{11}> – уровень усвоения теоретического материала $У_{ум}$ – <Y_{12}>.
Коэффициент усвоения физических понятий $К_{п}$ равен <Y_{13}>

Вопрос	Результат
Определение модели объекта или понятия	
<*Вопрос N*> ... <*Вопрос M*>	Y_{141} ... Y_{14N}
Обоснование необходимости введения модели или понятия	
<*Вопрос K*> ... <*Вопрос L*>	Y_{151} ... Y_{15N}

Коэффициент усвоения физических величин $К_{в}$ равен <Y_{5}>

Вопрос	Результат
Словесная формулировка	
<*Вопрос N*> ... <*Вопрос M*>	Y_{121l} ... Y_{121M}
Определительная формула	
<*Вопрос K*> ... <*Вопрос L*>	Y_{122l} ... Y_{122M}

Рис. 1. Фрагмент иерархического шаблона многопараметрической оценки учащегося

Формализация многопараметрической оценки учащегося была продолжена разработкой процедурной модели ее формирования. Полученный алгоритм представлен на рис. 2 и состоит из набора процедур, которые вызываются по мере необходимости и содержат запросы к базе данных на языке SQL. Все обозначения элементов многопараметрической оценки здесь даны в русской транскрипции для лучшего понимания и восприятия схемы. Полученные в результате выполнения запросов данные обрабатываются и используются при построении МПОУ. Формирование оценки начинается с интерпретации результатов контроля усвоения теоретического материала. Начиная с параграфа 1 части 1, вычисляются коэффициенты усвоения основных структурных единиц структуры физических знаний: физических понятий, величин, явлений и законов. Для каждой структурной единицы создается таблица, которая содержит номера тестовых заданий на проверку знания каждого из компонентов структурной единицы, а также результат выполнения заданий в виде знака «+» или «–» («+» – с заданием справился, «–» – с заданием не справился). Затем рассчитывается обученность учащегося по предмету по соответствующей формуле.

В ходе дальнейшего формирования многопараметрической оценки учащегося интерпретируются результаты контроля общеучебных умений и навыков (переход к части 2). Для этого вычисляется средний балл по шкале каждого из общеучебных умений и навыков (ОУН): «Интеллектуальные ОУНы», «Организационные ОУНы», «Коммуникативные ОУНы» и, исходя из этого, определяется группа, к которой относится учащийся, его статус и выдаются индивидуальные рекомендации.

Далее интерпретируются результаты психологического тестирования и диагностики воспитанности (переход к части 3), начиная с таблицы, в которую заносятся уровни развития основных психических процессов. Результаты психологического тестирования, диагностики воспитанности, а также индивидуальные рекомендации добавляются в оценку простым извлечением информации из базы данных, где они хранятся в явном виде. Заканчивается оценка интерпретацией результатов контроля воспитания[4].

Фрагмент процедурной модели формирования МПОУ учащегося представлен на рис. 3.

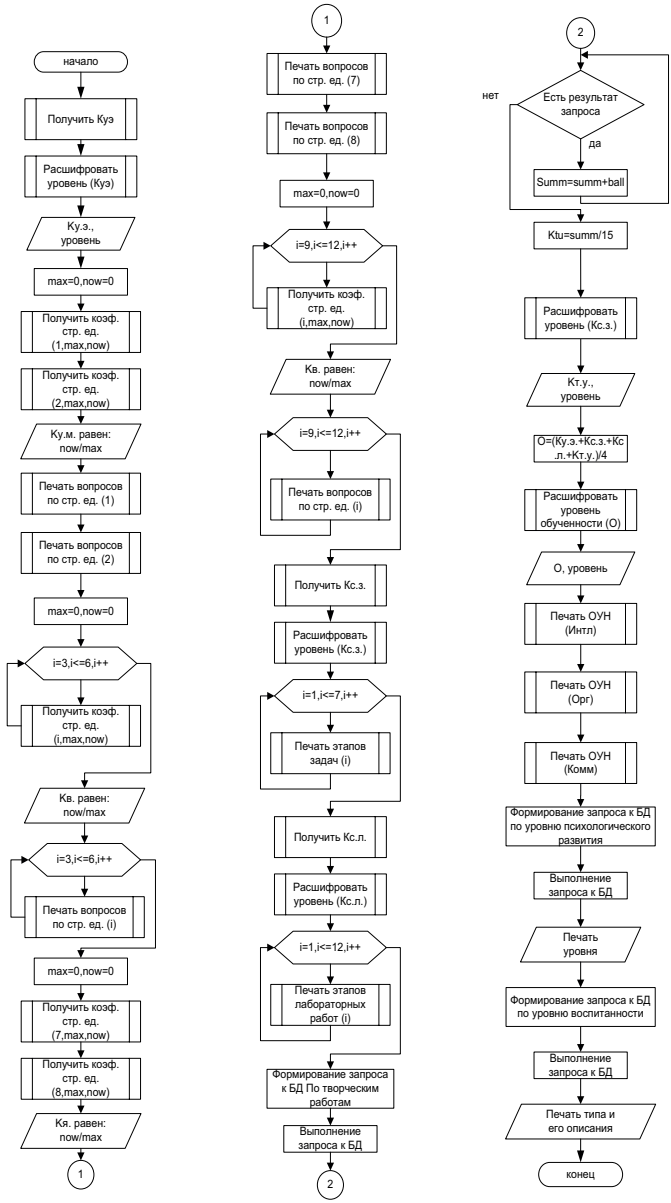


Рис. 2. Процедурная модель формирования многопараметрической оценки

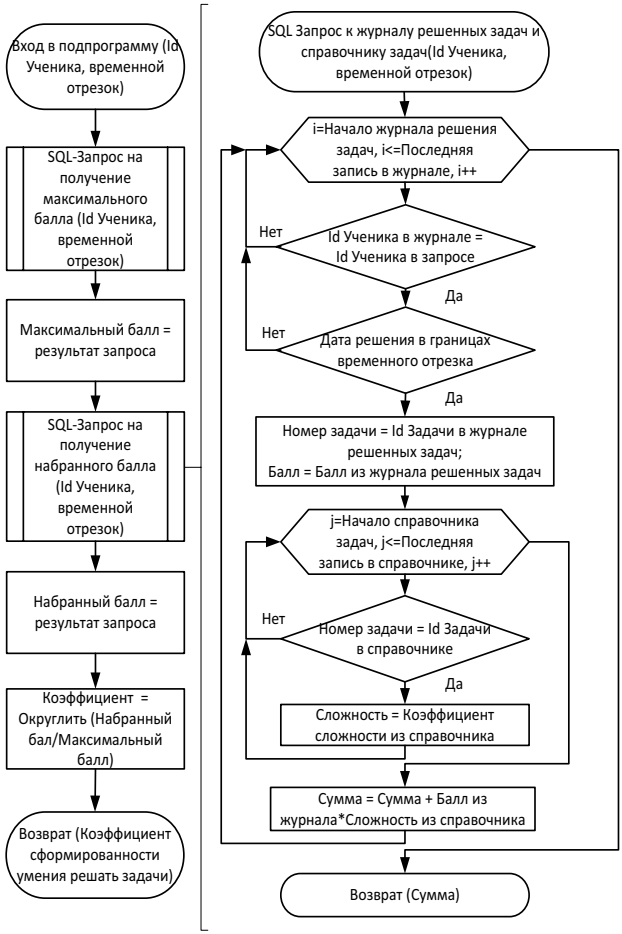


Рис. 3. Фрагмент процедурной модели формирования МПО

Время выполнения представленного на рисунке SQL-запроса напрямую зависит от количества строк в таблице журнала решения задач и справочнике задач. Если бы выборка происходила по таблице с журналом этапов решения задач, то время выполнения запроса было бы в несколько раз больше, так как количество строк в ней выше, а запрос включал бы в себя дополнительные обращения к справочнику этапов.

Разработанная математическая модель представляет собой вектор, элементы которого рассчитываются с использованием выведенных аналитических зависимостей и формируются по запросу пользователя в соответствии с шаблоном. Это позволяет формализованно описать результаты образовательной деятельности с позиции достижений учащегося. Разработанная процедурная модель представляет собой совокупность взаимосвязанных подпрограмм последовательного извлечения информации о результатах контроля из базы данных, описывает процесс заполнения иерархического шаблона многопараметрической оценки и отличается модульной структурой и использованием более простых запросов к таблицам с предварительно рассчитанными результатами контроля в информационном массиве. С помощью созданного алгоритма разработана программа генерирования итоговой информации о многопараметрическом контроле образовательной деятельности. Ближайшей перспективой является обеспечение адаптации предложенного алгоритма под тип пользователя: уровень школы – директор, учитель, психолог, ученик или родитель, уровень города и области – органы управления образованием.

Примечания

[1] См.: *Платонова А.С., Самохин А.В.* Проектирование информационной системы контроля и оценки результатов образовательной деятельности учащихся: архитектура, модель и структура базы данных // Информационные системы и технологии. 2011. № 3. С. 13–21.

[2] См.: Анализ производительности программного обеспечения при помощи математического планирования эксперимента [Электронный ресурс] // Сайт «Хабрахабр». URL: http://habrahabr.ru/post/129346/ (дата обращения: 01.03.2013).

[3] См.: *Платонова А.С.* Проектирование базы данных для информационной системы контроля и оценивания результатов образования // Вестник РГГУ. Серия «Информатика. Защита информации. Математика». 2012. № 14. С. 39–48.

[4] См.: *Платонова А.С.* Алгоритмы и программное обеспечение для информационной системы комплексного оценивания образовательных результатов школьников [Электронный ресурс] // Наука и образование: электрон. науч.-техн. журнал. 2011. № 11. URL: http://technomag.edu.ru/archive.html. (дата обращения: 01.03.2013).

С.М. Иглицкая

ПРОЕКЦИЯ МОДЕЛИ СЕМИОТИКО-ХРОМАТИЧЕСКИХ ГИПЕРТОПОСЕТЕЙ НА ОБЛАСТЬ СИНТЕЗА МУЗЫКАЛЬНОГО ТЕКСТА СТРОГОГО СТИЛЯ

В статье излагается концептуальный подход к построению моделей музыкальных текстов различных стилей на основе универсальной модели информационной составляющей состояний сложных динамических систем. Предложены методы построения моделей полифонического музыкального текста. Описана программная реализация модели одноголосного музыкального текста строгого стиля.

Ключевые слова: текст музыкальный, текст нотный, полифония строгого стиля, k-гиперпространство СХ-гипертопографов, СХ-гипертопосети.

Введение

К числу актуальных задач, лежащих на пересечении предметных областей информатики и теории музыки, относится задача разработки средств автоматизации анализа и синтеза музыкального текста (МТ). Если в сфере цифровой обработки звука в настоящее время достигнуты значительные результаты, то для графического представления музыкальных произведений, кроме обладающих ограниченным набором функций программ нотного набора, подобные средства фактически отсутствуют. Между тем исследование письменного МТ представляется гораздо более перспективным благодаря точности и детерминированности записи, с одной стороны, и историческому преимуществу графического канала передачи информации, с другой стороны.

Можно привести целый ряд прагматических задач, решение которых требует наличия средств автоматической обработки МТ:

• создание программ компьютерного распознавания МТ;

- формирование электронных библиотек нотно-музыкальных ресурсов;
- создание музыкальной поисковой системы;
- идентификация МТ:
  - установление авторства анонимных музыкальных произведений;
  - определение стилистической принадлежности фрагмента МТ;
  - распознавание по нотной записи вида оптимального для исполнения музыкального инструмента;
- изучение характеристик канала музыкальной коммуникации:
  - исследование канала связи, использующего МТ, его пропускной способности, возможностей и методов передачи по нему различных видов информации, не исключая секретной;
- анализ особенностей семантической музыкальной коммуникации коллектива антропоморфных интеллектуальных систем;
- исследование прагматического потенциала музыкальной информации;
- формализация и упорядочение терминологического аппарата музыковедения;
- разработка новых подходов к анализу музыкального произведения;
- формулировка критериев объективной оценки художественной ценности музыкального произведения или его исполнения.

Построение теоретического базиса для решения перечисленных задач необходимым образом связано с характеризацией информационной составляющей МТ и, следовательно, с выбором моделей представления информации и их адаптацией к специфике изучаемых явлений и процессов. Проведенный обзор состояния предметной области показал, что постановка цели в подобном виде в исследованиях по интересующей нас тематике не производилась.

Доступные источники можно классифицировать следующим образом:

1) Работы гуманитарной направленности.

Данный класс работ не представляет значительного интереса в контексте математического исследования, однако содержащаяся в них индуктивная база фактов позволяет выявить некоторые закономерности, которые могут быть положены в основу построения моделей информационной составляющей МТ.

В частности, в статьях М.Г. Арановского[1], Б.М. Гаспарова[2], Н.А. Горюхиной[3], Л.Б. Переверзева[4] обозначены подходы к описанию структуры МТ; в работах М.Г. Арановского[5], Р.Г. Болховского[6], И.В. Малышева[7], Г. Орлова[8], П.В. Соболева[9] рассматриваются вопросы семантики музыки и музыкальной коммуникации. Ряд работ посвящен проблемам моделирования творческих процессов[10]. Особо следует отметить труды М.Г. Бороды[11], построившего точный алгоритм разбиения одноголосного МТ на минимальные структурные единицы – «Ф-мотивы».

2) Исследования, связанные с применением точных методов в музыковедении.

Появление подобных исследований было обусловлено развитием кибернетики и вычислительной техники. В 1968 г. в СССР была создана постоянная Комиссия комплексного изучения художественного творчества, в последующем неоднократно проводились всесоюзные конференции по данной тематике («Точные методы в исследовании культуры и искусства», «Точные методы и музыкальное искусство», «Всесоюзный семинар по машинным аспектам алгоритмического формализованного анализа музыкальных текстов»).

Однако подробный анализ показывает, что большинство относящихся к указанной области работ либо носит обзорный характер, либо посвящено обсуждению общих вопросов и дискуссиям о принципиальной возможности применения точных методов в искусствознании[12].

В ряде работ решаются частные прикладные задачи[13]; целью целого класса исследований является выявление статистических закономерностей отдельных аспектов строения МТ[14].

В работах Г.А. Голицына[15], Э.Л. Рабиновича[16], М. Бензе[17], А. Моля[18] предпринимаются определенные шаги в направлении построения моделей творческого процесса и эстетического восприятия.

К числу исследований, связанных со всесторонним анализом структурных закономерностей строения МТ, можно отнести лишь уникальные работы Р.Х. Зарипова[19] и А.М. Степанова[20]. Однако используемая в них методология не позволяет говорить о создании структурных моделей, а сформулированные цели носят во многом идеалистический характер («способствовать раскрытию тайн природы творчества», «предвидеть стиль будущих композиторов»). Фактически же в упомянутых работах решается задача синтеза определенных классов МТ (песенных мелодий и их гармонизации у Зарипова и МТ строгого стиля у Степанова) на основе алгорит-

мического представления правил гармонии и полифонии, описанных в музыкально-теоретической литературе.

По результатам проведенного аналитического обзора можно сформулировать следующие выводы:

- к настоящему времени сформировались условия для постановки существенно более широкого круга актуальных задач, касающихся применения точных методов в теории музыки;
- разработанный в последние годы перспективный методологический аппарат, базирующийся на платформе информационно-эволюционного подхода к анализу и моделированию объективной реальности[21], позволяет перейти к прагматическому решению указанного класса задач.

Принципы моделирования музыкального текста аппаратом семиотико-хроматических гипертопосетей

В предшествующих работах[22] был обоснован выбор моделей СХ-гипертопографов[23] и гипертопосетей[24] для представления МТ различных стилей. Дальнейшие исследования показали необходимость модификации предложенного подхода в отношении проекции данных моделей на область анализа и синтеза музыкальной нотации.

Последующее изложение требует уточнения используемых терминов «музыкальный текст» (МТ) и «нотный текст» (НТ). Под МТ в общем случае понимается музыкальное произведение в любом способе его фиксации (как графическом, так и акустическом), термин «НТ» употребляется для обозначения МТ, представленного в форме традиционной пятилинейной европейской нотации (либо в любом другом однозначным образом сводимом к указанному виде).

Развивающийся во времени многоголосный акустический МТ представляет собой последовательность сменяющих друг друга созвучий. Совокупность символов НТ, соответствующих одновременно исполняемым звукам, в теории музыки принято называть вертикалью (точный термин отсутствует). При этом в общем случае каждая нота может входить в несколько вертикалей в зависимости от соотношения ее длительности с длительностями совпадающих с ней нот в других голосах (см. рис. 1).

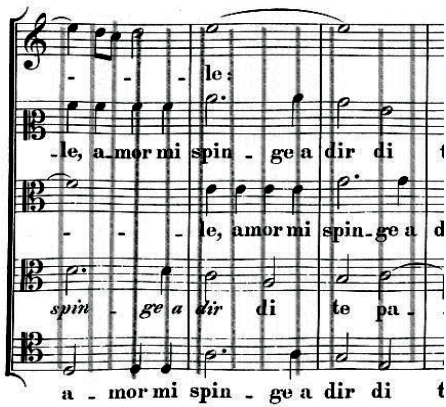


Рис 1. Последовательность вертикалей

Для устранения данной неоднозначности выберем определенную минимальную длительность таким образом, чтобы каждую ноту данного НТ можно было разбить на целое число отрезков равной ей длины (см. рис. 2). Тогда для каждого из полученных отрезков однозначно определена содержащая его вертикаль: в нее входят отрезки нот во всех голосах, совпадающие с данным. Назовем эту совокупность отрезков минимальным вертикальным соединением (МВС).

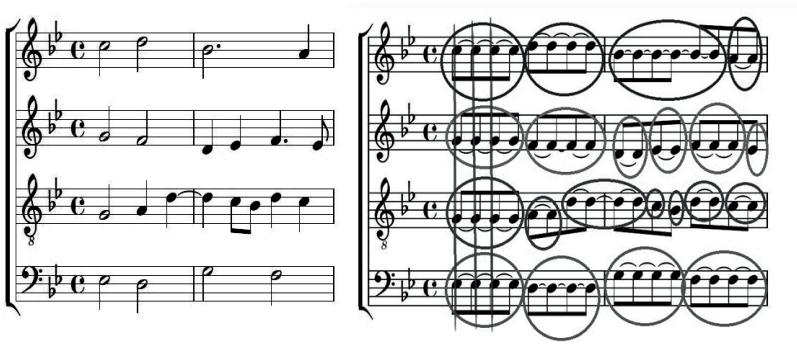


Рис. 2. Разбиение нотного текста
на минимальные вертикальные соединения

При моделировании МТ аппаратом СХ-гипертопосетей необходимо учесть следующие особенности данного вида текста. Любой МТ характеризуется сложной иерархией входящих в него элементов. Структура связей между ними как внутри МВС и в соседних или близко расположенных МВС, так и между отдельными МВС и их объединениями может быть весьма различной. Это определяется во многом стилистической принадлежностью музыкального произведения, а также особенностями его склада и фактуры. Однако для любого стиля связи между близко расположенными элементами чаще всего определены более явно и подвержены более строгой регламентации в музыкальной теории.

Поэтому в качестве состояний модели гипертопосети, представленных гипертопографами, логично рассматривать некоторые минимальные вертикальные комплексы (МВК), каждый из которых содержит одно или несколько соседних МВС в зависимости от специфики конкретного МТ. В частности, для произведений полифонического склада целесообразно включение в МВК одного МВС, для гомофонно-гармонического склада – объединения соседних МВС, принадлежащих одной гармонической функции. При этом различным уровням топологизации соответствуют элементы музыкальной ткани различных уровней иерархии (ноты, интервалы, аккорды).

Декларативные знания, описывающие свойства элементов и характер связей между ними, могут быть представлены на различных уровнях следующими хроматическими атрибутами:

- длительность ноты, тембр и громкость соответствующего ей звука;
- консонантность/диссонантность интервала;
- гармоническая функция аккорда;
- способ взаимосвязи аккорда с неаккордовым звуком и т. п.

Процедурные знания описывают закономерности перехода данного МВК в следующий.

Описанной гипертопосетью моделируется последовательность сменяющихся МВК. Помимо данной, будем рассматривать параллельно развивающуюся гипертопосеть, состоянием которой в фиксированный момент времени является совокупность полученных МВК, то есть фрагмент МТ, от начала до моделируемого в данный момент первой гипертопосетью МВК включительно. Таким образом, для второй гипертопосети на каждом шаге имеет место присоединение к гипертопографу нового элемента – гипертопографа, описывающего соответствующее состояние первой гипертопосети. Конечным состоянием второй гипертопосети будет являться в этом случае модель всего МТ.

При подобном подходе мы получаем возможность отражения в конструируемой модели связей между удаленными структурными единицами МТ и правил добавления к МТ следующего МВК с учетом этих связей.

В заключение данного раздела отметим, что изложенные принципы моделирования МТ моделью двух параллельно развивающихся гипертопосетей соответствуют описанному в музыкально-теоретических работах представлению о звучании музыкального произведения как процесса становления, под которым понимается «активное развитие, в котором каждый новый элемент способствует росту структуры вплоть до обретения целостности. <...> В каждом моменте становления видоизменяется структура обретением новых связей <...>. Становление есть отношение последующего к предыдущему, одновременно есть отношение части ко всему структурируемому целому»[25].

Модель музыкального текста строгого стиля

Основным объектом наших исследований является МТ строгого стиля (СС), поскольку его правила в наибольшей степени поддаются точному формальному изложению в музыкальной теории[26].

В соответствии с описанным выше подходом предложенная в предшествующих работах модель МТ СС была модифицирована. Если ранее данная модель была представлена одной гипертопосетью, то теперь, не внося существенных изменений в принципы построения последней, будем рассматривать ее лишь как первую из двух описывающих МТ гипертопосетей.

В качестве состояний указанной гипертопосети рассматриваются МВК, состоящие из одного МВС длительностью в одну восьмую. Множество-носитель гипертопографов, описывающих данные МВС, представлено совокупностью наборов всех возможных звуковысотных положений для всех голосов, при этом каждый элемент включает идентификатор (хроматический атрибут), обозначающий его принадлежность определенному голосу. Диапазон каждого голоса допускает 14 звуковысотных положений; таким образом, мощность множества-носителя равна $14n$, где n – число голосов моделируемого МТ.

Множество вершин 1-го уровня топологизации составляют n одноэлементных подмножеств множества-носителя с различными идентификаторами принадлежности голосам, что соответствует всем содержащимся в МВС нотам.

При таком подходе не возникает проблемы множественности экземпляров множества-носителя[27]. Кроме того, количество вершин 1-го уровня топологизации оказывается существенно меньшим мощности последнего.

Множество вершин 2-го уровня топологизации представлено созвучиями (интервалами и аккордами), образуемыми нотами, выбранными в качестве вершин.

На 3-м уровне топологизации рассматриваются отношения «пара голосов – третий голос» в трехголосии. Моделирование уровней топологизации выше 3 нецелесообразно, поскольку контрапунктические условия для четырех и более голосов не отличаются от таковых в трехголосии.

Рассмотрение, помимо данной, второй гипертопосети, состояния которой представлены совокупностью всех прошедших состояний первой, позволит в более удобном виде отразить особенности соотношений удаленных элементов МТ, в частности выявить:

- повторенные или варьированные фрагменты;
- наличие имитаций;
- применение полифонических преобразований и т. п.

Программная реализация модели одноголосного музыкального текста строгого стиля

В целях апробации описанных моделей была реализована (на языке C#) программа синтеза одноголосного МТ СС. Следует отметить, что разделение хроматических атрибутов элементов гипертопосети на декларативные и процедурные знания соответствует одному из принципов использования классов в объектно ориентированных языках программирования – наличию в них полей и методов.

В модели одноголосного МТ СС статическими состояниями первой гипертопосети являются вырожденные гипертопографы, состоящие из одной вершины (ноты). Данная гипертопосеть реализована в программе классом *Note*, поля которого описывают декларативные знания, представленные следующими хроматическими атрибутами:

- интервал от предыдущей ноты;
- положение текущей ноты внутри мелодии;
- длительность текущей ноты;
- является ли текущая нота звуком тритона;
- является ли текущая нота локальной мелодической вершиной.

Вторая гипертопосеть реализуется классом *Melody* и представляет собой список нот синтезируемой мелодии до текущей ноты. Данный класс содержит поля, характеризующие следующие свойства соответствующего отрезка мелодии:

- ключ;
- лад;
- тактовый размер;
- диапазон;
- продолжительность до текущего состояния;
- требуемая продолжительность.

Процедурные знания, относящиеся к элементам обеих гипертопосетей, используются для реализации алгоритма синтеза следующей ноты. В процедуре перехода в следующее состояние на выходе формируется список возможных вариантов присоединяемой к мелодии ноты с соответствующими весами (вероятностями). Выбор нужного варианта осуществляется в соответствии со значением вероятности перехода.

Кроме того, реализована процедура возврата в предыдущее или одно из предыдущих состояний, вызываемая в случае прихода к тупиковой ситуации, при которой синтез следующей ноты в рамках введенных ограничений невозможен.

Для записи сгенерированной мелодии в традиционной нотации использована программа LilyPond[28]. В отличие от стандартных программ нотного набора, предоставляющих пользователю возможность интерактивного ввода НТ, данная программа переводит специальным образом размеченный текстовый файл в файл в формате pdf, содержащий НТ в традиционной записи.

На рис. 3 приведен пример синтезированной мелодии.

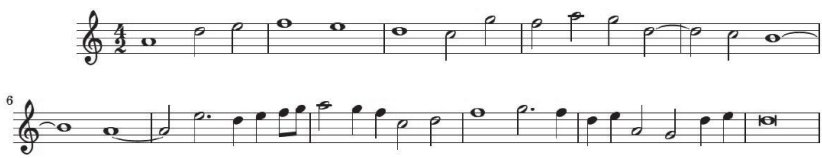


Рис. 3

В целях наглядной демонстрации динамики развития гипертопосетей помимо НТ программа также строит графическое представление процесса синтеза нот с отображением всех рассматриваемых на каждом этапе вариантов (см. рис. 4, 5). Построение

осуществляется с помощью программы GraphViz[29] – наиболее распространенного пакета визуализации графов.

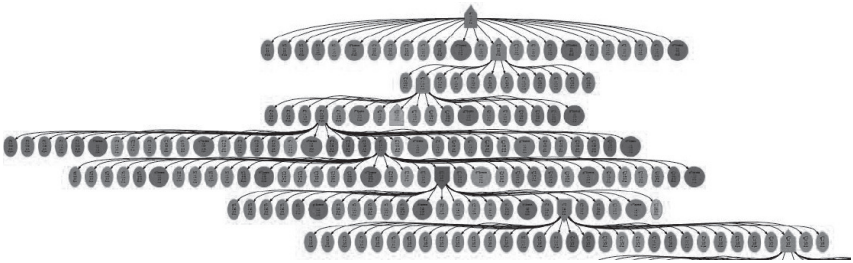


Рис. 4

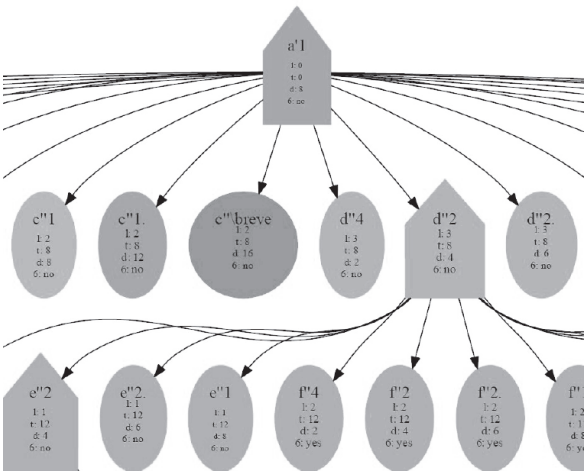


Рис. 5

Заключение

В рамках проводимых исследований информационной составляющей МТ на основе моделей СХ-гипертопографов и гипертопосетей была построена модель одноголосного МТ СС и реализована программа синтеза мелодий выбранного стиля с использованием указанной модели. Отсутствие на данный момент единого стандарта кодирования гипертопографов не позволяет хранить исполь-

зуемые в процессе работы программы модели гипертопографа и гипертопосети записанными в явном виде (фиксируются только их проекции на область нотной записи и схематического графического представления).

В настоящее время в Центре системного анализа и моделирования мышления[30] ведется работа по созданию универсальных программных библиотек для хранения и обработки информации, представленной моделью гипертопографов. По завершении этого процесса появится возможность внести необходимые изменения в описанную программу.

Кроме того, предполагается развитие программы для случаев двух-, трех- и четырехголосного МТ СС, связанное с разработкой соответствующих моделей. На начальном этапе создание и программная реализация модели одноголосного МТ являются вполне обоснованными, так как данная модель представляет собой необходимую составную часть моделей многоголосного МТ.

Автор выражает глубокую благодарность проф. А.Е. Барановичу за постановку задачи и ценные методические указания в процессе научной работы, а также М.М. Иглицкому за помощь в технических моментах программной реализации разрабатываемой модели.

Список аббревиатур

МТ – музыкальный текст
НТ – нотный текст
СС – строгий стиль
МВС – минимальное вертикальное соединение
МВК – минимальный вертикальный комплекс

Примечания

1 См.: *Арановский М.Г.* Опыт построения модели творческого процесса композитора // Методологические проблемы современного искусствознания. Л.: ЛГИТМиК, 1975. Вып. 1. С. 127–141.

2 См.: *Гаспаров Б.М.* О структурном описании музыкального языка // Точные методы в исследовании культуры и искусства: Мат-лы к симпозиуму. М., 1971. Ч. 2. С. 244–255; *Он же.* О некоторых принципах структурного анализа музыки // Проблемы музыкального мышления. М., 1974. С. 129–152.

3 См.: *Горюхина Н.А.* Музыкальное становление. Методика анализа // Музыкальное мышление: проблемы анализа и моделирования: Сб. науч. тр. Киев. гос. консерватории. Киев, 1988. С. 3–10.

[4] См.: *Переверзев Л.Б.* К построению кибернетической модели художественной деятельности // Точные методы в исследовании культуры и искусства: Матлы к симпозиуму. Ч. 1. С. 136–148.

[5] См.: *Арановский М.Г.* Мышление, язык, семантика // Проблемы музыкального мышления. С. 90–128.

[6] См.: *Болховский Р.Г.* Вещественность знака как фактор художественного воздействия // Эстетические очерки: Избранное. М.: Музыка, 1980. С. 156–171.

[7] См.: *Малышев И.В.* К определению понятия «Музыкальное произведение» // Там же. С. 103–124.

[8] См.: *Орлов Г.* Семантика музыки // Проблемы музыкальной науки. М., 1973. Вып. 2. С. 434–479.

[9] См.: *Соболев П.В.* «Художественная ценность»: к вопросу о содержании понятия // Художественное творчество: Вопросы комплексного изучения. Л., 1983. С. 239–244.

[10] См.: *Денисов Э.В.* О композиционном процессе // Эстетические очерки: Избранное. С. 242–253; см.: *Дранков В.Л.* Многогранность способностей как общий критерий художественного таланта // Художественное творчество... С. 123–139; см.: *Дыс Л.И.* Исследование проблем музыкального мышления: перспективы компьютерной реализации // Музыкальное мышление: проблемы анализа и моделирования... С. 30–37; *Медушевский В.В.* О динамическом контрасте в музыке // Эстетические очерки: Избранное. С. 125–155.

[11] См.: *Борода М. Г.* Принципы организации повторов на микроуровне музыкального текста: Автореф. дис. ... канд. искусствоведения. Тбилиси, 1979; *Он же.* О мелодической элементарной единице // Первый Всесоюзный семинар по машинным аспектам алгоритмического формализованного анализа музыкальных текстов. Ереван – Дилижан, 27.X – 1.XI.1975: Мат-лы. Ереван: Изд-во АН АрмССР, 1977. С. 112–120; *Борода М.Г., Орлов Ю.К.* О некоторых психологических аспектах количественной организации художественных текстов // Бессознательное (природа, функции, методы, исследования). Тбилиси, 1978. С. 302–309.

[12] См.: *Азгальдов Г.Г.* Поверить алгеброй гармонию. Можно ли? Нужно ли? // Число и мысль: Сб. М.: Знание, 1980. Вып. 3. С. 29–43; *Бирич И.А.* Научно-технический прогресс и художественная культура (научно-аналитический обзор советских исследований) // НТР и проблемы художественной культуры: Сб. обзоров и реф. М.: АН СССР, ИНИОН, 1981. С. 13–47; *Бирюков Б.В., Гутчин И.Б.* Машина и творчество: результаты, проблемы, перспективы. М.: Радио и связь, 1982. 152 с.; *Блок В.М.* Об эстетических предпосылках взаимоотношения кибернетики и музыки // Эстетические очерки. Вып. 2. М.: Музыка, 1967. С. 356–386; *Глушков В.М.* Кибернетика и творчество (реальность и поиски) // НТР и развитие художественного творчества / АН СССР, Науч. совет по истории мировой культуры, Комис. комплекс. изуч. худож. творчества. Л.: Наука, 1980. С. 166–175; *Завадский С.А.* Теория и практика «машинного ис-

кусства» // Искусство и научно-технический прогресс. М., 1973. С. 389–404; *Крон А.А.* Творческий процесс или имитация? // НТР и развитие художественного творчества. С. 228–232; *Мейлах Б.С.* НТР и возможности теории творчества // Там же. С. 20–30; *Митрофанов А.С.* Кибернетика и искусство // Кибернетика и современное научное познание. М., 1976. С. 360–425; *Нуйкин А.А.* О количественных критериях в искусствознании // Искусство и точные науки. М., 1979. С. 47–87; *Раппопорт С.Х.* Искусствознание и точные науки // Там же. С. 23–46.

13 См.: *Рыжов Л.* Моделирование оптимального этюда на ЭВМ // Точные методы и музыкальное искусство. Ростов н/Д: Изд-во РГУ, 1972. С. 108–119.

14 См.: *Гейн А.Г.* Возможность применения математических методов к анализу музыкальной формы // Там же. С. 68–73; *Детловс В.К.* Статистические методы в музыковедении // Там же. С. 51–54; *Зубарева Н.Б., Куличкин П.А.* Тайны музыки и математическое моделирование: Алгебра или гармония?.. Гармония и алгебра! М.: Книжный дом «ЛИБРОКОМ», 2010. 256 с.; *Рудь И.Д., Цуккерман И.И.* О возможности теоретико-информационного подхода к некоторым проблемам музыкального мышления и восприятия // Проблемы музыкального мышления. С. 207–229; *Цеханский В.М.* Некоторые закономерности вероятностного описания структуры музыкальной формы // Точные методы и музыкальное искусство. С. 54–60.

15 См.: *Голицын Г.А.* Информация и законы эстетического восприятия // Число и мысль: Сб. Вып. 3. С. 44–69.

16 См.: *Рабинович З.Л.* Некоторые вопросы автоматизации творческих процессов // Методологические проблемы кибернетики (Мат-лы к Всесоюзной конференции). Т. 2. М., 1970. С. 8–19.

17 См.: *Бензе М.* Введение в информационную эстетику // Семиотика и искусствометрия. М.: Мир, 1972. С. 198–215.

18 См.: *Моль А.* Теория информации и эстетическое восприятие. М.: Мир, 1975. 558 с.; *Моль А., Фукс В., Касслер М.* Искусство и ЭВМ. М.: Мир, 1975. 556 с.

19 См.: *Зарипов Р.Х.* Кибернетика и музыка. М.: Наука, 1971. 235 с.; *Он же.* Машинный поиск вариантов при моделировании творческого процесса. М.: Наука, 1983. 232 с.

20 См.: *Степанов А.М.* Эксперимент по моделированию структуры полифонической музыки строгого стиля // Эстетические очерки. Вып. 2. С. 387–407.

21 См.: *Баранович А.Е.* Введение в информациологию и ее специальные приложения: Дидактич. мат-лы к специальному курсу: Учеб. пособие. М.: РГГУ, 2011. 268 с.

22 См.: *Баранович А.Е., Иглицкая С.М.* О некоторых результатах сравнительного анализа музыкального и вербального текстов // Мат-лы X междунар. конф. «Интеллект. сист. и компьют. науки». М.: МГУ, 2011; *Иглицкая С.М.* К вопросу структурно-алгебраического и семантико-прагматического анализа музыкального текста // Вестник РГГУ. Сер. «Информатика. Защита инфор-

мации. Математика». 2011. № 13. С. 128–145; *Она же*. Об одном подходе к моделированию семантики полифонического музыкального текста // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2012. № 14. С. 187–198; *Баранович А.Е., Иглицкая С.М.* Моделирование музыкального текста строгого стиля аппаратом семиотико-хроматических гипертопосетей // Тр. IV Междунар. конгресса по интеллект. системам и информ. технол. / XII Междунар. научн.-техн. конф. «Интеллектуальные системы» (AIS'12). М.: Физматлит, 2012. Т. 2. С. 60–66.

[23] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект. М.: ГШ ВС РФ, 2003.

[24] См.: *Баранович А.Е.* Семиотико-хроматические гипертопосети: унифицированная модель представления знаний // Открытые семантические технологии проектирования интеллектуальных систем = Open Semantic Technologies for Intelligent Systems (OSTIS-2011): Мат-лы Междунар. научн.-техн. конф. / Редкол.: В.В. Голенков (отв. ред.) [и др.]. Минск: БГУИР, 2011. С. 71–86.

[25] См.: *Горюхина Н.А.* Указ. соч.

[26] См.: *Мазель Л.А., Цуккерман В.А.* Анализ музыкальных произведений. М.: Музыка, 1967. 752 с.; Музыкальная энциклопедия: В 6 т. / Гл. ред. Ю.В. Келдыш. Т. 5. Симон–Хейлер. М.: Советская энциклопедия, 1981. 528 с.; *Фраёнов В.П.* Учебник полифонии. М.: Музыка, 1987. 208 с.

[27] См.: *Баранович А.Е.* Многоосновные СХ-гипертопографы – однообъектная парадигма // Тр. III Междунар. конгресса по интеллект. системам и информ. технол. / XI Междунар. научн.-техн. конф. «Интеллектуальные системы» (AIS'11). М.: Физматлит, 2011. Т. 1. С. 377–385.

[28] См.: LilyPond... music notation for everyone [Электронный ресурс]. URL: http://lilypond.org (дата обращения: 30.04.2013).

[29] См.: Graphviz – Graph Visualization Software [Электронный ресурс]. URL: http://graphviz.org (дата обращения: 30.04.2013).

[30] См.: Сайт Центра системного анализа и моделирования мышления [Электронный ресурс]. URL: http://samtcenter.ru (дата обращения: 30.04.2013).

А.Е. Сатунина, Л.А. Сысоева

АНАЛИЗ МОДЕЛЕЙ УПРАВЛЕНИЯ СЕРВИС-ОРИЕНТИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ

В статье рассматриваются современные модели управления сервис-ориентированной информационной системой с целью их систематизации, определения их роли и места в информационных системах этого вида. Проводится анализ функций, уровней и объектов управления информационными системами с сервис-ориентированной архитектурой.

Ключевые слова: модели управления, сервис-ориентированная архитектура, управление сервис-ориентированной информационной системой.

Введение

В последнее десятилетие активное использование процессного подхода в управлении компаниями различного назначения обусловило повышение интереса к процессно-ориентированным архитектурам информационных систем, к числу которых относится и сервис-ориентированная архитектура (СОА). ИТ-архитекторы рассматривают СОА как подход к интеграции бизнес-процессов и поддерживающей их ИТ-инфраструктуры в форме безопасных и стандартизированных компонентов (сервисов), которые можно использовать многократно и комбинировать для адаптации к изменяющимся приоритетам бизнеса[1].

Управление сервис-ориентированной информационной системой требует разработки и применения таких методов управления, которые бы учитывали специфику архитектуры, проявляющуюся в следующих положениях[2,3,4,5]:

– функциональность системы реализуется на основе высокоуровневых компонент-сервисов;

– каждый сервис ассоциируется с конкретной бизнес-функцией, задачей или операцией;
– вызов или взаимодействие сервисов осуществляется в соответствии с логикой бизнес-процессов;
– динамичная адаптация архитектуры системы под требования бизнеса и изменения бизнес-процессов обеспечивается посредством взаимосвязи между ИТ-сервисами и бизнес-сервисами;
– композитная архитектура на основе сервисов позволяет достаточно гибко реагировать на инновации как на уровне бизнес-сервисов, так и на уровне ИТ-технологий;
– использование стандартов в процессе разработки, вызова и сборки сервисов повышает уровень их взаимодействия.

Переход к СОА в значительной мере был вызван тенденцией к усилению взаимосвязи ИТ и бизнеса и расширением сфер применения процессной модели управления[6], поэтому и управление информационной системой должно осуществляться с учетом процессного подхода.

Применение процессного подхода в управлении ИС позволяет оценивать эффективность функционирования системы в зависимости от уровня и степени управляемости многочисленными компонентами (сервисами) для достижения требуемого результата при помощи формально определенных и контролируемых бизнес-процессов[7]. Формализация различных видов деятельности в форме бизнес-процессов обеспечивает непрерывность управления как на уровне отдельных процессов, так и наборов взаимосвязанных процессов, что особенно важно для сервис-ориентированной архитектуры.

Целью данной статьи является анализ моделей управления сервис-ориентированной ИС и попытка их систематизации. Источниками информации являются публикации на порталах компаний-вендоров и консорциумов, занимающихся разработкой методологии СОА.

Современные модели управления сервис-ориентированной информационной системой

Более десяти лет назад идеи сервис-ориентированной архитектуры получили реальное развитие в виде методологий и концепций, но, несмотря на прошедшие годы, отсутствует единая методология СОА, которая бы могла быть принята в качестве единого стан-

дарта. На текущий момент компании-вендоры придерживаются в процессе разработки и внедрения сервис-ориентированных систем собственных методологических принципов и подходов.

Анализ моделей сервис-ориентированных архитектур, разработанных вендорами программного обеспечения IBM, Oracle, Microsoft[8,9,10], консорциумами OASIS[11] и Open Group[12], а также компанией Arcitura[13,14], показал, что отсутствует и единый подход к управлению сервис-ориентированной ИС.

В методологии СОА, разработанной и поддерживаемой компанией Arcitura, которая уже более 15 лет занимается формированием теоретических основ в данной области, управление СОА включает две составляющих[15,16]:

– управление СОА-проектами, которое связано с управлением сервисами в течение их жизненного цикла (анализ, проектирование, разработка, тестирование, внедрение и эксплуатация), управлением версиями сервисов, системой шаблонов проектирования, проектными командами и ролями в СОА-проектах;
– стратегическое управление СОА, которое включает организационные аспекты при создании и использовании корпоративной сервис-ориентированной ИС, вопросы формирования политик сервисов (правил предоставления сервисов потребителям с учетом возможных ограничений), актуализации и модернизации сервисов, выбора технологий и инструментальных средств для выполнения функций управления СОА.

Управление в методологии Arcitura направлено в первую очередь на управление сервисами, их жизненным циклом и механизмами вызова сервисов в соответствии с логикой бизнес-процесса.

В эталонной модели СОА, предлагаемой консорциумом OASIS[17], управление осуществляется с учетом этапов создания и перехода к сервис-ориентированной архитектуре ИС предприятия/организации:

– управление планированием СОА: включает формирование стратегии, цели, мотивации перехода к СОА;
– управление проектированием СОА: охватывает процессы управления разработкой сервисов, управление моделями взаимосвязей, поведения и действиями сервисов, управление системой шаблонов, использованием стандартов на различных этапах жизненного цикла СОА;
– управление эксплуатацией СОА: включает управление политиками, профилями, спецификациями сервисов, про-

токолированием выполнения процессов, вызова сервисов и реализации взаимосвязей сервисов.

Консорциумом Open Group[18], который занимается вопросами использования и применения стандартов в сфере ИТ, управление СОА рассматривается как управление процессами разработки, внедрения и применения сервисного подхода в организации в целом, и выделяются следующие уровни управления:

- управление сервисами, включающее управление жизненным циклом сервисов – анализ и моделирование, разработка, внедрение, мониторинг и контроль;
- управление приложениями, включающее управление жизненным циклом ИТ-приложений, созданных на основе сервисного подхода;
- управление (руководство) сервис-ориентированной архитектурой на уровне предприятия, которое связано с управлением стратегией предприятия в области СОА и ее практической реализацией.

Для структуризации процессов руководства была разработана специальная модель, включающая фазы: планирование, определение, внедрение (реализация), оценка.

Среди вендоров выделяются результаты теоретических исследований компании IBM в сфере управления СОА[19,20]. Разработанные на их основе модели управления сервис-ориентированной информационной системой имеют определенную эволюцию развития.

Этап 1. Создание модели управления жизненным циклом сервисов.

Разработка модели связана с формированием СОА как методологии построения программного обеспечения на основе сервисов и развитием модели сервис-ориентированного моделирования и архитектуры (SOMA)[21]. В контексте данной методологии архитектура сервис-ориентированной ИС рассматривается как многоуровневая структура (рис. 1):

- уровень инфраструктуры (программно-аппаратная платформа как совокупность ИТ-сервисов, на основе которой работают приложения);
- уровень корпоративных компонентов (функциональные компоненты приложений);
- уровень сервисов (атомарные прикладные функции, реализующие логику бизнес-процесса);
- уровень бизнес-процессов (модели бизнес-процессов и сборка сервисов в соответствии с логикой бизнес-процесса);

– уровень бизнес-сервисов (сервисы, предоставляемые потребителям; способы доступа к ним и методы их вызова/запуска);
– уровень интеграции (обеспечение межуровневого взаимодействия; определение функций ИТ при реализации бизнес-сервисов).

Управление СОА на данном этапе было ориентировано в первую очередь на управление сервисами в течение всего их жизненного цикла, состоящего из процессов планирования, моделирования, разработки, развертывания и мониторинга.

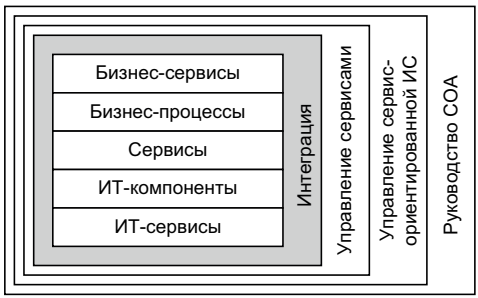


Рис. 1. СОА как многоуровневая структура

Этап 2. Создание модели управления сервис-ориентированной архитектурой.

Следующий этап связан с развитием методологии Smart SOA[22], где СОА рассматривается как подход к проектированию архитектуры ИС в масштабе предприятия с целью более тесной взаимосвязи между бизнесом и ИТ, и как следствие – повышение адаптивности и гибкости ИТ-приложений к изменяющимся требованиям бизнеса.

Компанией IBM с учетом методологии СОА консорциума Open Group был разработан набор моделей управления: модель жизненного цикла СОА (IBM SOA Foundation) и модель жизненного цикла СОА-руководства (IBM SOA Governance)[23].

Жизненный цикл СОА (IBM SOA Foundation) включает четыре фазы (рис. 2):

Моделирование (проведение бизнес-анализа: определение бизнес-целей, расстановка приоритетов, разработка требований, выявление и формальное описание бизнес-процессов и правил, формирование KPI на уровне бизнес-сервисов, бизнес-процессов, сервисов;

проведение ИТ-анализа: описание и классификация ИТ-сервисов информационной системы, разработка требований к сервисам).

Сборка (выявление сервисов, обеспечивающих реализацию бизнес-процессов; определение правил сборки сервисов; формирование политик вызова и предоставления сервисов; назначение параметров различным политикам; обоснование необходимости создания новых сервисов; проверка реализации отдельных бизнес-процессов и бизнес-сервисов в реальной среде и реальном масштабе времени).

Развертывание (проверка условий функционирования; уточнение требований к инфраструктуре; урегулирование и настройка зависимостей между бизнес-сервисами и ИТ-сервисами; конфигурирование ИТ-сервисов и приложений; функциональное тестирование реализации бизнес-сервисов; тестирование производительности; проверка уровня интеграции приложений; оценка приложений пользователями и др.).

Управление (включает методы, технологии и программное обеспечение, используемые для управления сервисами, бизнес-процессами и ИТ-инфраструктурой).

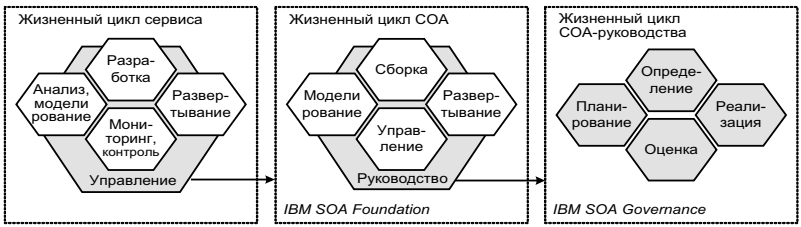


Рис. 2. Модели управления СОА

Переход к сервис-ориентированной архитектуре требует не только управления архитектурой, но и согласования развития бизнеса и информационных технологий на стратегическом уровне управления предприятием. Кроме того, необходимы изменения и в организационном управлении, поскольку успешность перехода к новой архитектуре зависит и от уровня координации руководителей различных подразделений, рабочих групп и отдельных сотрудников, деятельность которых связана с разработкой, внедрением и сопровождением СОА. Для решения вышеперечисленных задач компанией IBM была разработана модель руководства СОА (IBM SOA Governance), представленная в форме жизненного цикла,

состоящего из четырех этапов: планирование, определение, реализация и оценка (рис. 2).

Структуризация целей и задач, осуществляемых в ходе жизненного цикла руководства СОА[24,25,26], позволила определить перечень реализуемых процессов (табл. 1).

Таблица 1

Процессы жизненного цикла СОА-руководства

Фаза	Процессы
1	2
1. Планирование	Обоснование перехода к СОА и определение методов и средств управления СОА: – выделение в ИТ-стратегии направления стратегии СОА; – определение роли и преимуществ СОА для организации; – разработка стратегии развития СОА; – формирование принципов СОА; – исследование методов и моделей управления СОА; – анализ имеющихся ресурсов и средств управления; – анализ потребностей бизнеса в ИТ; – разработка плана управления реализацией стратегии СОА
2. Определение	Выработка подходов и методов управления СОА: – создание центра компетенций СОА; – определение организационных структур, ролей и уровней ответственности участников СОА; – выявление необходимой реорганизации существующей ИТ-инфраструктуры для перехода к сервисной архитектуре; – согласование политики повторного использования сервисов в различных приложениях ИС; – формирование механизма стимулирования повторного использования сервисов; – формирование политик предоставления сервисов; – определение рисков СОА; – разработка методов и средств, обеспечивающих требуемый уровень предоставления сервисов (SLA)
3. Реализация	Внедрение и эксплуатация модели управления: – внедрение новых методов управления сервис-ориентированной ИС и создание инфраструктуры для их поддержки; – управление безопасностью СОА; – обучение сотрудников методологии СОА

Окончание табл. 1

1	2
4. Оценка (Измерения)	Мониторинг и анализ показателей функционирования сервис-ориентированной информационной системы: – контроль методов управления СОА; – контроль выполнения разработанных политик и внесения изменений в них; – мониторинг и анализ уровня предоставления сервисов, выполнения требований, закрепленных в SLA; – мониторинг реализации процессов управления сервисами в СОА: мониторинг доступности сервисов; мониторинг изменений сервисов; мониторинг инцидентов, проблем, событий, связанных с функционированием сервисов; мониторинг безопасности сервисов и др.; – анализ уровня повторного использования сервисов; – анализ соответствия сервисов требованиям стандартов; – анализ показателей эффективности ИТ-сервисов и СОА; – анализ показателей риска ИТ-сервисов и СОА

Несмотря на различие в подходах как к методологии СОА, так и к управлению СОА, во всех моделях функции управления осуществляются сервисами управления и администрирования.

Всем моделям СОА свойственно, что сервисы, входящие в архитектуру информационной системы, подразделяются с позиций реализуемых функций на основные (базовые) и обеспечивающие (поддерживающие) сервисы. Выполнение основных сервисов связано с вызовом бизнес-сервисов и последующим запуском соответствующих бизнес-процессов, которые осуществляются путем сборки и запуска сервисов с учетом модели и логики бизнес-процесса. Обеспечивающие сервисы характеризуются тем, что отвечают за реализацию сервисов, не включающих бизнес-функциональность, к числу которых относятся и сервисы управления и администрирования.

Специфика управления сервис-ориентированной информационной системой

Проведенный анализ показал, что модели управления сервис-ориентированными информационными системами формируются с учетом функций, уровней и объектов управления (рис. 3).

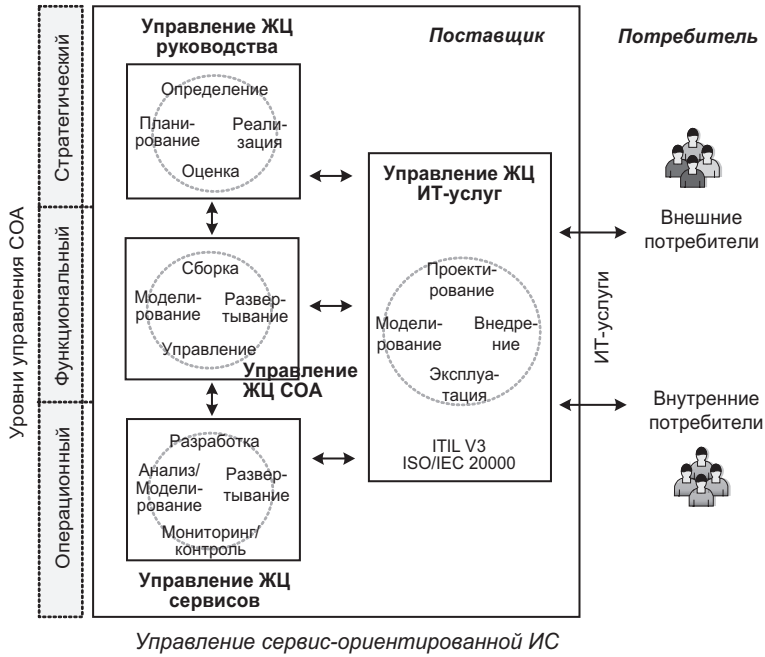


Рис. 3. Интегрированная среда управления сервис-ориентированной ИС

Объектами управления в СОА в зависимости от уровня управления являются:

- сервисы (сервисы как отдельные атомарные единицы);
- совокупность сервисов (множество взаимосвязанных сервисов, реализующих логику отдельного бизнес-процесса; композитные сервисы);
- компоненты, функциональные модули, приложения (разработанные на основе сервисной архитектуры и обеспечивающие реализацию бизнес-сервиса посредством взаимосвязанного набора сервисов);
- ИТ-сервисы как услуги, предоставляемые внутренним и внешним потребителям;
- сервис-ориентированная информационная система в целом.

Учитывая многообразие объектов, управление в сервис-ориентированных системах должно быть направлено и на отдельные сервисы, и на процесс их сборки, оркестровки при запуске биз-

нес-процессов, и на мониторинг показателей сервисов при реализации бизнес-сервисов.

В состав основных функций управления СОА входит управление сервисами в процессе их жизненного цикла, обеспечение безопасности, мониторинг и согласование сервисов.

Функции администрирования/руководства СОА включают управление жизненным циклом СОА, управление рисками, оценкой и измерением эффективности сервисов и СОА, управление качеством сервисов, определение полномочий для принятия решений в сфере СОА и др.

Выделяют три уровня управления СОА:

– стратегический – осуществление стратегического планирования бизнеса и ИТ с учетом их взаимовлияния (формирование и руководство ИТ-стратегией; анализ потребностей бизнеса в ИТ; управление инновациями; оценка эффективности СОА; управление финансами; формирование политики постоянного улучшения сервисов и др.);
– функциональный – обеспечение функционирования СОА (управление жизненным циклом СОА; управление доступностью, непрерывностью сервисов; управление изменениями; управление безопасностью и др.);
– операционный – обеспечение функционирования сервисов (управление жизненным циклом сервисов; управление запросами; управление доступом; управление событиями и инцидентами; управление эксплуатацией, техподдержкой и др.).

Анализ моделей управления СОА выявил следующие особенности управления сервис-ориентированной ИС:

– управление охватывает все уровни и объекты архитектуры, а также этапы жизненного цикла сервисов и СОА;
– управление осуществляется в интегрированной среде управления;
– система управления должна динамично и гибко реагировать на изменения бизнес-процессов и бизнес-сервисов (принцип СОА о взаимосвязи ИТ с бизнес-сервисами);
– система управления должна быстро адаптироваться к изменяющимся требованиям потребителей сервисов и внешней среды (принцип СОА о взаимосвязи ИТ с бизнес-сервисами);
– система управления должна обеспечивать функционирование и взаимодействие сервисов с учетом политик использования и предоставления сервисов (принцип СОА о свободном соединении сервисов);

– система управления должна соответствовать требованиям стандартов в сфере управления ИТ и лучшим практикам управления ИТ-сервисами, отраженным в ITIL (принцип СОА о стандартизации процессов и сервисов);
– функции управления СОА реализуются сервисами управления, в состав которых входят сервисы управления жизненным циклом, управления политиками, управления версиями, управления тестированием, управления мониторингом, управления безопасностью.

Заключение

В сервис-ориентированных ИС возрастает значение и роль функций управления, что обусловлено спецификой СОА, которая проявляется в динамичности и гибкости архитектуры к изменяющимся бизнес-процессам и требованиям.

Архитектура системы, включающая множество функциональных и обеспечивающих сервисов, требует централизованного управления сервисами, постоянного мониторинга их показателей и контроля процесса их взаимодействия. Для реализации требуемых функций управления на всех стадиях жизненного цикла СОА информационных систем необходим отдельно выделенный сервис, реализующий функции управления определенными объектами на определенных уровнях управления. Выполненный анализ современных моделей управления для СОА информационных систем выявил их общие и отличительные характеристики, что будет способствовать обоснованному принятию решений при выборе той или иной модели управления.

Примечания

[1] См.: *Биберштейн Н. и др.* Компас в мире сервис-ориентированной архитектуры (SOA): ценность для бизнеса, планирование и план развития предприятия: Пер. с англ. М.: КУДИЦ-ПРЕСС, 2007. 228 с.

[2] См.: *Lewis G., Smith D.B., Kontogiannis K.* A Research Agenda for Service-Oriented Architecture (SOA): Maintenance and Evolution of Service-Oriented Systems [Электронный ресурс] // Software Engineering Institute. URL: http://www.sei.cmu.edu/library/abstracts/reports/10tn003.cfm?RL=library&WT.ac=RLlibrary (дата обращения: 30.04.2013).

[3] См.: *Buecker A. et al.* Understanding SOA security: design and implementation // IBM Redbooks. [Электронный ресурс] URL: http://www.redbooks.ibm.com/redbooks/pdfs/sg247310.pdf (дата обращения: 30.04.2013).

[4] См.: *Биберштейн Н. и др.* Указ. соч.

[5] SOA Governance: Governing Shared Services On-Premise & in the Cloud. Boston, MA: Prentice Hall/Pearson PTR, 2011. 704 p.

[6] См.: *Биберштейн Н. и др.* Указ. соч.

[7] См.: The SOA Source Book [Электронный ресурс] // Open Group. URL: http://www.opengroup.org/soa/source-book/intro (дата обращения: 30.04.2013).

[8] См.: *Buecker A. et al.* Op. cit.

[9] См.: Oracle: SOA Suite Developer's Guide / K. Chu, O. Cordero, M. Korf, C. Pickersgill, R. Whitmore [Электронный ресурс] // Oracle Application Server. Documentation library. URL: http://download.oracle.com/docs/cd/B31017_01/core.1013/b28764/preface004.htm (дата обращения: 30.04.2013).

[10] См.: Microsoft: SOA & Business Process [Электронный ресурс] // Microsoft. URL: http://www.microsoft.com/soa (дата обращения: 30.04.2013).

[11] См.: OASIS Reference Architecture for Service Oriented Architecture [Электронный ресурс] // Сайт OASIS. URL: http://docs.oasis-open.org/soa-rm/soara/v1.0/csd03/soa-ra-v1.0-csd03.pdf (дата обращения: 30.04.2013).

[12] См.: The SOA Source Book.

[13] *Erl Th.* Service-Oriented Architecture: Concepts, Technology & Design. Boston, MA: Prentice Hall/Pearson PTR, 2008. Chapter 8, 9. P. 760.

[14] SOA Governance: Governing Shared Services On-Premise & in the Cloud.

[15] *Erl Th.* Op. cit.

[16] SOA Governance: Governing Shared Services On-Premise & in the Cloud.

[17] См.: OASIS Reference Architecture for Service Oriented Architecture.

[18] См.: The SOA Source Book.

[19] См.: *Buecker A. et al.* Op. cit.

[20] См.: *Биберштейн Н. и др.* Указ. соч.

[21] См.: *Arsanjani A., Ghosh S., Allam A., Abdollah T., Ganapathy S., Holley K.* SOMA: A Method for Developing Service-Oriented Solutions // IBM Systems Journal. 2008. Vol. 47. № 3. P. 377–396.

[22] См.: *Lewis G., Morris E.J., Smith D.B., Simanta S.* SMART: Analyzing the Reuse Potential of Legacy Components in a Service-Oriented Architecture Environment. [Электронный ресурс] // Software Engineering Institute. URL: http://www.sei.cmu.edu/library/abstracts/reports/08tn008.cfm (дата обращения: 30.04.2013).

[23] См.: *Биберштейн Н. и др.* Указ. соч.

[24] См.: *Arsanjani A., Ghosh S., Allam A., Abdollah T., Ganapathy S., Holley K.* Op. cit.

[25] См.: *Биберштейн Н. и др.* Указ. соч.

[26] SOA Governance: Governing Shared Services On-Premise & in the Cloud.

Н.О. Никитин

К ВОПРОСУ МОДЕЛИРОВАНИЯ ДИНАМИЧЕСКИХ ПРОЦЕССОВ НАКОПЛЕНИЯ ЗНАНИЙ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ*

В рамках однообъектной парадигмы теории графов рассматривается операция слияния СХ-гипертопографов, основанная на редукции классических операций объединения и соединения в k-гиперпространстве СХ-гипертопографов и положенная в основу процедуры моделирования. Формулируется критерий полноты подсистемы знаний. Последовательно вводится понятие операции слияния для графов, гиперграфов, гипертопографов и СХ-гипертопографов. Исследуются задачи синтеза эталонов запретных отношений в модели семантики. Используемые обозначения введены в ряде опубликованных работ[1].

Ключевые слова: гипертопограф семиотико-хроматический, k-гиперпространство семиотико-хроматических гипертопографов, «слияние» гипертопографов семиотико-хроматических, подсистема знаний, подсистема принятия решений, полнота подсистемы знаний.

Введение

В процессе своего функционирования антропоморфные интеллектуальные системы (ИС) различного генезиса оперируют информационными образами объективной реальности (ОР) в используемой терминологии именуемыми далее знаниями об объекте или знаниями. Они же – классические «декларативные» знания – содержатся в подсистеме знаний (ПЗ) ИС, «процедурные»

* Статья подготовлена в рамках реализации Программы стратегического развития РГГУ, проект 2.1.1 «Решение комплексных проблем в области общественных и информационных наук» в Центре системного анализа и моделирования мышления ИИНТБ.

знания же используются в подсистеме принятия решений (ППР) ИС. ПЗ ИС представляет собой накопленные ИС в процессе своего адаптивного существования знания, ППР ИС содержит механизмы их использования и преобразования, включая генерацию, трансформацию, развитие, пополнение, реструктуризацию, фильтрацию и т. п., а также передачу, восприятие, пополнение информации[2] при коммуникации ИС.

В предлагаемой модельной интерпретации ПЗ ИС есть не что иное, как статическая в момент времени t модель ОР, представленная семиотико-хроматическим гипертопографом (СХ-гипертопографом) в k-гиперпространстве СХ-гипертопографов Гs[3], последовательно формируемая, в т. ч. при интеллектуальной обработке инструментарием ППР ИС входящей информации, воспринятой средствами сенсориума[4].

Гипертопограф HTG_V^k с множеством-носителем праэлементов V[5] уровня топологизации k есть произвольный элемент B_{k+2}^V линейно упорядоченного булеана k + 2-го уровня топологизации множества-носителя ($HTG_V^k \in (B_{k+2}^V \setminus B_{k+1}^V)$), где $HTG_V^k \in (V_{k+2}^\tau \setminus V_{k+1}^\tau)$, $V_{k+1}^\tau \subseteq B_{k+1}^V$, $V_{k+2}^\tau \subseteq B_{k+2}^V$ (элемент HTG_V^k есть топовершина $V_{k+2}^\tau \setminus V_{k+1}^\tau$)[6].

СХ-гипертопограф HTG_V^k с носителем V уровня топологизации k есть тройка вида (V_{k+2}^τ, $P^{V_{k+2}^\tau}$, $\Theta^{V_{k+2}^\tau}$) где $P^{V_{k+2}^\tau}$ – множество цветов элементов множества топовершин V_{k+2}^τ булеана B_{k+2}^V множества-носителя праэлементов V *опорного* гипертопографа HTG_V^k, $\Theta^{V_{k+1}^\tau}$: $V_{k+2}^\tau \to B^{P^{V_{k+2}^\tau}}$ – отображение, сопоставляющее элементам множества топовершин V_{k+2}^τ их цвета, и $B^{P^{V_{k+2}^\tau}}$ – булеан множества[7] $P^{V_{k+2}^\tau}$.

Функциональный набор процедур из ППР ИС, представленный соответствующей метаалгеброй в Гs, может быть весьма разнообразен и изменяться в соответствии с телеологической направленностью ИС. Однако ввиду того, что к числу основных критериев интеллектуальности кибернетических систем[8] относится их способность к обучению, неотъемлемым компонентом ППР ИС является инструмент «накопления» знаний, поступающих в ИС из внешней среды, в качестве элемента операционной сигнатуры в моделирующей ППР ИС метаалгебре, реализующего указанную процедуру, предлагается использовать операцию «слияния» СХ-гипертопографов[9].

«Слияние» СХ-гипертопографов как развитие операций объединения и соединения графов, по А. Зыкову[10], следует рассматривать в качестве обобщенной (нетривиальной) операции на Гs, мо-

делирующей динамику накопления и концентрации знаний в ИС. Эволюция классических операций над графами в используемой метамодели представлена в ряде работ[11] операциями «трансформации», преобразующей исходный граф $HTG_V^k x$ в результирующий граф $\overline{HTG_V^k x}$, и «развития» (частный случай трансформации при $HTG_V^k x \subseteq \overline{HTG_V^k x}$). Принципиальным отличием операции слияния является наличие в результирующем графе потенциально существующей информации, что крайне важно для реально функционирующих ИС.

Действительно, обширные результаты анализа процессов функционирования произвольных ИС свидетельствуют о том, что ПЗ ИС подвержены многочисленным и трудно формализуемым диффузионным процессам, что не согласуется с «однозначностью» операций «трансформации–развития». Известные же операции[12] моделируют лишь актуально существующую информацию.

Соответственно, в ходе моделирования функционирования динамических систем возникает необходимость строгого разграничения множества потенциальных отношений в модели на допустимые и недопустимые. Последние есть не что иное, как семантически противоречивое подмножество модели. В случае задания вполне определенных семантических критериев и соответствующей расширенной алгоритмизации процедуры «слияния» СХ-гипертопографов вероятно получение работоспособной ИС с возможностью адекватного накопления знаний в ПЗ, например, при обработке вербальной информации, когда «объединенная» субъективная семантика двух последовательных сообщений не эквивалентна их индивидуальным субъективным семантикам.

Результатом применения операции должно явиться получение обновленной ПЗ ИС в момент времени f в случае наличия «новых» знаний[13] во входящей информации относительно состояния ПЗ в момент времени t ($f \succ t$).

Актуальность работы характеризуется бурным развитием интеллектуальных средств и активными научными исследованиями в области семантического анализа данных, включая, например, такие направления, как Data Mining или управление эволюцией мультимодального контента.

Новизна работы обусловлена применением информационно-эволюционного подхода к системному анализу и моделированию исследуемых динамических процессов накопления знаний[14].

Теоретическая значимость работы заключается в развитии теоретико-множественного аппарата метамоделирования информаци-

онных процессов. Практическая ценность кроется в возможностях использования, например, операции «слияния» при реализации самообучения ИС, а аппарат выделения семантических противоречий позволит решать задачи в области семантико-прагматической фильтрации.

I. Подходы к построению модели слияния

В рамках моделирования информационных процессов в Гs возможны два основных подхода к решению задачи построения модели семантики: восходящий – конструктивный и нисходящий – на основе системы ограничений. Отметим, что использование обоих подходов предполагает получение семантически эквивалентных образов при идентичных ПЗ и ППР ИС.

Восходящий подход «снизу вверх» основывается на выделении в прообразе множества объектов и их характеристических свойств с последующим построением множества актуальных связей по правилам, содержащимся в ППР ИС. Данная совокупность правил может быть основана, например, на известной совокупности отношений «подчинения»[15], заимствованной из естественного языка (ЕЯ) как наиболее исследованной модели представления знаний. Множество же актуальных связей реализуется в Гs совокупностью гипертоповершин[16].

Нисходящий подход «сверху вниз» также базируется на выделении объектов и их свойств, однако следующим этапом становится построение булеана $k + 1$-го порядка множества объектов и его хроматизация булеаном множества цветов. Полученная модель потенциальной информации[17] подвергается «фильтрации» за счет системы ограничений, реализованных механизмами ППР ИС. Подобные механизмы формируются, в первую очередь, иконическими методами, за счет статистики, полученной из ЕЯ и ПЗ ИС, аналогично эталонам запретных n-грамм[18], определяющих информационную энтропию.

Наиболее целесообразным, с нашей точки зрения, представляется использование гибридного подхода при решении задачи накопления знаний, когда вначале необходимо построить модель семантики входящей информации методом «снизу вверх», затем произвести соединение полученной модели с ПЗ ИС и «отфильтровать» противоречивые отношения «сверху вниз».

II. Семантические противоречия в модели семантики

Для обозначения актуально существующих, потенциально существующих, несуществующих[19], т. е. *семантически противоречивых*[20], элементов в модели, введем соответственно символизмы $A\exists$, $P\exists$ и $P\not\exists$.

Тогда актуально существующие в момент времени f элементы ПЗ ИС обозначим через $(HTG^{k}_{V_{\xi f}}x)_{A\exists} \equiv HTG^{k}_{V_{\xi f}}x$, где $HTG^{k}_{V_{\xi f}}x$ – статическое состояние модели в момент времени t ($f \succ t$), несуществующие – $(HTG^{k}_{V_{\xi f}}x)_{P\not\exists}$, потенциально существующие – $(HTG^{k}_{V_{\xi f}}x)_{P\exists}$.

При использовании Гs в качестве метамодели ИС для выделения подмножеств $(HTG^{k}_{V_{\xi f}}x)_{A\exists}$, $(HTG^{k}_{V_{\xi f}}x)_{P\exists}$, $(HTG^{k}_{V_{\xi f}}x)_{P\not\exists}$ удобно применять аппарат хроматизации множеств. Подобную хроматизацию множества $B^{V_{mrg}}_{k+1}$ назовем хроматизацией существования и обозначим через $\exists$ – *хроматизацией*.

При разработке методики слияния ПЗ ИС с информацией, поступающей на вход ИС, наибольший интерес вызывает подмножество $(HTG^{k}_{V_{\xi f}}x)_{P\exists}$, которое, в свою очередь, требует определения подмножества $(HTG^{k}_{V_{\xi f}}x)_{P\not\exists}$ семантических противоречий.

Семантические противоречия (СП) в модели Гs можно разделить на структурные СП (запретные отношения) и СП по хроматическим атрибутам (запретные характеристики). Структурные СП основываются на невозможности существования некоторых связей в опорной модели семантики, СП по хроматическим атрибутам же базируются на «несовместимости» некоторой совокупности характеристик с опорным гипертопографом моделируемого объекта.

Формирование СП целесообразно осуществлять путем ведения некоторой структурной статистики в ПЗ ИС с целью поиска маловероятных отношений, а также на основе совокупности ряда вполне определенных семантических правил, возможно, заложенных в ИС при создании[21] – обучение с учителем и / или развиваемых в процессе существования – обучение без учителя.

Представляется интересным при моделировании СП использовать конструкцию шаблонов[22]. Пусть задан алфавит Д. Холланда[23], состоящий из трех символов {0,1,*}. Шаблоном называется вектор, состоящий из элементов {0,1,*}, где {0,1} есть инварианты относи-

тельно операции слияния, {*} – вариант, принимающий при отображении в булев вектор значение {0,1}.

Рассмотрим пример определения потенциально существующих элементов СХ-гипертопографа с учетом некоторых заранее известных семантических противоречий с использованием аппарата шаблонов.

Пример 1.

$V \equiv \{a,b,c,d,e\}$;

$(HTG_V^1)_{A\exists} \equiv \{(a,b,c,d,e,(ab),(bc),(ac),(ad),(de))\}$;

$(HTG_V^1)_{P\not\exists} \equiv \{(000),(0000),(00000)\}$;

$(HTG_V^1)_{P\not\exists}{}' \equiv \{(******)\}$.

Тогда

$(HTG_V^1)_{P\exists} \equiv \hat{B}_{k+1}^V \setminus \{(HTG_V^1)_{A\exists} \cup (HTG_V^1)_{P\not\exists} \cup (HTG_V^1)_{P\not\exists}{}'\}$.

Как видно из примера 1, шаблоны $(HTG_V^1)_{P\not\exists}$ и $(HTG_V^1)_{P\not\exists}{}'$ позволяют не только задавать потенциально несуществующие элементы {(000),(0000),(00000)}, но и потенциально несуществующие структуры {(******)}[24].

III. Состояния подсистемы знаний. Критерий ε-полноты

При обработке входящей информации немаловажным является понятие «семантика». *Объективная семантика* информации характеризует информационные формы существования материальных систем ОР и взаимосвязана с формой, структурой и организацией материальных систем. *Семантика субъективная* интерпретируется как динамический информационный образ объективной семантики, инициализированный в ПЗ ИС[25].

В рамках используемой модели возможны различные варианты реализации операции «слияние» ПЗ ИС ξ, имеющей в момент времени t статическое состояние $HTG^k_{V_{\xi t}} x$ с множеством-носителем[26] $V_{\xi t}$, и поступающей на вход ИС информации I_1, после обработки ППР ИС имеющей вид $HTG^k_{V_{I_1}} x$ и образом которой в ПЗ ИС есть модель субъективной семантики $HTG^k_{V_{\xi t}} x_{I_1}$, с точки зрения полноты ПЗ ИС[27], на основе которых можно сформулировать критерий полноты ПЗ ИС относительно информации I_1.

1. ПЗ ИС ξ *пуста*, если $HTG^k_{V_{\xi t}} x \equiv \varnothing$.

2. ПЗ ИС ξ ε – *полна относительно входящей информации* I_1, если содержит в себе семантически эквивалентный с точностью до ε ($s\varepsilon$-эквивалентный) образ входящей информации[28] I_1, т. е. $HTG^k_{V_{I_1}} x \subseteq \{HTG^k_{V_{\xi t}} x\}$, где $\{HTG^k_{V_{\xi t}} x\}$ есть допустимое множество СХ-гипертопографов с носителем V ИС ξ в момент времени t.

3. ПЗ ИС ξ *не полна относительно* I_1 в противном случае.

4. ПЗ ИС ξ содержит абстрактный *информационный клон* входящей информации I_1 («совершенно полна»), если $HTG^k_{V_{I_1}} x \subseteq \{HTG^k_{V_{\xi t}} x\}_{A\exists}$.

Утверждение 1 (Критерий ε-полноты). ПЗ ИС ξ ε – *полна относительно* I_1 тогда и только тогда, когда $V_{I_1} \subseteq V_{\xi t}$ и $P^{V_{I_1}} \subseteq P^{V_{\xi t}}$, где V_{I_1} есть множество-носитель I_1, $P^{V_{I_1}}$ – множество цветов I_1. $\lhd$

Доказательство (от противного):

1. Пусть на вход поступила информация I_1, в ППР ИС преобразованная в $HTG^k_{V_{I_1}} x$, что $V_{I_1} \subseteq V_{\xi t}$, $P^{V_{I_1}} \subseteq P^{V_{\xi t}}$ и $HTG^k_{V_{I_1}} x \notin \{HTG^k_{V_{\xi t}} x\}$. Тогда $\{HTG^k_{V_{I_1}} x\} \notin \{HTG^k_{V_{\xi t}} x\}$, следовательно, $V_{I_1} \notin V_{\xi t}$ и/или $P^{V_{I_1}} \notin P^{V_{\xi t}}$. Получили противоречие.

2.а. Пусть на вход поступила информация I_1, в ППР ИС преобразованная в $HTG^k_{V_{I_1}} x$, что $V_{I_1} \notin V_{\xi t}$, $P^{V_{I_1}} \subseteq P^{V_{\xi t}}$ и $HTG^k_{V_{I_1}} x \subseteq \{HTG^k_{V_{\xi t}} x\}$. Из $V_{I_1} \notin V_{\xi t}$ следует, что в ПЗ $\not\ni HTG^k_{V_{\xi t}} x_{I_1} \subseteq \{HTG^k_{V_{\xi t}} x\}$, что $HTG^k_{V_{I_1}} x \equiv HTG^k_{V_{\xi t}} x_{I_1}$, следовательно, $HTG^k_{V_{I_1}} x \notin \{HTG^k_{V_{\xi t}} x\}$. Получили противоречие.

2.б. Для $V_{I_1} \subseteq V_{\xi t}$, $P^{V_{I_1}} \notin P^{V_{\xi t}}$ и $HTG^k_{V_{I_1}} x \subseteq \{HTG^k_{V_{\xi t}} x\}$ доказательство аналогично 2.а. $\lhd\lhd$

IV. Алгебраизация модели: операция слияния с теоретико-множественной точки зрения

В рамках общей проблемы моделирования динамики функционирования интеллектуальных систем произвольного генезиса возникает задача алгебраизации исследуемой модели семиотического k-гиперпространства СХ-гипертопографов Гs[29].

Определим операцию слияния последовательно для графов, гиперграфов, гипертопографов и СХ-гипертопографов.

При введении понятия «слияние» графов используем некоторые иные известные определения.

Определение 1. Объединение графов G_1 и G_2 ($G_1 \cup G_2$) есть результирующий граф $G^1_{V_{un}} \equiv (V_{un})^\tau_1$ с носителем $V_{un} \equiv V(G_1) \cup V(G_2)$ уровня топологизации 1, где $(V_{un})^\tau_1 \equiv V(G_1)^\tau_1 \cup V(G_2)^\tau_1$.◁

Определение 2. Соединение графов G_1 и G_2 ($G_1 + G_2$) есть результирующий граф $G^1_{V_{con}} \in (B^{V_{con}}_2 \setminus B^{V_{con}}_1)$ с носителем $V_{con} \equiv V(G_1) \cup V(G_2)$ уровня топологизации 2, где $G^1_{V_{con}} \in ((V_{con})^\tau_2 \setminus \{(V_{con})^\tau_1 \cup (G^1_V)_{P\not\exists} \cup (G^1_{V'})_{P\not\exists}\})$, $(V_{con})^\tau_1 \subseteq B^{V_{con}}_1$, а $(V_{con})^\tau_2 \subseteq B^{(V_{con})^\tau_1}_1 \equiv B^{V_{con}}_2$ ◁

Определение 3. Слиянием[30] графов G_1 и G_2 ($G_1 \cup^* G_2$) назовем результирующий граф $G^1_{V_{mrg}} \in (B^{V_{mrg}}_2 \setminus B^{V_{mrg}}_1)$ с носителем $V_{mrg} \equiv V(G_1) \cup V(G_2)$ уровня топологизации 2, где $G^1_{V_{mrg}} \in (V_{mrg})^\tau_2 \setminus \{(V_{con})^\tau_1 \cup ((V_{mrg})^\tau_2)_{P\not\exists}\})$, $(V_{mrg})^\tau_1 \subseteq B^{V_{mrg}}_1$, а $(V_{mrg})^\tau_2 \subseteq B^{(V_{mrg})^\tau_1}_1 \equiv B^{V_{mrg}}_2$ ◁

Отметим, что множества B^V_k, B^V_{k+1} представляют собой модели потенциальной информации[31], а V^τ_k, V^τ_{k+1}, – актуальной.

Определение 4. Слиянием гиперграфов HG_1 и HG_2 назовем результирующий гиперграф $HG^1_{V_{mrg}} \in (B^{V_{mrg}}_2 \setminus B^{V_{mrg}}_1)$ с носителем $V_{mrg} \equiv V(HG_1) \cup V(HG_2)$ уровня топологизации 2, где $HG^1_{V_{mrg}} \in (V_{mrg})^\tau_1 \cup ((V_{mrg})^\tau_2)_{P\not\exists}\}$, $(V_{mrg})^\tau_1 \subseteq B^{V_{mrg}}_1$, а $(V_{mrg})^\tau_2 \subseteq B^{(V_{mrg})^\tau_1}_1$ ◁

Рассмотрим слияние гипертопографов как обобщенный случай слияния графов и гиперграфов.

Определение 5. Слиянием гипертопографов HTG_1 и HTG_2 назовем результирующий гипертопограф $HTG^1_{V_{mrg}} \in (B^{V_{mrg}}_{k+1} \setminus B^{V_{mrg}}_k$ уровня топологизации k+1 с носителем $V_{mrg} \equiv V(HTG_1) \cup V(HTG_2)$, где $HTG^k_{V_{mrg}} \in (V_{mrg})^\tau_{k+1} \setminus \{(V_{mrg})^\tau_k) \cup ((V_{mrg})^\tau_{k+1})_{P\exists}\}$, $(V_{mrg})^\tau_k \subsetneq B^{V_{mrg}}_k$, а $(V_{mrg})^\tau_{k+1} \subseteq B^{V_{mrg}}_{k+1}$ ◁

Определение 6. Слиянием СХ-гипертопографов HTG_1x и HTG_2x ($HTG_1x \cup^* HTG_2x$) назовем результирующий СХ-гипертопограф $HTG^k_{V_{mrg}} x$ уровня топологизации k+1 с носителем $V_{mrg} \equiv V(HTG_1) \cup V(HTG_2)$ и множеством цветов $P^{(V_{mrg})^\tau_{k+1}} \equiv P^{(HTG_1)^\tau_{k+1}} \cup P^{(HTG_2)^\tau_{k+1}}$, где $HTG^k_{V_{mrg}} \in (V_{mrg})^\tau_{k+1} \setminus \{(V_{mrg})^\tau_k) \cup ((V_{mrg})^\tau_{k+1})_{P\not\exists}\}$, $(B^{P^{(V_{mrg})^\tau_{k+1}}})_{P\not\exists} \notin B^{P^{(V_{mrg})^\tau_{k+1}}}$, $HTG^k_{V_{mrg}} x \equiv \{HTG^{k-1}_{V_{un}} x\} \setminus \{HTG^{k-1}_{V_{un}} x\}_{P\not\exists}$, $(V_{mrg})^\tau_k \subseteq B^{V_{mrg}}_k$, а $(V_{mrg})^\tau_{k+1} \subseteq B^{V_{mrg}}_{k+1}$ ◁

Пример 1.

Пусть имеется граф G_1, изображенный на рис. 1.А, такой, что $V(G_1) = \{a,b,c\}$, $V(G_1)_1^\tau \setminus V(G_1) = \{(ab),(bc),(ac)\}$ и G_2 (рис. 1.Б), $V(G_2) = \{c,d,e\}$, $V(G_2)_1^\tau \setminus V(G_2) = \{(ad), (de)\}$.

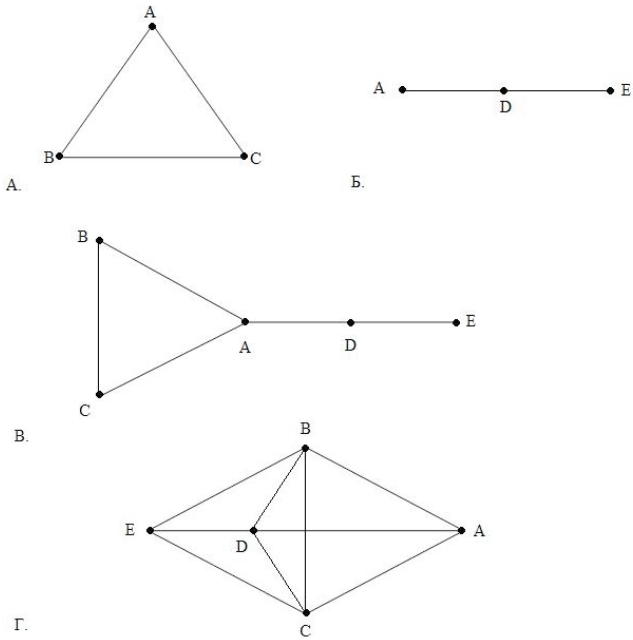


Рис. 1. А. Граф G_1, Б. Граф G_2, В. Объединение графов $G_1 \cup G_2$, Г. Соединение графов $G_1 + G_2$

Объединения (рис. 1.В) графов $G_1 \cup G_2 = \{(a,b,c,d,e,(ab),(bc),(ac),(ad),(de))\}$. Соединение (рис. 1.Г) графов $G_1 + G_2 = \{(a,b,c,d,e,(ab),(bc),(ac),(ad),(de))\}$. Слияние (рис. 2) графов $G_1 \cup^* G_2 \equiv B_2^{V_{mrg}}$, где $V_{mrg} = \{a,b,c,d,e\}$.

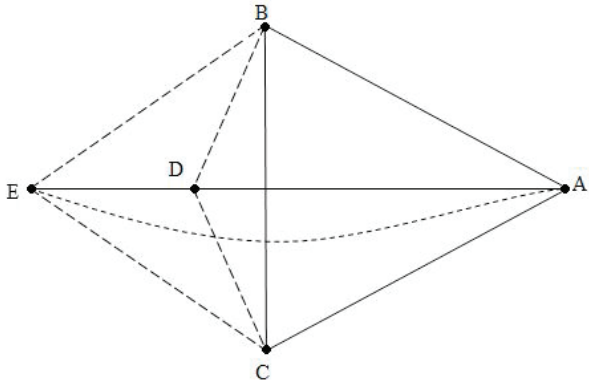


Рис. 2. Слияние графов G_1 U* G_2 [32]

В дальнейшем в работе нас будут интересовать только слияние СХ-гипертопографов и их опорных моделей.

V. Слияние при наличии ε-полной подсистемы знаний

Первичным этапом слияния входящей информации I_1 с ПЗ ИС ξ является выделение объектов-прообразов[33] в I_1 и идентификация соответствующих им образов в ПЗ ИС, что является «необходимым условием реализации операций <...> на множестве элементов <...> СХ-гипертопографов в Гs»[34]. Множество объектов-прообразов есть V_{I_1}, множество образов – некоторое подмножество элементов $(HTG^k_{V_{\xi t}}x)_{A\exists}$, каждому из которых соответствует некоторый вектор из булева гиперпространства $[GF(2)]^{|\hat{B}^{V_{\xi_{t-1}}}|}$, которому, в свою очередь, в однозначное соответствие поставлен вектор из *объединенной базовой шкалы* (ОБШ) независимых и измеримых частных свойств[35] и вектор их области допустимых значений, позволяющие моделировать совокупность свойств-прообразов P_{I_1} и их значения в ПЗ ИС.

Каждый объект из $(HTG^k_{V_{\xi t}}x)_{A\exists}$ может быть представлен тривиальным фреймом, изображенным на рис. 3. Тогда уникальное имя

для каждого элемента $(HTG^{k}_{V_{\zeta t}}x)_{A\exists}$ может быть представлено результатом конкатенации вектора из булева гиперпространства длины n – имени-индикатора опорной модели элемента, вектора из ОБШ длины m – имени-индикатора цвета элемента и вектора значений свойства длины m – имени-индикатора значения из интервала цветности.

Имя-индикатор опорной модели элемента	Имя-индикатор соотв. цветов	Имя-индикатор соотв. значений из интервала цветности	Текст на ЕЯ (ASCII / Unicode)	Звук (WAV / MP3)	Видео (AVI / MP4)	Фото (JPEG / GIF)

Рис. 3. Универсальный фрейм некоторого элемента $(HTG^{k}_{V_{\zeta t}}x)_{A\exists}$

Соответственно, методика «слияния» СХ-гипертопографов непосредственным образом будет следовать из методики идентификации тождественных объектов.

Методика 1. Слияние вербальной текстуальной информации I_1, поступающей на вход ИС, с ПЗ ИС («модель времени по наступлению события»).

1. Фиксируется множество объектов-прообразов V_{I_1} в I_1. Для каждого элемента множества V_{I_1}, имеющего определенную семиотическую структуру (СС) в ASCII / Unicode, производится поиск аналогичной СС во множестве универсальных фреймов[36].

2. Происходит выделение области поиска в $(HTG^{k}_{V_{\zeta t}}x)_{A\exists}$ за счет номинации найденных в п. 1 образов праэлементами для данного сеанса моделирования.

3. Фиксируется множество свойств-прообразов P_{I_1} и / или множество значений некоторых свойств-прообразов, в т. ч. явным образом отсутствующих в тексте, и производится поиск, аналогичный п. 1 в области, выделенной в п. 2.

4. Объекты-прообразы, свойства-прообразы и их значения, для которых не найден образ во множестве универсальных фреймов, последовательно добавляются к соответствующим множествам $(HTG^{k}_{V_{\zeta t}}x)_{A\exists}$.

5. В соответствии с совокупностью правил ЕЯ, реализованных в ППР ИС, происходит поиск отношений-прообразов[37] между элементами I_1 также на множестве универсальных фреймов, поиск которых происходит аналогично п. 1, а добавление ненайденных в соответствии с п. 4.

6. В связи с обновлением $(HTG^k_{V_{\xi t}}x)_{A\exists}$ до $(HTG^k_{V_{\xi t}}x)_{A\exists}$, изменилось множество потенциально существующих знаний, определяемое как $(HTG^k_{V_{\xi t}}x)_{A\exists} \equiv \hat{B}^{V_{\xi f}}_{k+1} \setminus \{(HTG^k_{V_{\xi t}}x)_{A\exists} \cup (HTG^k_{V_{\xi t}}x)_{P\exists}\}$.

Заключение

В работе рассмотрены некоторые вопросы моделирования динамики функционирования ИС. Предложен критерий различения неполных / полных с точностью до ε ПЗ ИС, позволяющий выделить две подзадачи в рамках создания аппарата «накопления» знаний: идентификации тождественных объектов с добавлением новых элементов и моделированием непротиворечивых отношений, и построения модели семантики ОР средствами ППР при достаточном наборе средств сенсориума. Для первой предложена методика разрешения, последнюю же следует упомянуть в постановочном плане. Речь идет о возможности ППР в автоматическом режиме создавать и заполнять универсальные фреймы при пустой ПЗ, например, за счет сопоставления звука изображению, изображения тексту и т. д. Идеи формирования первичных знаний из потока неструктурированной информации предложены в рамках исследования модели «сознания-подсознания»[38].

Операция слияния, описанная в статье с теоретико-множественной точки зрения, может быть реализована при любой схеме кодирования СХ-гипертопографов. В рамках последующих исследований предстоит использование данной операции в задаче последовательного семантического анализа в криптосемантике[39].

Полученные результаты в области создания механизмов моделирования семантических противоречий имеют ряд актуальных приложений, в т. ч. могут быть использованы в задачах семантико-прагматической фильтрации, имеющих целый ряд важных приложений, включая защиту «от информации» и управление эволюцией социума.

Стоит отметить, что вербальная текстуальная информация есть статическая модель (образ), включающая в себя, однако, не только прообразы-объекты, но и прообразы-процессы. Подобным свой-

ством обладает и музыкальный текст, моделирующий динамику произведения[40].

В рамках перспективных исследований динамики функционирования ИС целесообразно изучить возможность обновления не только ПЗ ИС, но и некоторых механизмов ППР ИС при поступлении на вход информации, что может повлечь усиление интеллектуальных способностей ИС.

Автор выражает глубокую благодарность проф. А.Е. Барановичу за непрерывную помощь в научных исследованиях и ценные рекомендации при написании работы.

Аббревиатуры

Гs – семиотическое *k*-гиперпространство СХ-гипертопографов
ЕЯ – естественный язык
ИС – интеллектуальная система
ОБШ – объединенная базовая шкала
ОР – объективная реальность
ПЗ – подсистема знаний
ППР – подсистема принятия решений
СП – семантическое противоречие
СС – семиотическая структура
СХ-гипертопограф – семиотико-хроматический гипертопограф

Примечания

[1] См.: *Баранович А.Е.* Многоосновные СХ-гипертопографы – однообъектная парадигма // Тр. III Междунар. конгресса по интеллект. системам и информ. технологиям (AIS-IT'11). М.: Физматлит, 2011; *Он же*. Семиотико-хроматические гипертопосети: унифицированная модель представления знаний // Открытые семантические технологии проектирования интеллектуальных систем = Open Semantic Technologies for Intelligent Systems (OSTIS-2011): Мат-лы Междунар. научн.-техн. конф. Минск: БГУИР, 2011. С. 71–86; *Баранович А.Е., Никитин Н.О.* О некоторых областях приложений алгебраической модели k-гиперпространства СХ-гипертопографов // Там же; *Баранович А.Е., Никитин Н.О., Ромодина Д.Д.* О последовательном критерии различения семантических гипотез // Тр. IV Междунар. конгресса по интеллект. системам и информ. технологиям (AIS-IT'12). М.: Физматлит, 2012; Сайт Центра системного анализа и моделирования мышления [Электронный ресурс]. URL: http://samtcenter.ru (дата обращения: 30.04.2013).

[2] В том числе секретной. См.: *Баранович А.Е., Никитин Н.О., Ромодина Д.Д.* Указ. соч.; *Баранович А.Е.* Семантические аспекты информационной безопасности: криптосемантика // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2012. № 14. С. 92–113.

[3] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект. М.: ГШ ВС РФ, 2003.

[4] Отметим, что получение «новых» знаний возможно и при соответствующем преобразовании ПЗ ИС без задействования дополнительной информации из внешней среды.

[5] См.: *Barwise J.* Admissible Sets and Structures: An Approach to Definability Theory // Perspectives in Mathematical Logic. Vol. 7. Berlin: Springer-Verlag, 1975.

[6] См.: *Баранович А.Е.* Многоосновные СХ-гипертопографы – однообъектная парадигма.

[7] См.: Там же.

[8] Любых систем, обрабатывающих информацию.

[9] См.: *Баранович А.Е.* Семиотико-хроматические гипертопосети: унифицированная модель представления знаний. См.: *Глушков В.М., Цейтлин Г.Е., Ющенко Л.Е.* Алгебра. Языки. Программирование / АН УССР, Ин-т кибернетики им. В.М. Глушкова. Киев: Наук. думка, 1989. См.: *Мальцев А.И.* Алгебраические системы. М.: Наука, 1970.

[10] См.: *Зыков А.А.* Основы теории графов. М.: Наука, 1984.

[11] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект. См.: *Баранович А.Е., Боровиков Д.В., Лакуша Е.Л.* Об алгебраизации модели k-гиперпространства СХ-гипертопографов: операции трансформации – развития // Мат-лы X Междунар. конф. «Интеллект. сист. и компьют. науки». М.: МГУ, 2011.

[12] См.: Там же.

[13] См.: *Баранович А.Е., Никитин Н.О., Ромодина Д.Д.* Указ. соч.

[14] См.: *Баранович А.Е.* Информационно-эволюционный подход в теории интеллектуальных систем // Интеллектуальные системы. Т. 15. Вып. 1–4. М., 2011. С. 15–52.

[15] Иконические отношения в ЕЯ есть гомоморфная проекция естественно-научных законов ОР на область ЕЯ-знаний. Следовательно, наряду с фиксацией отношений семантики в ЕЯ (эмпирический уровень), целесообразно строить единую физическую картину мира с фиксацией объективных отношений в ней и наследованием их проекций на антропоморфный социум.

[16] Гипертопоребер в двухобъектной парадигме.

[17] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект.

[18] См.: *Иглицкая С.М.* К вопросу структурно-алгебраического и семантико-прагматического анализа музыкального текста // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2011. № 13. С. 128–145.

[19] Актуально и потенциально.

[20] См.: *Баранович А.Е.* Универсальный подход к структурному моделированию директивно-целевых информационных процессов: Сб. раб. М.: ВС РФ, 1997.

[21] Генетическое наполнение ИС.

[22] См.: *Гладков Л.А., Курейчик В.В., Курейчик В.М.* Генетические алгоритмы: учебник для студентов вузов / Под ред. В.М. Курейчика. М.: Физматлит, 2010.

[23] См.: *Holland J.H.* Adaptation in Natural and Artificial Systems: An Introductory Analysis with Application to Biology, Control, and Artificial Intelligence. Ann Arbor: University of Michigan, 1975.

[24] Шаблон $(HTG^{k}_{V_{\xi t}} x)_{P\beta}$' позволяет запретить наличие в результирующей графе всех гипертоповершин, состоящих из шести элементов/праэлементов. См.: *Barwise J.* Op. cit.

[25] См.: *Баранович А.Е., Никитин Н.О., Ромодина Д.Д.* Указ. соч.

[26] $V_{\xi t}$ есть совокупность всех объектов в ПЗ.

[27] Будем считать, что ППР ИС содержит весь инструментарий для семантического анализа входящей информации, например, для вербальной текстуальной информации имеется лингвистический процессор ЕЯ без эталонов, позволяющий автоматически представить текст в формате универсальной модели представления знаний путем морфологического и синтаксического разбора (т. н. моделирование поверхностной семантики). См.: *Апресян Ю.Д., Богуславский И.М., Иомдин Л.Л. и др.* Лингвистический процессор для сложных информационных систем. М.: Наука, 1992. Также не будем учитывать вопросы защиты ИС от потенциально «вредной» информации, подробно изложенные в работах: см.: *Баранович А.Е.* Защита «от информации» как компонент информационной безопасности интеллектуальных систем: аксиологические WEB-фильтры // Тр. VIII Междунар. научн.-техн. конф. «Интеллектуальные системы» (AIS'08). М.: ФИЗМАТЛИТ, 2008. С. 316–321; *Он же.* Прагматические аспекты информационной безопасности интеллектуальных систем // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2009. № 10. С. 56–70; *Он же.* О некоторых семантико-прагматических механизмах информационной безопасности // Системы высокой доступности. Т. 7. М., 2011. С. 84–89.

[28] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах. М.: МО РФ, 2002.

[29] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект.

[30] «Процесс, осуществляющийся на основе композиции (сцепления) поименованных Х-гиперграфов с исключением (минимизацией числа) возможных омонимов и семантической противоречивости результата». См.: *Баранович А.Е.* Универсальный подход к структурному моделированию директивно-целевых информационных процессов.

[31] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект.

[32] Сплошная линия – актуально существующие связи в G_1, G_2, штрих – потенциальные связи, возникающие в результате слияния, пунктир – семантически противоречивые связи.

[33] Объект-прообраз есть элемент входящей информации, соответствующий информационный образ которого есть элемент ПЗ ИС. Для вербальной информации, например, существительные.

[34] См.: *Баранович А.Е.* К вопросу идентификации тождественных объектов в модели k-гиперпространства Гs // Тр. I Конгресса по интеллектуальным системам и информационным технологиям «AIS-IT'09». Т. 1. М.: Физматлит, 2009. С. 481–490.

[35] См.: *Баранович А.Е.* О задаче отождествления / различения элементов декларативных знаний в модели k-гиперпространства СХ-гипертопографов // Тр. II Конгресса по интеллектуальным системам и информационным технологиям «AIS-IT'10». Т. 2. М.: Физматлит, 2010. С. 11–19.

[36] Множество фреймов может быть реализовано на ЭВМ средствами многомерных кубов данных (технология OLAP), доступными в современных СУБД.

[37] Отношений синтаксического подчинения. См.: *Апресян Ю.Д., Богуславский И.М., Иомдин Л.Л. и др.* Указ. соч.

[38] См.: *Ханковский Д.Б.* О моделировании процесса первичного этапа формирования знаний в автономно эволюционирующей интеллектуальной системе // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2013. № 14 (в печ.); *Баранович А.Е., Ханковский Д.Б.* О моделировании взаимодействия подпроцессов мышления уровней «сознания-подсознания» // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2012. № 14. С. 169–186.

[39] См.: *Баранович А.Е., Никитин Н.О., Ромодина Д.Д.* Указ. соч.

[40] См.: *Иглицкая С.М.* Об одном подходе к моделированию семантики полифонического музыкального текста // Там же. С. 187–198.

Д.Б. Ханковский

О МОДЕЛИРОВАНИИ ПРОЦЕССА ПЕРВИЧНОГО ЭТАПА ФОРМИРОВАНИЯ ЗНАНИЙ В АВТОНОМНО ЭВОЛЮЦИОНИРУЮЩЕЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ*

В рамках информационно-эволюционного подхода к системному анализу и моделированию объективной реальности исследуются механизмы формирования первичных знаний в подсистеме знаний интеллектуальных систем уровней «сознание»–«подсознание». Формируются основы алгоритмической реализации процесса формирования первичных знаний из потока информации внешней в отношении интеллектуальной системы среды. Статья продолжает цикл работ, посвященных моделированию универсальных механизмов интеллектуальной деятельности различного генезиса.

Ключевые слова: информация, мышление, знания, интеллектуальные системы, сознание, подсознание.

Введение

Неотъемлемой особенностью интеллектуальных систем (ИС) является способность оперировать индивидуально-имманентными информационными моделями объективной реальности (ОР). Данная способность предполагает наличие в ИС вполне определенных подсистем знаний, той или иной степени развития, включающих механизмы сенсориума, синтеза, анализа, хранения и преобразования моделей ОР (знаний различного уровня генезиса). До последнего времени основное внимание в области теории интел-

* Статья подготовлена в рамках реализации Программы стратегического развития РГГУ, проект 2.1.1 «Решение комплексных проблем в области общественных и информационных наук» в Центре системного анализа и моделирования мышления ИИНТБ.

лектуальных систем уделялось разработке механизмов логического программирования, сенсорного восприятия внешних сигналов и хранения знаний. Однако при решении задач синтеза универсальных эволюционных механизмов интеллектуальной деятельности необходимым образом возникает вопрос о построении механизмов автоматического формирования знаний из сверхбольших объемов внешней (по отношению к ИС) информации.

Исследования механизмов обучения и самообучения (формирования знаний) проходят в основном в рамках различных направлений семиотико-логической[1] или нейросетевой[2] парадигмы. Оба подхода, а также гибридные на их основе[3], являются априори индуктивными. Их использование позволяет успешно решать целый ряд задач имитационного характера[4]. Логический подход, родившийся из моделей естественного языка (ЕЯ), к настоящему времени исчерпывает себя, отражая лишь базовые процессы логико-вербального мышления антропных систем, что выражается в постоянно декларируемых кризисах, «трудно разрешимых» в методологии имитации (копирования) антропного интеллекта в антропогенном. Бионический подход развивается в направлении от частного к общему, от изучения основных закономерностей организации и функционирования мозга к построению моделей такого функционирования. Это делает данное направление вполне определенно ограниченным особенностями реализации биологического носителя интеллекта.

Использование информационно-эволюционного подхода[5] (ИЭП) к системному анализу и моделированию (САМ) позволяет взглянуть на задачи информационной самоорганизации в ИС с новых позиций. Данный подход является дедуктивным и позволяет предложить более универсальные механизмы наполнения подсистем знаний ИС, чем традиционно исследуемые.

1. Краткий обзор достигнутых результатов

В используемом нами представлении информационное функционирование ИС реализуется в двух «плоскостях»: «сознание» и «подсознание». Будем считать, что в ИС осуществляются логические алгоритмические вычисления, реализующие механизм принятия решений, включающий аппарат логического вывода, происходит формирование, расширение, преобразование подсистемы знаний ИС. Уровень, на котором реализуются перечисленные процедуры, мы будем идентифицировать понятием «сознание».

Информационное функционирование ИС, однако, не исчерпывается процессами, реализуемыми на данном уровне. Предполагается, что ИС способна также реализовывать алогические функции, базирующиеся, в частности, на аппарате нелинейной динамики[6]. Уровень, на котором функционирует данный аппарат, будем связывать с понятием «подсознание» («бессознательное»)[7].

В качестве модели, описывающей функционирование ИС на «сознательном» уровне – уровне оперирования знаниями, будем использовать модель-универсум информации ИЭП САМ ОР[8]. Абстрактной экспликацией модели-универсума информации в контексте представления и моделирования знаний является *k-гиперпространство семиотико-хроматических (СХ) гипертопографов* (*ητ-графов*) *Γ*s[9]. Используемая экспликация модели-универсума обеспечивает моделирование и сенсориума, и подсистем знаний и коммуникации, и пространство целей, и объектов внешней среды, их свойств и отношений. Поскольку подсистема знаний относится к динамическим системам, в качестве динамических моделей представления знаний в зависимости от постановки задач используются конечные *метаалгебраической системы*, *метаалгебры* и *метаавтоматы*, или *семиотико-хроматические гипертопосети*[10].

Весьма интересным с точки зрения обоснованности результатов проведенных исследований является их сравнительный анализ с близкими, независимо полученными результатами научной группы В.И. Бодякина ИПУ РАН в отношении использования при моделировании эволюционных механизмов формирования «сознания» (подсистемы знаний ИС) аппарата нейроподобных[11] сетевых (теоретико-графовых) структур[12]. Заметим, что введенное В.И. Бодякиным понятие нейросетевой структуры свободно интерпретируется в аксиоматике абстрактной модели семиотико-хроматической гипертопосети, что позволяет легко спроецировать полученные результаты на используемый нами универсальный аппарат моделирования мышления уровней «сознание–подсознание», где в качестве базовой модели «бессознательного» («подсознание») используем *p*-адическую модель мышления[13].

В процессе исследования механизмов взаимодействия уровней «сознание–подсознание», то есть морфизмов моделей мышления уровней «сознание–подсознание», ранее был предложен ряд формальных алгоритмов и процедур[14]. Синтезированные процедуры построения соответствий и отображений используемых моделей позволяют реализовать механизм формирования информационного запроса из подпроцесса уровня «сознания»

в подпроцесс уровня «подсознания» с сохранением прагматической разнозначимости структуры запроса. Обратное отображение результата функционирования модели «подсознания» на уровень «сознания» носит «диффузный» характер, так как в результате работы модели динамической системы «подсознания» мы получаем точку $[GF(2)]^n$, где $n \to \infty$, которую в настоящих условиях невозможно однозначным образом идентифицировать конкретным актуальным Γs-объектом. Однако мы имеем возможность идентифицировать некоторый «размытый» результат работы «подсознания», соотнеся его с некоторым классом гипертопографов. Такая «размытость» вполне соответствует эмпирическим наблюдениям в области психологии и может быть охарактеризована как интуитивно-образное мышление.

Таким образом, чтобы перевести данное исследование в область экспериментальной апробации теоретических результатов, необходимо разработать аппарат информационной самоорганизации подсистемы знаний ИС, решив вопрос об априорно-апостериорном наполнении областей «подсознание/сознание».

2. Формирование области «подсознания»

В предлагаемой нами модельной интерпретации в процессе взаимодействия материальных систем возникает актуальное возмущение среды взаимодействия, являющейся материальным носителем информации о процессе взаимодействия, номинируемой нами термином *сигнал*. Сигналы воспринимаются соответствующими сенсорами ИС. На уровне сенсорного восприятия происходит потеря информации о прообразе, так как сенсоры воспринимают лишь ограниченную часть информационного прообраза в рамках своей способности различения. В развитии гипотезы *языка внутренней речи*[15], по Н.И. Жинкину, полученные информационные образы можно рассматривать как универсальный внутренний код ИС. В рамках общей теории кодирования и моделей фон Неймана данные образы могут быть представлены в формате $GF(2)$. Получающиеся двоичные последовательности (векторы вида $\vec{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$, где $\alpha_i \in \{0,1\}$, $i = \overline{1, n}$) суть первичные модели (информационные образы) «внешнего» мира (ОР). Область «подсознания» последовательно формируется из таких первичных моделей.

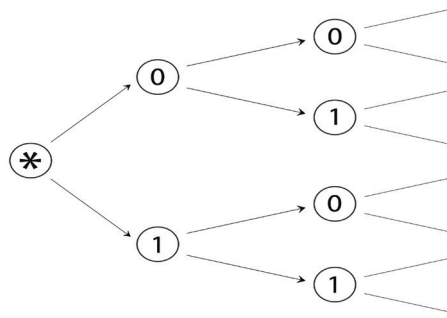


Рис. 1. 2-адическое дерево «подсознания»

Процесс информационного наполнения области «подсознания» происходит с использованием категорий «тождества/различия», по Г. Лейбницу[16], и реализуется в модели времени «по наступлении события». Будем считать, что первоначально данная область пуста. В процессе взаимодействия ИС с внешним миром начинает функционировать сенсориум ИС. В предлагаемой нами модельной интерпретации результатом такого функционирования являются двоичные последовательности. Начальная двоичная последовательность $\vec{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$, где $\alpha_i \in \{0,1\}$, $i = \overline{1, n}$, которая попадает в «подсознание», представляет собой модель однородной среды, где образы внешнего мира неразличимы. Однако уже следующий набор сигналов, воспринимаемый сенсориумом, может с какого-то места отличаться от предыдущего. То есть ИС может сгенерировать двоичную последовательность $\vec{\beta} = (\beta_1, \beta_2, ..., \beta_n)$, где $\beta_i \in \{0,1\}$, $i = \overline{1, l}$, имеющую общий корень определенной длины с первой последовательностью $\vec{\alpha}$, но с какого-то момента отличающуюся от нее. При этом 2-адическая метрика на $\vec{\alpha}$, $\vec{\beta}$ приобретет значение $\rho_2(\vec{\alpha}, \vec{\beta}) = 1/2^t$, где t наименьший номер, такой, что $\alpha_t \neq \beta_t$, $t \leqslant \max(l, n)$, $t \in \mathrm{N}$. Это означает, что в однородной среде был выделен некоторой отличимый объект, то есть произошла детализация ранее неразличимого внешнего мира. Все дальнейшее наполнение области «подсознания» происходит по принципу постоянной детализации. Учитывая, что для кодирования мы используем двоичные последовательности, в процессе детализации на каждом шаге возможно выделить лишь один объект. Этот процесс аналогичен построению 2-адического дерева[17] (рис. 1).

Вопрос о том, конечен ли этот процесс и конечную ли длину имеют получающиеся векторы, сводится к вопросу о возможности построения гипермножества[18], синтезируемого с использованием принципа «бесконечной» *делимости* «целого» на «части». А также к эпистемологической проблеме о принципиальной познаваемости мира.

В любом случае процесс информационного наполнения области «подсознания» можно отождествить с процессом построения части 2-адического дерева, которое можно рассматривать как некоторое счетное или конечное подмножество множества целых 2-адических чисел Z_2.

В процессе существования ИС 2-адическое дерево, соответствующее ее «подсознательной» области, постоянно «разрастается»: длины ветвей увеличиваются, появляются все новые и новые ветви. В какой-то момент, возможно, отделяется одна очень крупная ветвь, соответствующая специфическому набору сигналов. Этот набор сигналов можно назвать «внутренним», то есть характеризующим и описывающим информацию ИС о самой себе. Таким образом, можно предполагать, что в ИС появляется некая первичная модель самой ИС.

3. Формирование вторичных моделей ОР (знаний)

На некотором этапе развития ИС в отношении ее информационного наполнения осуществляется качественное преобразование информации в соответствии с диалектическим законом «перехода количества в качество». Информация, представленная на уровне «подсознания» в виде 2-адического дерева (двоичные последовательности большой длины), компрессируется. Преобразование информации происходит согласно концепции «концентрации знаний»[19] и представляет собой формирование вторичных моделей ОР.

В рамках данной модельной интерпретации реализация качественного преобразования информации поддается достаточно простому формальному описанию. Первоначальное формирование знаний в нашем представлении реализуется по достижении двух условий, связанных с 2-адическим деревом области «подсознания». Первое условие – достаточная длина общего корня у любых ветвей некоторого поддерева, второе – достаточно большое количество ветвей в этом поддереве. Другими словами, знание формируется тогда, когда мощность множества А достаточно близких двоичных векторов становится больше некоторого порогового значения:

1. $\rho_2(\vec{\alpha}_i, \vec{\alpha}_j) < q \; \forall \vec{\alpha}_i, \vec{\alpha}_j \in$ A, где $i, j = \overline{1, l}, q \in R$;
2. $|A| > n$, где $n \in$ N.

Таким образом, любую достаточно большую ветвь 2-адического дерева можно рассматривать как единый объект. Общий корень ветви говорит о том, что этот объект формировался из достаточно близких сигналов, воспринятых сенсориумом ИС. Собственно, общий корень непосредственно определяет получившийся объект, а ветвление, то есть расхождение этого общего корня, можно рассматривать как набор хроматических атрибутов – цветов (свойств) и/или их значений. Также можно произвести поименование сформированного объекта. Формируется первичный уровень области «сознания».

Процесс построения знаний связан с постоянным отображением некоторых ветвей 2-адического дерева в форму СХ-*ητ-графов Г*s. Однозначность такого отображения частично решает вопрос «диффузности» отражения результата функционирования модели «подсознания» на уровень «сознания». Отражение всех таких ветвей порождает часть пространства гипертопографов *Г*s. Так как процесс построения знаний носит постоянный характер, то данное пространство должно постоянно расширяться и преобразовываться. Более того, операции[20] в пространстве *Г*s семиотико-хроматических гипертопографов позволяют синтезировать и информационные модели более высокого порядка, то есть строить метамодели, метазнания.

Можно предположить, что крупная ветвь 2-адического дерева, соответствующая первичному информационному образу ИС о самой себе, эволюционирует до вторичной модели, то есть в ИС сформируется знание о самой себе. Этот процесс можно считать зачатком формирования у ИС эго, самосознания.

Заключение

Предложенные базовые универсальные механизмы, основанные на ИЭП, позволяют заложить основу алгоритмической реализации процесса формирования первичных знаний из потока информации, внешней в отношении ИС среды.

Данный подход является дедуктивным и позволяет частично решить вопрос о биективности отображения результатов функционирования области «сознания» в область «подсознания», а также дает возможность выделять часть хроматических атрибутов формируемых вторичных моделей ОР, то есть позволяет синтезировать полихромные гипертопографы.

В перечень последующих исследований предполагается включить изучение возможности представления предложенных условий первоначального формирования знаний в виде статистического критерия. Необходимо произвести расчет параметров такого критерия, определить вид функции распределения процесса формирования знаний. С этой целью предполагается алгоритмизация разработанного аппарата и перевод исследования в область экспериментальной апробации теоретических результатов, то есть переход к имитационно-статистическому моделированию.

Автор выражает глубокую благодарность проф. А.Е. Барановичу за постановку задачи и ценные методические указания в процессе научной работы.

Аббревиатуры

ЕЯ – естественный язык
ИС – интеллектуальная система
ИЭП – информационно-эволюционный подход
ОР – объективная реальность
САМ – системный анализ и моделирование
СХ – семиотико-хроматический

Примечания

1 См.: *Поспелов Д.А.* Логико-лингвистические модели в системах управления. М.: Энергоиздат, 1981. 232 с.; *Тарасов В.Б.* Логико-лингвистические модели: прошлое, настоящее и будущие // Политехн. чтения: Сб. тр. Вып. 7. Искусственный интеллект – проблемы и перспективы / Политехн. музей: науч. ред. Г.Г. Григорян, В.Л. Стефанюк. М., 2006. С. 48–54.

2 См.: *Редько В.Г.* Эволюционная кибернетика. М.: Наука, 2001. 156 с.; *Он же.* Модели адаптивного поведения – бионический подход к искусственному интеллекту // Моделирование процессов / Под ред. В.А. Райхлина. Казань: КГУ, 2007. С. 109–134.

3 См.: *Ярушкина Н.Г.* Основы теории нечетких и гибридных систем: Учеб. пособие. М.: Финансы и статистика, 2004. 320 с.

4 См.: *Андрейчиков А.В., Андрейчикова О.Н.* Интеллектуальные информационные системы: Учебник. М.: Финансы и статистика, 2006. 424 с., ил.

5 См.: *Баранович А.Е.* Информационно-эволюционный подход в теории интеллектуальных систем // Интеллектуальные системы. Т. 15. Вып. 1–4. М., 2012. С. 15–52.

6 См.: *Кадомцев Б.Б.* Динамика и информация. М.: Наука, 1998. 394 с.; *Капица С.П., Курдюмов С.П., Малинецкий Г.Г.* Синергетика и прогнозы будущего. М.: Наука, 1997. 285 с.

[7] См.: *Франц М.-Л.* Прорицание и синхрония: психология значимого случая / Пер. с англ. З. Кривулиной; Под общ. ред. В. Зеленского. СПб.: Изд. Группа «Азбука-классика», 2009. 224 с.

[8] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах. М.: МО РФ, 2002. 316 с.

[9] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект. М.: МО РФ, 2003. 404 с., ил.

[10] См.: *Баранович А.Е.* Семиотико-хроматические гипертопосети: унифицированная модель представления знаний // Открытые семантические технологии проектирования интеллектуальных систем = Open Semantic Technologies for Intelligent Systems (OSTIS-2011): Матер. Междунар. научн.-техн. конф. / Редкол.: В.В. Голенков (отв. ред.) [и др.]. Минск: БГУИР, 2011. С. 71–86.

[11] Функция активации в классической модели искусственного нейрона Маккалока–Питтса заменяется на сложный многопараметрический функционал.

[12] См.: *Бодякин В.И.* Механизм автоматического формирования информационной модели в информационно-управляющей системе, построенной на базе нейросемантической парадигмы // Нелинейная динамика в когнитивных исследованиях: Мат-лы II Всерос. конф. ИПФ РАН. Нижний Новгород, 2011. С. 20–23.

[13] См.: *Хренников А.Ю.* Моделирование процессов мышления в *p*-адических системах координат. М.: Физматлит, 2004. 295 с.

[14] См.: *Баранович А.Е., Ханковский Д.Б.* О моделировании взаимодействия подпроцессов мышления уровней «сознание»–«подсознание» // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2012. № 14. С. 169–186; см.: *Баранович А.Е., Ханковский Д.Б.* О реализации механизмов взаимодействия моделей подпроцессов мышления различного генезиса // Конгресс по интеллектуальным системам и информационным технологиям «IS&IT 2012»: В 4 т. Дивноморское, 2012. С. 312–317.

[15] См.: *Жинкин Н.И.* О кодовых переходах во внутренней речи // Вопросы языкознания. 1964. № 6. С. 26–38.

[16] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект. С. 172.

[17] См.: *Хренников А.Ю.* Моделирование процессов мышления в *p*-адических системах координат.

[18] См.: *Barwise J., Moss L.* Hypersets // Mathematical Intelligencer. 1991. Vol. 13. № 4. P. 31–41; *Idem.* Vicious circles and the mathematics of non-well-founded, Phenomena. Stanford: CSLI Public., 1996. P. 390.

[19] См.: Сайт Центра системного анализа и моделирования мышления [Электронный ресурс]. URL: http://samtcenter.ru (дата обращения: 30.04.2013).

[20] См.: *Никитин Н.О.* К вопросу моделирования динамических процессов накопления знаний в интеллектуальных системах // Вестник РГГУ. Сер. «Информатика. Защита информации. Математика». 2013. № 14 (115) (в печ.).

В.А. Лекае, В.П. Челноков

СИСТЕМА ПОСТОЯННЫХ URL

В статье рассматривается реализация системы постоянных URL под названием PURLRU, работающей в научной библиотеке РГГУ. Эта система сделана вместо свободно распространяемой американской системы PURL, оказавшейся у нас неработоспособной. Предложена и реализована простая схема объединения всех библиотечных клиентов под управлением одного PROXY-сервера. Эта система называется «мобильный библиотечный куст».

Образование такого куста крайне важно для повышения качества обслуживания абонентов путем расширения их возможностей за счет унификации доступа к информационным ресурсам библиотеки.

Ключевые слова: система PURL, URL, постоянный URL, локальный URL, свободно распространяемое программное обеспечение, мобильный библиотечный куст, система Handle, DOI.

Введение

В США была предложена концепция поддержки постоянных URL (persistent URL, PURL), ссылающихся на реальные библиотечные объекты (например, тексты книг). Этот механизм поддерживается OCLC (некоммерческий компьютерный библиотечный сервис). Общественной целью этой организации является расширение доступа к мировой информации и сокращение расходов на информацию. Более 72 000 библиотек в 170 странах и территориях используют услуги OCLC для поиска, приобретения, каталогизации, заимствования и сохранения библиотечных материалов. OCLC предоставляет доступ к библиографической, аннотационной и полнотекстовой информации.

Сущность механизма PURL заключается в следующем: для каждого объекта, нуждающегося в постоянной URL-ссылке, создается такая ссылка и регистрируется на специальном сервере, хранящем эти постоянные ссылки. Там же хранится и соответствующая локальная URL-ссылка, реально указывающая на этот объект; эта ссылка может не совпадать с постоянной ссылкой. При поступлении WEB-обращения с постоянной ссылкой к этому серверу происходит следующее: эта постоянная ссылка заменяется на локальную. Тем самым обеспечивается перенаправление запроса на реальный объект.

Обеспечить постоянство подобных ссылок могут, например, национальные библиотеки, поскольку они имеют стабильное финансирование и государственную поддержку, или крупные организации, имеющие в своем составе много филиалов и/или институтов, в частности РГГУ.

В рамках действующего проекта OCLC был разработан пакет программного обеспечения, его реализующий. Этот пакет доступен для скачивания на сайте http://purl.org. Он предназначен для работы в операционной системе LINUX.

Однако этот пакет оказался не работающим у нас (по крайней мере, Option A этого пакета) и слабодокументируемым в отношении выбора инструментальной операционной системы (вида Linux, предпочтения между сервером или настольной машины), а также в отношении самого процесса инсталляции.

Поэтому с другими американскими коллегами было принято решение написать собственный PURLRU на языке PHP. Программа оказалась удивительно простой и предлагается нами для использования в рамках свободно распространяемого обеспечения. Она работоспособна как в среде UNIX, так и в Windows.

Программа PURLRU

Программа PURLRU состоит из двух частей: программы замены постоянного URL на локальный и программы настройки подобных замен. Программа настройки подготавливает основную таблицу замен PURL. Таблица PURL хранится как реляционная таблица в базе данных PURL, работающей на сервере MySQL. Подчеркнем, что настраивать PURLRU может только администратор.

Первое поле таблицы PURL с именем CONSTANT содержит постоянный URL, а второе поле LOCAL – реальный, локальный URL. В дополнительном поле DATE хранится дата последнего изменения строки этой таблицы.

Программа PURLRU обрабатывает каждый поступающий WEB-запрос клиента на обслуживание. Она проверяет, указан ли в таблице PURL в качестве постоянного URL поступившего запроса. Если это так, производится его замена на URL, взятый из поля LOCAL; если же это не так, используется поступивший URL. Затем производится переадресация к объекту по полученному таким образом URL.

Программа настройки таблицы замен URL содержит основные опции для создания строки подмены, ее изменения или удаления. Эта технология может эффективно использоваться для создания *мобильного библиотечного куста*[1].

Действительно, пусть мы имеем набор серверов, содержащих данные одной библиотеки. Поставим в качестве корня этой иерархии PROXY-сервер, который будет транслировать для всех приходящих WEB-запросов их постоянные URL в реальные URL.

Пусть все библиотечные серверы объединены в локальную сеть (мобильный библиотечный куст). Пусть также корнем этого куста является подобный PROXY-сервер, на котором работает программа PURL. Взаимодействие с внешним миром идет через этот сервер (в частности, он принимает все приходящие в данную локальную библиотечную сеть Web-запросы).

Пусть интернет-адрес произвольного объекта выглядит следующим образом: «http://<ПУТЬ-К-PROXY>/<ПУТЬ>». Здесь ПУТЬ-К-PROXY это часть URL, указывающая на путь именно к PROXY-серверу; а ПУТЬ – оставшаяся часть URL, уточняющая размещение объекта в рамках мобильного библиотечного куста. Предположим также, что этот интернет-адрес первоначально и является реальным интернет-адресом искомого объекта. Тогда в таблице PURL нет никакой информации о перенаправлении и при поступлении запроса по такому интернет-адресу производится переадресация к объекту именно с этим поступившим адресом.

Далее допустим, что наш мобильный куст сменил домен: путь к PROXY-серверу и стал равным ПУТЬ-К-PROXY_1. В этом случае интернет-адрес произвольного объекта данного мобильного куста стал равным: «http:// < ПУТЬ-К-PROXY_1>/<ПУТЬ>». При этом мы полагаем, что ПУТЬ к объекту остается прежним. Действительно, намного чаще будет меняться домен адреса, а не размещение объекта в кусте.

Тогда, чтобы старый интернет-адрес работал, в таблицу PURL должна быть записана следующая строка: поле CONSTANT: <ПУТЬ-К-PROXY>; поле LOCAL: <ПУТЬ-К-PROXY_1>. В этом случае при поступлении запроса на старый адрес: <ПУТЬ-

К-PROXY> и при сравнении его с записями в поле CONSTANT таблицы PURL такая запись обнаружится в указанном поле упомянутой таблицы и программа заменит старый адрес прокси-сервера в запросе на значение, взятое из поля LOCAL, т. е. на новый адрес прокси-сервера, т. е. на <ПУТЬ-К-PROXY_1>. В результате адрес текста запроса преобразуется в реально существующий на данный момент адрес объекта и программа переадресует к искомому объекту с актуальным адресом, т. е. к объекту с реальным адресом http:// «< ПУТЬ-К-PROXY_1>/<ПУТЬ>».

Приведем поясняющий пример. Пусть постоянный интернет-адрес объекта такой: '*http://localhost:8080/net/partialexample/*foo/bar/baz', а интернет-адрес реального объекта стал равным '*http://example.com/partialtest/*foo/bar/baz'. Легко видеть, что в обоих адресах ПУТЬ равен 'foo/bar/baz' (указание ПУТЕЙ-К-PROXY в обоих адресах выделено курсивом).

Нетрудно видеть, что при поступлении постоянного интернет-адреса должна производиться только смена ПУТЕЙ-К-PROXY для получения адреса локального объекта. Значит, соответствующая строка таблицы PURL должна иметь вид: CONSTANT: '*http://localhost:8080/net/partialexample/*'; поле LOCAL: '*http://example.com/partialtest/*'.

Полагаем также, что если в интернет-запросе содержатся параметры, то они не меняются. Тогда вызов *'http://localhost:8080/net/partialexample/foo?bar=baz'* будет преобразован в следующий: '*http://example.com/partialtest/*foo?bar=baz' (напоминаем, что изменяется только ПУТЬ-К-PROXY-серверу – этот путь выделен курсивом в приведенных выше адресах).

В программе PURL также могут быть реализованы и реализуются в настоящее время расширенные виды перенаправления: частичный (Partial), частичный с добавлением расширения (Partial-append-extension), частичный с игнорированием расширения (Partial-ignore-extension) и частичный с заменой расширения (Partial-replace-extension). Приведем краткое, неформальное их описание, используя для этого примеры.

Частичное перенаправление было описано выше. Суть частичного метода с добавлением расширения заключается в следующем: добавляется расширение в локальный адрес. Пусть строка таблицы PURL имеет вид: CONSTANT: *http://net/partialappendextension/*; поле LOCAL: *http://example.com/partialappendtest*.

Пусть также постоянный интернет-адрес есть *'http://localhost:8080/net/partialappendextension/*foo/bar/bam?id=fizzle'. Тогда этот адрес преобразуется в *'http://example.com/partialappendtest/*bar/bam.

foo?id= fizzle'. Нетрудно видеть, что первый компонент ПУТИ 'foo' удаляется из адреса и вставляется в качестве расширения файла '.foo'.

Суть частичного метода с игнорированием расширения заключается в том, что при проведении операции замены удаляется расширение имени файла из локального адреса. Например, постоянный интернет-адрес *'http://localhost:8080/net/partialignoreextension/*foo.html' будет преобразован в *'http://example.com/partialignoretest/*foo'.

Частичный метод с заменой расширения является комбинацией двух последних методов. Использование этих методов расширяет гибкость при изменении интернет-адресов.

Этот механизм позволяет правильно конструировать мобильный библиотечный куст. При этом создатели куста обеспечивают пользователей возможностью изменять провайдера, не изменяя URL.

Существует и другая платная система Handle, решающая аналогичные задачи обеспечения постоянства URL-объектов. Возможности использования данной системы рассматриваются ниже.

Система Handle используется для уникальной идентификации информационных объектов (их содержания) в цифровой среде. При этом само содержание не обязательно должно иметь цифровую форму. Каждый объект идентифицируется с помощью DOI – digital object identifier (цифровой идентификатор).

Структурно DOI является строкой из букв и цифр, образующих два компонента DOI – *префикс* (Publisher ID) и *суффикс* (Item ID). Эти компоненты разделяются знаком «прямой слэш» (/). Ограничений на длину DOI нет, однако рекомендации советуют ограничиваться 128 символами.

Префиксы выдаются одним из официальных агентств DOI или Международным фондом DOI. Суффиксы DOI для информационных объектов формируют сами издатели. Приведем пример DOI:

DOI:10.1126/science.1169616 – статья из журнала "Science".

К сожалению, для получения суффикса DOI нужно его оплатить. А описываемая в этой статье система бесплатна. Эту систему можно также использовать и для создания кластеров библиотек, архивов и пр., обеспечивающих пользователей нецифровой информацией.

Поэтому излагаемая в данной работе разработанная технология может быть применена и весьма перспективна для России в части решения важных задач аналогичного плана для хранилищ нецифровых информационных объектов, например хранилищ оригиналов документов архивного плана, кинофотодокументов и пр.,

поскольку в отличие от системы Handle префикс можно выдавать бесплатно, а суффиксы назначаются самой библиотекой.

Система PURLRU была отлажена и эффективно используется в библиотеке РГГУ.

Выводы

1. В работе рассмотрены широко применяемые в мире технологии формирования кластеров из библиотек, архивов и других информационных систем, обеспечивающих интеграцию сведений о хранящихся в них информационных ресурсах цифрового и нецифрового характера. Показана эффективность их использования, поскольку такой подход существенным образом повышает качество обслуживания абонентов за счет формирования метаданных об адресах хранения их информационных ресурсов и, как следствие, упрощает доступ к ним.

2. Показано, что разработана аналогичная технология и для России за счет создания простой программной системы, обеспечивающей ее реализацию.

3. Отмечено, что разработка позволяет реализовывать создание кластеров держателей информации цифрового и нецифрового плана, а также обеспечивает возможность ее использования на компьютерах с разнообразными операционными системами.

Примечания

[1] См.: *Jha Sh., Merzky A., Fox G.* Programming Abstractions for Clouds // CCA-08: Cloud Computing and Its Applications (Chicago, 22–23 October, 2008). 6 p. URL: http://grids.ucs.indiana.edu/ptliupages/publications/cca08/pdf.

Г.А. Шевцова, С.В. Березовский

ПОРЯДОК ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ЭЛЕКТРОННОЙ ПОДПИСИ КАК СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ МЕЖВЕДОМСТВЕННОМ ЭЛЕКТРОННОМ ВЗАИМОДЕЙСТВИИ

Порядок применения технологии электронной подписи при межведомственном электронном взаимодействии рассматривается с позиции участников межведомственного электронного взаимодействия, предоставляющих государственные и муниципальные услуги и исполняющих государственные и муниципальные функции в электронной форме.

Технологическое обеспечение информационного взаимодействия органов и организаций показано на примере единых технологических решений. Рассматриваются виды, технология применения и проверки электронной подписи в электронных сообщениях, проходящих через узлы системы межведомственного электронного взаимодействия, а также особенности порядка использования участниками межведомственного электронного взаимодействия электронных служебных подписей и электронных подписей органа власти.

Защита электронного документа включает в себя защиту технологии с применением средств криптографической защиты информации.

Ключевые слова: электронная подпись, квалифицированный сертификат ключа, межведомственное электронное взаимодействие, защита информации.

В настоящее время с внедрением современных информационных и автоматизированных технологий интенсивное развитие получило межведомственное электронное взаимодействие, осуществляемое, прежде всего, в целях предоставления государственных и муниципальных услуг. В соответствии с нормами Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»

данный вид взаимодействия реализуется в процедурах, связанных с обменом документами и информацией в электронной форме между различными органами и организациями, участвующими в предоставлении услуг.

При этом применение электронных подписей, формируемых при межведомственном информационном обмене с использованием единой системы межведомственного электронного взаимодействия в целях предоставления государственных и муниципальных услуг и исполнения функций в электронной форме, становится приоритетным направлением и все более востребованным способом осуществления межведомственного запроса о предоставлении необходимых документов и информации.

Межведомственное информационное взаимодействие в целях представления и получения документов и информации в электронной форме с использованием единой системы и подключаемых к ней региональных систем осуществляется в соответствии с Положением «О единой системе межведомственного электронного взаимодействия», утвержденным постановлением Правительства Российской Федерации от 8 сентября 2010 г. № 697, Правилами использования усиленной квалифицированной электронной подписи органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, утвержденными постановлением Правительства Российской Федерации от 9 февраля 2012 г. № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи» и принятыми в соответствии с этими документами правовыми актами высших исполнительных органов государственной власти субъектов Российской Федерации о региональных системах межведомственного электронного взаимодействия.

Система межведомственного взаимодействия представляет собой федеральную государственную информационную систему, включающую информационные базы данных, в том числе содержащие сведения об используемых органами и организациями программных и технических средствах, обеспечивающих возможность доступа через систему взаимодействия к их информационным системам. Кроме того, информационная система содержит сведения об истории движения в системе взаимодействия электронных сообщений при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в

электронной форме. В информационной системе находятся также сведения о программных и технических средствах, обеспечивающих взаимодействие информационных систем органов и организаций, используемых при предоставлении в электронной форме государственных и муниципальных услуг и исполнении государственных и муниципальных функций.

Технологическое обеспечение информационного взаимодействия органов и организаций с применением системы взаимодействия достигается путем использования сервис-ориентированной архитектуры, представляющей собой совокупность электронных сервисов, построенных по стандартам и техническим требованиям, а также путем использования единых технологических решений, классификаторов и описаний структур данных.

Основными функциями системы взаимодействия являются следующие:

– обеспечение передачи запросов в виде документов и сведений, необходимых для получения государственных и муниципальных услуг и поданных заявителями через единый портал;
– обеспечение обмена электронными сообщениями между органами и организациями, информационные системы которых подключены к системе взаимодействия, при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций;
– обеспечение передачи на единый портал запросов, иных документов и сведений, обработанных в информационных системах органов и организаций, а также информации о ходе выполнения запросов о предоставлении государственных или муниципальных услуг и результатах их предоставления.

Таким образом, основная функция системы взаимодействия заключается в обеспечении:

– доступа к электронным сервисам информационных систем, подключенных к системе взаимодействия;
– получения, обработки и доставки электронных сообщений в рамках информационного взаимодействия органов и организаций с обеспечением фиксации времени передачи, целостности и подлинности электронных сообщений, указания их авторства и возможности предоставления сведений, позволяющих проследить историю движения электронных сообщений при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в электронной форме;

– возможности использования централизованных баз данных и классификаторов информационными системами, подключенными к системе взаимодействия;
– защиты передаваемой информации от несанкционированного доступа, ее искажения или блокирования с момента поступления указанной информации в систему взаимодействия до момента передачи ее в подключенную к системе взаимодействия информационную систему;
– хранения информации, содержащейся в реестре электронных сервисов информационных систем органов и организаций, подключенных к системе взаимодействия, и мониторинга работоспособности электронных сервисов, включенных в данный реестр[1].

При межведомственном электронном взаимодействии для оказания государственных услуг электронные подписи подразделяются на две категории:
– электронные подписи субъектов взаимодействия – физических лиц;
– электронные подписи информационных систем – субъектов взаимодействия[2].

При межведомственном электронном взаимодействии применяются следующие виды электронных подписей:
– простая или усиленная квалифицированная электронная подпись пользователя, формируемая от имени пользователя Единого портала государственных услуг, осуществляющего заказ услуг в электронном виде;
– усиленная квалифицированная электронная подпись – служебная подпись, формируемая от имени должностного лица органа власти, участвующего в межведомственном электронном взаимодействии при оказании государственных услуг (аналог собственноручной подписи);
– усиленная квалифицированная электронная подпись органа власти, формируемая информационной системой от имени органа государственной власти, участвующего в межведомственном электронном взаимодействии при оказании государственных услуг (аналог гербовой печати);
– электронные подписи системы межведомственного электронного взаимодействия и электронные подписи региональных систем межведомственного электронного взаимодействия (технологические), формируемые соответственно федеральными или региональными узлами системы межведомственного электронного взаимодействия

при обработке электронных сообщений, передаваемых через них;
– электронная подпись портала государственных услуг, формируемая информационной системой Единого портала государственных услуг при обмене электронными сообщениями, передаваемыми в информационные системы органов власти.

Процесс осуществления электронного взаимодействия в ходе реализации государственных услуг можно технологически представить следующим образом.

На первом этапе происходит формирование пользователем портала в Едином портале государственных услуг или должностным лицом органа власти в информационной системе органа власти запроса к информационному ресурсу другого ведомства и подписание электронных документов, передаваемых в запросе, своей электронной подписью (электронной подписью пользователя и усиленной квалифицированной электронной подписью должностного лица соответственно) и размещение его в конверте электронного сообщения, которое подписывается усиленной квалифицированной электронной подписью органа власти. Необходимо отметить, что порядок формирования и подписания электронной подписью ответа на запрос осуществляется аналогично формированию и подписанию электронной подписью запроса, поступившего в электронном виде. Конверт же электронного сообщения представляет собой файл формата, предназначенного для передачи электронных документов из одной информационной системы в другую (XML) и позволяющего системам, использующим разные программные средства обработки и хранения данных, обмениваться структурированной информацией, обеспечивать ее правильное преобразование и представление в любой среде.

Перед подписанием электронного документа и конверта системой проверки и генерации электронной подписи портала в автоматическом режиме проверяется наличие у должностного лица соответствующих полномочий и действительности его квалифицированного сертификата ключа проверки электронной подписи.

На втором этапе подписанный квалифицированными электронными подписями должностного лица и органа власти запрос поступает в систему межведомственного электронного взаимодействия. При этом система межведомственного электронного взаимодействия автоматически осуществляет:
– идентификацию информационной системы отправителя по квалифицированному сертификату ключа проверки электронной подписи информационной системы органа власти;

– проверку наличия и действительности сертификата ключа проверки электронной подписи информационной системы в реестре информационных систем, зарегистрированных в единой системе идентификации и аутентификации;
– проверку возможности обращения информационной системы к информационной системе адресата (получателя) электронного сообщения по реестру прав доступа, т. е. единой матрице доступа системы межведомственного электронного взаимодействия;
– подписание запроса технологической электронной подписью системы межведомственного электронного взаимодействия соответствующего узла с простановкой метки (штампа) времени электронного документа, которые являются достоверной информацией о моменте подписания документа и которые присоединяются к электронному документу или иным образом связываются с ним;
– гарантированную доставку запроса до информационной системы адресата.

На третьем этапе информационная система адресата, получив из системы межведомственного электронного взаимодействия запрос, может осуществить три проверки.

1. Наличия и действительности сертификата и корректности формирования технологической электронной подписи системы межведомственного электронного взаимодействия в запросе.

Успешность проверки гарантирует:
– поступление запроса от системы межведомственного электронного взаимодействия именно как от информационной системы, а не от иного источника;
– поступление запроса от информационной системы ведомства в систему межведомственного электронного взаимодействия во время, указанное в метке (штампе) времени;
– право на обращение информационной системы отправителя электронного сообщения к информационной системе получателя запроса.

2. Наличия и действительности сертификата и корректности формирования электронной подписи органа власти информационной системой в запросе, что при получении положительных результатов ее проведения гарантирует:
– поступление запроса в систему межведомственного электронного взаимодействия именно от информационной системы отправителя межведомственного запроса; целостность (подтверждение поступления запроса к информационной

системе получателя от информационной системы его отправителя в неизменном виде);
– формирование запроса порталом информационной системы органа власти; обладание информационной системой на момент подписания запроса соответствующими полномочиями на обращение с запросом к информационному ресурсу адресата.

3. Наличия и действительности сертификата и корректности формирования электронной подписи должностного лица отправителя запроса.

Успешность проверки гарантирует формирование запроса конкретным должностным лицом отправителя запроса и целостность переданного электронного документа.

Осуществление всех трех проверок сертификатов и подписей на поступивших документах не является обязательным – достаточно наличия и соответствующей успешной проверки только лишь электронных подписей системы межведомственного электронного взаимодействия и органов власти, что в целом гарантирует:
– целостность электронного документа отправителя и доставку его получателю в неискаженном виде;
– право отправителя на обращение к получателю;
– наличие соответствующих полномочий у должностного лица на формирование документа в информационной системе.

Существуют общие требования к электронным подписям, формируемым узлами системы межведомственного электронного взаимодействия и Единым порталом государственных услуг.

Ключи электронных подписей и соответствующие им квалифицированные сертификаты ключей проверки электронных подписей используются для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных услуг (функций).

Сертификаты и ключи электронной подписи системы межведомственного электронного взаимодействия, а также региональных систем межведомственного электронного взаимодействия, используемые для формирования электронных подписей в сообщениях, проходящих через федеральный и региональные узлы системы межведомственного электронного взаимодействия, выдаются на имя оператора соответствующей системы межведомственного электронного взаимодействия.

Электронная подпись этих двух систем подтверждает:
– факт достоверности прохождения электронного сообщения через узлы систем;

– факт аутентификации и авторизации в соответствии с правилами, указанными в реестре прав доступа к электронным сервисам (матрице доступа);
– неизменность сведений, внесенных в электронное сообщение систем.

Сертификат электронной подписи системы (региональной) межведомственного электронного взаимодействия выдается на каждый отдельный узел системы межведомственного электронного взаимодействия.

Сертификаты ключей проверки электронной подписи и ключи электронной подписи портала государственных услуг, используемые для формирования электронных подписей в сообщениях, формируемых в Едином портале государственных услуг, выдаются на имя оператора Единого портала государственных и муниципальных услуг (функций).

Электронная подпись портала государственных услуг подтверждает:
– факт формирования запроса на оказание услуг в электронном виде в информационной системе Единого портала государственных и муниципальных услуг (функций);
– факт аутентификации и авторизации в личном кабинете Единого портала государственных услуг лица, сформировавшего запрос в электронном виде на оказание услуг;
– неизменность переданных данных при передаче к информационной системе потребителя.

При обращении в электронной форме за получением государственной или муниципальной услуги заявление и каждый прилагаемый к нему документ подписываются тем видом электронной подписи, допустимость использования которых установлена федеральными законами, регламентирующими порядок предоставления государственной или муниципальной услуги либо порядок выдачи документа, включаемого в пакет документов. В случаях, если указанными федеральными законами используемый вид электронной подписи не установлен, вид электронной подписи определяется в соответствии с критериями определения видов электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг. Правила определения видов электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг, утверждены постановлением Правительства Российской Федерации от 25 июня 2012 г. № 634. Этим же документом определены критерии определения видов электронной

подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг.

Рассмотрим более подробно особенности применения усиленной квалифицированной электронной подписи в электронных документах, передаваемых с использованием системы межведомственного электронного взаимодействия в адрес территориального органа, и в передаваемых электронных документах, формируемых территориальным органом.

В электронных сообщениях могут использоваться следующие усиленные квалифицированные электронные подписи:

– электронные подписи субъектов взаимодействия – физических лиц – электронные служебные подписи, формируемые от имени должностных лиц территориального органа, участвующих в межведомственном электронном взаимодействии при оказании государственных услуг (аналог собственноручной подписи);
– электронные подписи в информационной системе как субъекте взаимодействия – электронная подпись органа власти, формируемая от имени государственного учреждения и его территориальных органов (как юридических лиц), участвующих в межведомственном электронном взаимодействии при оказании государственных услуг (аналог гербовой печати государственного учреждения)[3].

Ключи электронной служебной подписи и квалифицированные сертификаты ключей проверки электронной подписи выдаются аккредитованными Минкомсвязью России удостоверяющими центрами должностным лицам территориальных органов в соответствии с предоставленными им полномочиями по применению электронной подписи. Данные ключи и сертификаты используются для формирования (проверки) в информационных системах электронных подписей от имени указанных должностных лиц при оказании государственных и муниципальных услуг (функций) с использованием системы межведомственного электронного взаимодействия.

Структура квалифицированного сертификата ключа проверки электронной подписи должна соответствовать требованиям к единой структуре сертификата ключа проверки электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи» и разработанным Минкомсвязью России «Рекомендациям по составу квалифицированного сертификата ключа проверки электронной подписи».

Электронная подпись признается равнозначной собственноручной подписи в документе на бумажном носителе проставившего ее должностного лица. Такая подпись подтверждает:

– факт формирования в информационной системе территориальных органов межведомственных запросов;
– факт наличия у должностного лица, сформировавшего в информационной системе электронный документ (запрос либо ответ), соответствующих полномочий по подписанию электронной подписью (ее проверке) на момент формирования электронного документа.

В случае возникновения обстоятельств, не позволяющих участнику межведомственного электронного взаимодействия (уполномоченному лицу участника межведомственного электронного взаимодействия) правомерно использовать электронную подпись и средства электронной подписи при осуществлении межведомственного электронного взаимодействия, участник данного вида взаимодействия обязан не позднее одного рабочего дня со дня наступления таких обстоятельств в обязательном порядке письменно уведомить об этих обстоятельствах аккредитованный удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи и ключ электронной подписи, для прекращения их действия.

Участники межведомственного электронного взаимодействия при использовании электронных подписей обязаны:

– обеспечивать конфиденциальность ключей электронной подписи, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;
– уведомлять аккредитованный удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи (компрометации ключа) незамедлительно (не позднее одного рабочего дня со дня получения информации о таком нарушении) для прекращения действия сертификата, выданного для проверки этого ключа;
– не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
– использовать для создания и проверки электронной подписи и ключей электронных подписей средства электронной подписи, получившие подтверждение соответствия требованиям, установленным ФСБ России[4].

Таким образом, применение электронной подписи не только повышает оперативность в предоставлении государственных услуг, но и обеспечивает юридическую значимость (силу) и достоверность заверяемых ею электронных документов и позволяет определять авторство электронных сообщений.

Необходимо иметь в виду, что все организационно-методологическое руководство организацией работ по обеспечению безопасности применения средств криптографической защиты информации, включая ключи электронных подписей и контроль за обращением с ними, осуществляют структурные подразделения по защите информации в соответствии с возложенным на них функционалом и решаемыми задачами.

Примечания

[1] См.: Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Российская газета. Федеральный выпуск № 5247. 2010. 30 июня.

[2] См.: Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // Российская газета. Федеральный выпуск № 5451. 2011. 8 апр.

[3] См.: Постановление Правительства Российской Федерации от 25 августа 2012 г. № 852 «Об утверждении правил использования усиленной квалифицированной электронной подписи при обращении за получением государственных и муниципальных услуг и о внесении изменения в правила разработки и утверждения административных регламентов предоставления государственных услуг».

[4] См.: Постановление Правительства Российской Федерации от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия».

Л.И. Воронова, А.С. Трунов,
В.И. Воронов

РАЗРАБОТКА МЕТОДОВ ПАРАЛЛЕЛЬНОГО РАСЧЕТА КОРРЕЛИРОВАННОЙ МНОГОЧАСТИЧНОЙ СИСТЕМЫ НА ГРАФИЧЕСКОМ ПРОЦЕССОРЕ*

В статье рассматривается разработка методов высокопроизводительных вычислений, реализуемых на сетевом вычислительном ресурсе РГГУ (информационно-исследовательская система ИИС «MD-Slag-Melt»)[1], позволяющих исследовать структуру и свойства коррелированных систем многих частиц методом молекулярной динамики. Рассмотрены элементы модели неоднородных дескрипторов для распределенного МД-моделирования, на основе которой строятся методы распределения расчетных потоков данных. Подробно описаны метод равномерной загрузки вычислителей и метод параллельного расчета коррелированной системы N-частиц на графическом процессоре с использованием технологий MPI и CUDA.

В заключение представлены тестовые результаты компьютерных экспериментов.

Ключевые слова: параллельные алгоритмы, высокопроизводительные вычисления, автоматизированные системы научных исследований, молекулярная динамика, шлаковые расплавы.

Введение

В настоящее время особое значение для повышения эффективности научных исследований приобретает автоматизация научного эксперимента, которая позволяет получать достаточно точные и полные модели исследуемых объектов и явлений, значительно сократить время проведения эксперимента, изучать сложные объекты и процессы.

---

* Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации, проект 14.132.21.1792.

Одним из приоритетных направлений современной науки является создание новых металлических материалов с заранее заданными свойствами. В этой области широко применяется компьютерное моделирование (КМ), в том числе метод молекулярной динамики, позволяющий определять целый комплекс свойств (структурные, термодинамические, транспортные) и исследовать взаимосвязи наноструктуры и физико-химических свойств.

С точки зрения математической формализации эти системы описываются классом моделей коррелированных систем N-частиц, требующих специфических методов расчета.

Особенности предметной области таковы, что в настоящее время при последовательном моделировании удается просчитывать за реальное время взаимодействие и групповое поведение систем, содержащих в лучшем случае десятки тысяч частиц. Однако существует ряд задач, в частности связанных с определением пространственных наноразмерных неоднородностей, для которых необходимо увеличение размерности модельной системы до миллиона частиц. Промоделировать подобную систему на локальном компьютере в последовательном режиме практически не удается, т. к. это связано с большими временны́ми затратами: эксперимент может занять несколько месяцев.

Для построения адекватных моделей и получения практически значимых результатов моделирования коррелированных систем N-частиц со сложным многочастичным взаимодействием необходимо увеличение числа модельных частиц до 10^5–10^7, что требует разработки и внедрения новых методов высокопроизводительных вычислений.

Постановка задачи

В рамках компьютерного моделирования выделим важный класс задач, в которых возможно *распределять* вычисления для совокупности объектов, находящихся в определенных отношениях друг с другом. К этому классу относятся и задачи моделирования коррелированных систем N-частиц методом молекулярной динамики (МД).

В физике под коррелированной системой понимается система взаимодействующих объектов (частиц), в которой часть характеристик индивидуального объекта или системы в целом зависит от совокупности характеристик всех остальных объектов. Каждая модельная частица имеет набор сохраняющихся и переменных атрибутов.

В этом случае МД-моделирование представляет собой численное решение краевой задачи Коши; это означает, что в момент времени t=0 задается начальное состояние системы в некоторой ограниченной области пространства (расчетная область), на поверхности которой поддерживаются заданные граничные условия. Моделирование состоит в прослеживании временно́й эволюции этой конфигурации. Основной частью вычисления является цикл по временно́му шагу, в котором состояние физической системы изменяется по времени на малый шаг Δt.

Состояние физической системы определяется атрибутами конечного ансамбля частиц, а эволюция системы определяется законами взаимодействия этих частиц.

Модель неоднородных дескрипторов для распределенного МД-моделирования

В настоящее время разработан ряд программных комплексов, реализующих методы распределенного расчета задач класса N-частиц[2,3,4]. Эти методы основаны на расчете двухобъектных отношений[5,6]. Предметом этой статьи являются методы, основанные на двухобъектных отношениях с учетом трехобъектных и многообъектных отношений[7,8,9].

Особенности концептуальной модели предметной области требуют разработки математической модели, которая обеспечила бы высокопроизводительные вычисления для коррелированных систем со сложным многочастичным взаимодействием, содержащих 10^5–10^7 частиц. В связи с этим авторами разработана модель неоднородных дескрипторов для *распределенного* МД-моделирования коррелированной системы N-частиц.

Основными элементами модели, обеспечивающими возможность распределения расчетов без детализации всех взаимодействий между частицами, являются объект и дескриптор. Под объектом понимается некоторая совокупность частиц исходной коррелированной системы и отношений между ними, выделяемая по определенным правилам и обеспечивающая возможность декомпозиции системы для распределения и распараллеливания расчетов.

Объекты идентифицируются с помощью неоднородных дескрипторов, которые содержат разнотипные элементы описания выделенного объекта, необходимые для распределения расчетов.

Таким образом, система – это совокупность объектов, описываемых неоднородными дескрипторами, расчет которых можно

распределять по совокупности вычислителей, комбинируя полученные результаты по определенной схеме.

На основе концептуальной модели МД-метода и тщательного анализа программного кода legacy application – локального МД-приложения[10,11] построены наборы дескрипторов, описывающих бизнес-логику МД-приложения с точки зрения разделения его кода на блоки, пригодные для распределения.

Выделено два класса: одночастичные дескрипторы ($D1s(i)$, $D1v(i)$) и агрегаторы (двух- и трехчастичные ($D\sum 2(i)$, $D\sum 3(i)$) дескрипторы). Оба класса предполагают возможность параллельного расчета дескрипторов на разных вычислителях. Однако если одночастичные дескрипторы можно произвольно распределять по вычислителям, то агрегаторы (содержат элементы, описывающие перекрестные отношения разных порядков между одночастичными дескрипторами и/или агрегаторами) являются «зависимыми» от одночастичного дескриптора и рассчитываются на том же вычислительном устройстве, где и «родительский» одночастичный дескриптор.

Таким образом, предложенный подход позволяет отвлечься от конкретного наполнения элементов дескрипторов, перенести акцент с описания физических взаимодействий в системе на информационное описание перераспределения потоков данных между дескрипторами.

Метод равномерной загрузки вычислителей

Для обеспечения параллельного расчета коррелированной системы N-частиц авторами разработан метод равномерной загрузки вычислителей в однородной вычислительной среде, в которой каждый вычислитель обладает одинаковой производительностью и имеет свою независимую память.

Равномерная загрузка подразумевает разделение множества на подмножества с мощностью, равной $k = N/p$, где N – количество одночастичных дескрипторов системы, p – количество вычислителей, выполняющих расчет. Эффективной считается загрузка, при которой вычислители завершают расчет дескрипторов одновременно.

Конечной целью расчета каждого вычислителя является получение новых значений элементов одночастичных дескрипторов $\{Dlv(i)\}$, рассчитываемых по формуле (1). Для получения новых значений элемента $\bar{F}_i \in Dlv(...)$ требуется расчет элементов $f_{ij} \in$

$D\sum 2(i)$, в которых идет пересчет отношений i и j элемента, для всех фиксированных i со всеми j и где i ≠ j

$$\overline{F}_i \in Dlv(i) = \sum_{j\neq i}^{N} \overline{f_{ij}} \in D\sum 2(i). \qquad (1)$$

Эта часть расчета имеет квадратную зависимость от числа дескрипторов $\{Dlv(i)\}$ и является самой затратной по времени в процессе моделирования системы. Сократить время расчета можно за счет уменьшения обсчитываемых отношений между дескрипторами.

Для этого применяется алгоритм «диагональной матрицы», в котором элемент $\overline{f_{ij}} \in D\sum 2(i) = -\overline{f_{ij}} \in D\sum 2(i)$. В этом случае время расчета $Dlv\{\overline{F}_i\}$ сокращается в два раза, а количество обсчитываемых отношений становится равным $(N(N\text{-}1))/2$. На рис. 1 наглядно отображен расчет элементов $\overline{f_{ij}} \in D\sum 2(i)$ с использованием алгоритма «диагональной матрицы».

В этом случае количество отношений, которые нужно обсчитывать для накопителя $\sum\overline{f2} \in D\sum 2(1)$, равно N-1, а для $\sum\overline{f2} \in D\sum 2(N)$, равно 0. Следовательно, если формировать рассчитываемые подмножества дескрипторов $\{Dlv(i)\}$ для каждого вычислителя последовательными диапазонами с мощностью N/p, то загруженность вычислителей становится неравномерной. Для равномерной загрузки вычислителей разработан встречный алгоритм выборки дескрипторов в диапазон.

i,j	i_1	i_2	...	i_n
j_1		$-\overline{f_{j_1 i_2}}$	...	$-\overline{f_{j_1 i_n}}$
j_2	$\overline{f_{i_1 j_2}}$		....	$-\overline{f_{j_2 i_n}}$
...	...	...		...
j_n	$\overline{f_{i_1 j_n}}$	$\overline{f_{i_2 j_n}}$	...	

Рис. 1. Применение алгоритма «диагональной матрицы» для расчета элементов двухчастичного дескриптора $D\sum 2(i)$

Подмножества одночастичных дескрипторов $\{Dlv(i)\}$, рассчитываемых каждым вычислителем, формируются по схеме, отображенной на рис. 2.

Все множество дескрипторов разбивается на два интервала [$Dlv(i_1)$, $Dlv(i_{N/2})$] и [$Dlv(i_{N/2+1})$, $Dlv(i_N)$]. Внутри каждого интервала дескрипторы распределяются по номерам, где i_1 – номер первого дескриптора, i_N – номер последнего дескриптора. Количество дескрипторов, содержащихся в рассчитываемом подмножестве и передаваемых каждому вычислителю, равно k.

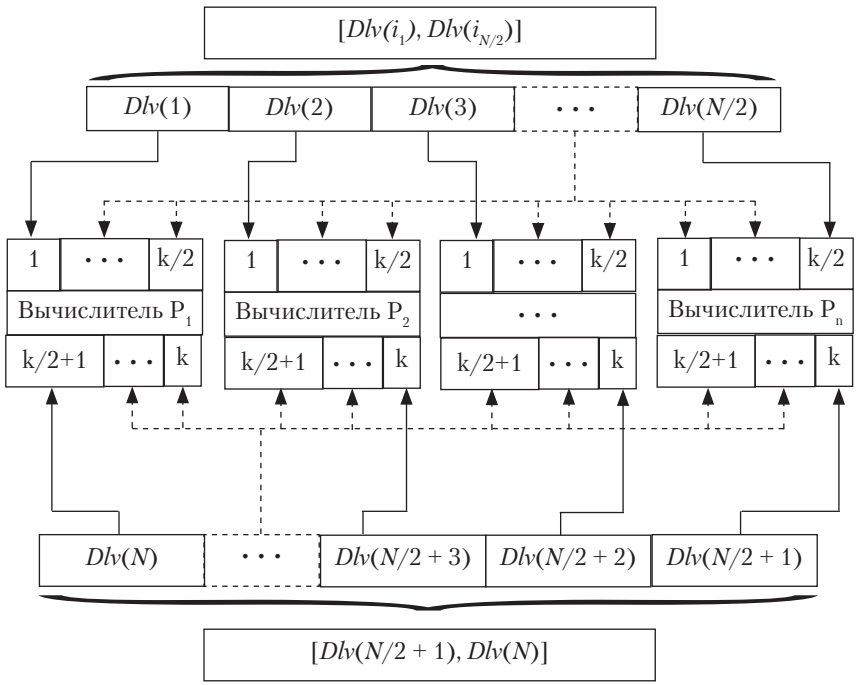


Рис. 2. Формирование подмножеств одночастичных дескрипторов {$Dlv(i)$} с применением встречного расчета

Из номеров дескрипторов, находящихся на интервале [$Dlv(i_1)$, $Dlv(i_{N/2})$], формируется первая половина подмножества, а из номеров интервала [$Dlv(i_{N/2+1})$, $Dlv(i_N$] формируется вторая половина подмножества.

Выборка дескрипторов происходит поочередно: сначала из первого интервала, начиная с $Dlv(i_1)$, затем из второго интервала в обратном направлении с $Dlv(i_N)$. Каждое подмножество получает следующий дескриптор через шаг, равный p. На рис. 2 отображено

распределение дескрипторов между вычислителями с использованием метода равномерной загрузки.

Метод равномерной загрузки вычислителей коррелированной системы N-частиц является оптимальным для однородной вычислительной среды и применяется для параллельного расчета дескрипторов в модели с распределенной памятью. Реализация данного метода в гетерогенной среде, когда совместно используются вычислители разные по типу и производительности, требует доработки, так как из-за разницы в производительности более мощные вычислители, выполнив свои расчеты, простаивают.

В настоящее время разработанный метод равномерной загрузки вычислителей для параллельного расчета коррелированной системы N-частиц проходит апробацию в программном комплексе «MD-SLAG-MELT»[12,13].

Метод параллельного расчета коррелированной системы N-частиц на графическом процессоре

Применение вычислителей на основе графических процессоров (GPU) при параллельном расчете дескрипторов позволит существенно уменьшить время моделирования системы N-частиц.

В разработанном авторами методе учитываются особенности архитектуры графических процессоров NVIDIA и технологии CUDA. Параллельный расчет выполняется большим числом нитей, сгруппированных в блоки. В отличие от вычислителей, реализующих расчеты на центральных процессорах, GPU содержит семь видов памяти, различающихся по размеру, возможности записи и скорости чтения. Графический процессор не выполняет параллельный расчет самостоятельно, функции запуска расчета, отслеживания хода выполнения расчета и передачи дескрипторов в память GPU выполняет центральный процессор.

На рис. 3 представлен алгоритм параллельного расчета одночастичных дескрипторов на GPU.

Все множество значений элементов дескрипторов *{Dlv(i)}* передается в глобальную память (обладает большой вместимостью) GPU из-за большого количества передаваемых данных. В константную и текстурную память передаются дескрипторы *{Dls(i)}*, что позволяет разгрузить глобальную память.

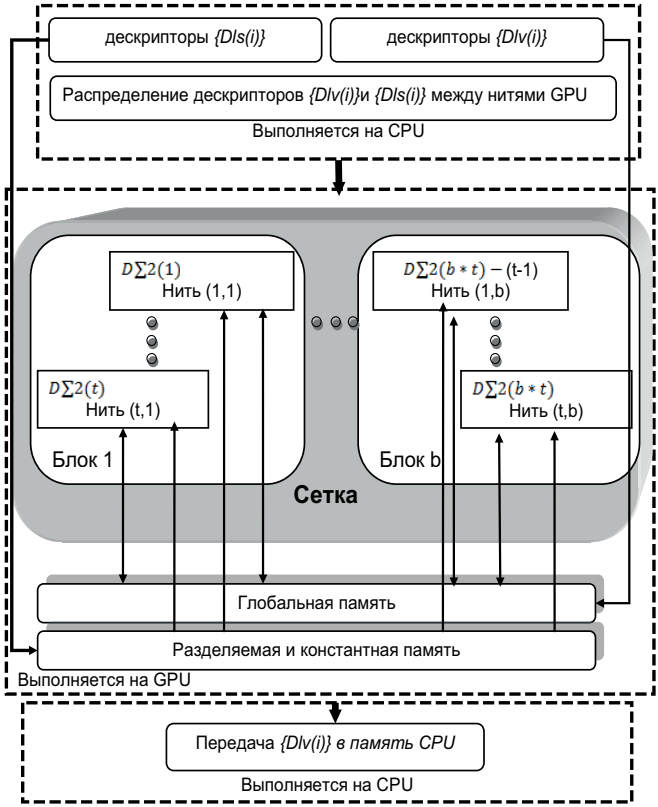


Рис. 3. Алгоритм параллельного расчета одночастичных дескрипторов на GPU

Центральный процессор формирует специальную сетку, состоящую из блоков (b), в которых определяется количество нитей (t), необходимых для расчета. Разделение множеств дескрипторов на подмножества и передача их на нити реализуется с помощью метода равномерной загрузки вычислителей.

Каждая нить производит расчет одного двухчастичного $D\sum 2(i)$-агрегатора и на основе полученных результатов обновляет значения элементов одночастичных векторных дескрипторов.

Для расчета двухчастичных $\{D\sum 2(i)\}$-агрегаторов на графическом процессоре применяется алгоритм «диагональной матрицы». Так как память для всех вычислителей одна, то возможны кон-

фликты записи, когда вычислители обращаются к одному и тому же значению элемента дескриптора. Для этого на каждой итерации результат расчета значений элемента $\overline{f_{ij}} \in D\sum 2(i)$ передается в специальный двумерный накопитель. Так же на каждой итерации цикла производится синхронизация. Расчет будет возобновлен только после прохождения одной итерации расчета значений элемента $\overline{f_{ij}} \in D\sum 2(i)$ всеми нитями.

Тестирование

Для оценки эффективности разработанного метода проведен ряд экспериментов, имитирующих расчет коррелированной системы N-частиц. В экспериментах сравнивается время, затраченное на проведение локального варианта расчета коррелированной системы N-частиц, и параллельный расчет с технологией CUDA. Дескрипторы заполняются тестовыми значениями элементов. Тестирование модели, в основе которой заложен расчет с использованием технологии CUDA, проведено на графическом процессоре GForceGTS 450. Результаты компьютерных экспериментов представлены в табл. 1.

Тестирование реализованных методов производилось на кластере, состоящем из 16 вычислителей Intel Core 2 Duo E6800, а также на видеокарте GEFORCE GTS 450. В табл.1 представлены результаты расчетов коррелированной системы N-частиц с использованием технологии MPI, а в табл. 2 – с использованием технологии CUDA.

Таблица 1

Результаты расчетов коррелированной системы N-частиц, технология MPI

Кол-во частиц		10240	50176	250880	401408
Кол-во вычислителей	Время расчета, с				
2		0,29	7,89	101	361
4		0,23	7,6	76	217
8		0,15	5,1	49	137
16		0,02	4,2	28	71

Таблица 2

Результаты расчетов
с использованием технологии CUDA

Кол-во частиц	10240	50176	250880	401408
Время расчета, с	0,02	0,14	3,53	9,1

Согласно результатам тестирования, серьезное ускорение наблюдается при расчете системы на графическом процессоре GTS 450. Также в модели параллельного расчета коррелированной системы N-частиц для графического процессора заложены процедуры, позволяющие хранить данные в быстрой разделяемой и константной памяти GPU, что существенно сокращает время проведения моделирования.

В настоящее время модель распределенных вычислителей проходит апробацию в программном комплексе ИИС «MD-SLAG-MELT»[14,15].

Выводы

Описанные в статье модели и методы, разработанные для реализации высокопроизводительных вычислений, позволяют существенно расширить круг решаемых задач в рамках молекулярно-динамического моделирования коррелированных многочастичных систем.

Применение этих моделей для legacy application, используемых в такой предметной области, как физическая химия оксидных расплавов, позволит резко увеличить размерность модельных систем и адекватность модельных результатов.

Внедрение разработанных методов высокопроизводительных вычислений в программный комплекс ИИС «MD-SLAG-MELT» предоставляет широкому кругу исследователей возможность удаленного доступа к проведению компьютерного эксперимента и физико-химическим результатам, обладающим прогнозными возможностями.

Примечания

[1] См.: Информационно-исследовательская система «MD-SLAG-MELT» [Электронный ресурс]. URL: http://nano-md-simulation.com (дата обращения: 30.04.2013).

[2] См.: SAGE MD2 [Электронный ресурс]. URL: http://www.sagemd.com/htmls/about_sagemd.htm (дата обращения: 30.04.2013).

[3] См.: HyperChem [Электронный ресурс]. URL: http://www.hyper.com/ (дата обращения: 30.04.2013).

[4] См.: XMD (Molecular Dynamics for Metals and Ceramics) [Электронный ресурс] URL: http://xmd.sourceforge.net/ (дата обращения: 30.04.2013).

[5] См.: *Brown, W.M., Kohlmeyer, A., Plimpton, S.J., Tharrington, A.N.* Implementing molecular dynamics on hybrid high performance computers – Particle-particle particle-mesh // Computer Physics Communications. 2012. Vol. 183. Issue 3. March. P. 449–459.

[6] См.: *Le Grand, S., Götz, A.W., Walker, R.C.* SPFP: Speed without compromise – A mixed precision model for GPU accelerated molecular dynamics simulations // Computer Physics Communications. 2013. Vol. 184. Issue 2. February. P. 374–380.

[7] См.: *Воронова Л.И., Григорьева М.А., Воронов В.И.* Разработка методов компьютерного моделирования наноструктуры многокомпонентных расплавов // Фундаментальные исследования. 2011. № 8 (3). С. 617–622.

[8] См.: *Воронова Л.И., Трунов А.С.* Оптимизация параллельного алгоритма подсистемы распределенного молекулярно-динамического моделирования // Межотраслевая информационная служба. 2011. № 3. С. 1–12.

[9] См.: *Воронова Л.И., Григорьева М.А.* Разработка информационной модели физико-химических свойств расплава для исследовательского программного комплекса MD-SLAGMEL // Межотраслевая информационная служба. 2011. № 2. С. 30–36.

[10] См.: *Воронова Л.И., Григорьева М.А., Воронов В.И., Трунов А.С.* Программный комплекс «MD-SLAG-MELT» для моделирования наноструктуры и свойств многокомпонентных расплавов // Расплавы. 2013. № 2. С. 1–16.

[11] См.: *Voronova L.I., Grigorjeva M.A., Voronov V.I., Trunov A.S.* Computer simulation of the polymerizable oxide melts nanostructure using the descriptor-graph model // Materials Science and Metallurgy Engineering. 2013. № 1. P. 1–12 [Электронный ресурс]. URL: http://pubs.sciepub.com/msme/1/1/1/#12/ (дата обращения: 30.04.2013).

[12] См.: *Voronova L.I., Voronov V.I.* "The Research-Information System 'MD-SLAG-MELT". Certificate of state registration of computer programs № 2012615018 from 05.06.2012.

[13] См.: *Трунов А.С., Воронова Л.И.* «Подсистема распределенного молекулярно-динамического моделирования информационно-исследовательской сис-

темы “MD-SLAG-MELT”». Свидетельство о государственной регистрации программы для ЭВМ, № 2012615017 от 05.06.2012.

14 Там же.

15 См.: *Воронова Л.И., Григорьева М.А., Воронов В.И., Трунов А.С.* Программный комплекс «MD SLAG MELT» информационно-исследовательской системы «Шлаковые расплавы» версии 10.0 // Деп. в ВИНИТИ РАН, 2012. № 29-В2012. С. 16.

Abstracts

A. Anosov

"ACCIDENTAL" TRAFFIC FILTERING METHODS IN DYNAMIC ONLINE RESOURCES

In this paper the principle of administrative monitoring systems automation based on the analysis and traffic filtering module integration in the dynamic part of the web resources is proposed. Main attention is paid to the content filtering module development in the dynamic part of the information-analytical system "American studies in Russia, Russian studies in the United States".

Key words: content filtering, monitoring, negative information, traffic analysis methods.

A. Baranovich

MULTIMODAL CONTENT EVOLUTION CONTROL IN OPEN INFORMATION NETWORKS

For a well-defined class of information and psychological security threats of open cyberspace, which is characterized by intensive development of information and communication mass technology, a promising strategic concept of directed multimodal content evolution in open information networks is being formulated. The concept is based on the information and post-non-classic information and evolutionary approach to systems analysis and objective reality modelling, attribute-ingredient information theory, machine-driven natural language evolution and methodological grounds of crypto-semantics.

Key words: knowledge concentration, attribute-ingredient information theory, cyber security threat, open cyberspace, crypto-semantics, information and evolutionary approach, semantic and axiological filters, controlled evolution.

V. Grigoriev, V. Kuznetsov

ADAPTATION OF THE ROLE ACCESS CONTROL MODEL IN CLOUD COMPUTING SYSTEMS

The approach to a role-based access control model adaptation with reference to the cloud computing systems is offered. 3 models of expansion of a cloudy infrastructure, a private cloud, a public cloud and a hybrid cloud, are considered. The role-based access control model expansion is built on the threats basis model of the suggested cloudy system.

Key words: role-based access control, private cloud, public cloud, hybrid cloud, cloud computing, model of threats.

V. Grigoriev, A. Novikov

CLOUD COMPUTING – THE NETWORK CENTRIC WARFARE STRATEGIC RESOURCE

A global network information infrastructure creation led to radical changes in views of the West political and military establishment at an information epoch war. The concept, corresponding to the general tendency of networking social resources, communications and services, was named the Network Centric Warfare. Occurrence and interpeneter of cloud computing and Web 2.0 technologies stimulated special interest of military-industrial circles to their consideration as a new operational environment for carrying out of the future Network Centric Operations and war operations in global virtual space. Under forecasts of experts these technologies and connected with them global transformation processes will radically influence practically all spheres of civilisation infrastructures of the society: the industry, education and the state activity in approximately the same way as industrial and information revolutions in due time did.

Key words: clouds, cloud computing, virtualization, Cloud Computing Federal Strategy, Network Centric Warfare.

S. Iglitskaya

SEMIOTICS-CHROMATICAL HYPERTOPONETWORKS MODEL PROJECTION ON FIELD OF STRICT STYLE MUSICAL TEXT SYNTHESIS

The article presents the conceptual approach to musical texts models design of different styles on the basis of the information component of a universal model of complex dynamic systems states. The methods of polyphonic musical text models design are proposed. The software implementation of musical strict style monophonic text model is considered.

Key words: musical text, notation, strict style polyphony, k-hyperspace of SH-hypertopograph, SH-hyper-toponetworks.

O. Kazarin, A. Tarasov

MODERN CONCEPTS OF CYBERSECURITY OF LEADING FOREIGN COUNTRIES

Dynamic development of the global information space is connected, on the one hand, with the affordance of unprecedented information opportunities for the humanity, but on the other – with the new threats emergence. There was a new phenomenon – "cyber security", which is associated with concepts such as "cybercrime", "cyber-terrorism", "cyber war". The national information infrastructure secure operation will be most likely determined by the relevant cyber security concepts developed by almost all developed countries and major international organisations. Analysis of the leading foreign countries concepts is the subject of this article.

Key words: global information space, information and communication technologies, information warfare, cyber security.

D. Khankovsky

ABOUT MODELLING PROCESS OF THE PRIMARY STAGE OF KNOWLEDGE CREATION IN THE INTELLIGENT SYSTEM WITH AUTONOMOUS EVOLVING

Within the limits of the information-evolutionary approach to the systems analysis and modelling of objective reality the mechanisms of formation of basic knowledge in the subsystem level knowledge

of intelligent systems “consciousness” – “subconscious” are studied. Essentials for algorithmic implementation of the basic knowledge from the flow information outside are formulated. Article continues a cycle of works about modelling of the universal mechanisms of intellectual activity of various genesis.

Key words: information, thinking, knowledge, intelligence systems, consciousness, subconsciousness.

D. Kondratiev, A. Nenashev, S. Petrov, A. Tarasov

DIGITAL CULTURAL HERITAGE PRESERVATION IN THE CONTEXT OF INFORMATION SECURITY

The article considers on the information security problems in culture generated by the information technology explosive growth in the processes of formation, storage and access to cultural heritage that defines, in fact, the direction of the transition “vector” to a digital representation. From the position of the digital heritage as a complex system the major threats affecting its integrity and availability, as well as the management automation problems are analysed. As one of the cultural institutions development trends the “intelligent museum” concept, including “smart exhibits” which are capable of dialogue with the visitor, is examined.

Key words: culture security, cultural heritage integrity, digital heritage, smart museum, spiritual avatar.

D. Larin

ON THE SOVIET CRYPTOGRAPHERS, CRYPTANALYSTS, RADIO INTERCEPTERS AND OPERATORS CONTRIBUTION INTO THE VICTORY IN KURSK BATTLE. KURSK BATTLE CRYPTOGRAPHY ASPECTS

The 70th anniversary of the Kursk battle (05/07–23/08/1943) falls at the summer of 2013. After the victories of Moscow and Stalingrad, the victory at Kursk was achieved by Soviet soldiers unparalleled heroism and was once the top of the Soviet military triumphant military genius, the defeat in this battle led the Nazi Germany to the strategic initiatives loss. The Soviet army began active offensive operations to liberate the occupied territories and to defeat aggressors completely. A great contribution to the victory at Kursk was made by Soviet

cryptographers, radio interceptors, operators, intelligence and counter-intelligence agents. Radio interceptors and cryptanalysts successfully intercepted and deciphered enemy cipher correspondence. The most valuable cryptographic information came from abroad through intelligence agents. At the same time, communication experts and operators managed encryption services to ensure our communications safety, which were used for army control. Counterintelligence with cryptographers managed to play with the Germans a number of radio quizzes in order to deceive the enemy.

Key words: Kursk battle, cryptography, encryption, decryption, code, encoder, communications.

V. Lekae, V. Chelnokov

THE SYSTEM OF PERSISTENT URL

The article considers the implementation of system for persistent URL. This system is implemented in the library of RSUH. This system was made instead of American PURL-system that did not worked. Also this article includes the concept of mobile library bush that uniforms all resources of library.

Key words: PURL-system, URL, persistent URL, local URL, free software, mobile library bush, Handle-system, DOI.

L. Morozova, M. Pazhdin

SPIRITUAL-INTELLIGENT PERSONALITY DEVELOPMENT AS THE BASIS FOR DESTRUCTIVE INFORMATION-PSYCHOLOGICAL IMPACT PREVENTION IN INFORMATION WARFARE CONTEXT

The article is an attempt to reflect information warfare fundamentals on the Orthodox Church doctrine area, as well as to set the spiritual and intellectual individual development against the destructive informational and psychological influence.

Key words: information warfare, government, individual, Orthodoxy, spiritual and intellectual development.

N. Nikitin

THE PROBLEM OF DYNAMIC LEARNING PROCESS MODELING IN INTELLIGENT SYSTEMS

Within the single-object paradigm of graph theory the SC-hypertopographs merge operation based on reduction of classical union and connection operations in k-hyperspace of SC-hypertopographs and formed the modelling procedure basis is considered. The integrity criteria for knowledge subsystem is proposed. The concepts of a merge operation for graphs, hypergraphs, hypertopographs and SC-hypertopographs are consistently introduced. The synthesis problem of forbidden relationships standards in the semantics model is studied. The designations were introduced in a number of published papers.

Key words: semiotic-chromatic hypertopograph, k-hyperspace of SC-hypertopographs, SC-hypertopographs "merge", knowledge subsystem, decision-making subsystem, knowledge subsystem integrity.

A. Platonova

MATHEMATICAL AND PROCEDURAL MODELS OF MULTIVARIABLE STUDENT EVALUATION FORMATION

Article is devoted to development of multiple parameter student assessment mathematical model and its formation procedural model within information system design of educational activity multiple parameter control on the example of the secondary general education. Offered models differ from existing by what allow to automate student achievements control taking into account 12 controlled parameters groups and 80 control results on these parameters. Models design is one of steps towards design methodology improvement of information support to educational activity information monitoring systems according to modern requirements.

Key words: multiple parameter student assessment, mathematical model, procedural model.

E. Poznyakova

ABOUT THE ORGANISATION OF PROTECTED INTERACTION WITH WEB-RESOURCES BASED ON INFORMATION SYSTEM FUNCTIONAL RECONFIGURATION

The paper discusses the main security challenges of information-analytical system "American studies in Russia, Russian studies in the United States". The method for information security safeguarding based on the information security system functional reconfiguration is proposed.

Key words: safety, stability, information security system, degradation strategy, reconfiguration, information security management.

A. Satunina, L. Sysoeva

THE MANAGEMENT MODELS ANALYSIS FOR SERVICE ORIENTED INFORMATION SYSTEM

The modern management models of service oriented information system are discussed in this article for their systematisation and defining their role in system architecture. These models are analysed considering functions, levels and objects of service oriented information system control.

Key words: management models, service oriented architecture, service oriented information system management.

G. Shevtsova, S. Berezovsky

DIGITAL SIGNATURE TECHNOLOGY IMPLEMENTATION AS CRYPTOGRAPHIC PROTECTION TOOL FOR THE INTERAGENCY ELECTRONIC INTERACTION

The order of digital signature technology application for interagency electronic interaction is considered from the perspective of interagency electronic interaction participants, providing state and municipal services, and executing state and municipal functions in electronic form.

Engineering support of information interaction of agencies and organisations is shown on the example of common technological solutions. The types of digital signatures technology application and verification

in e-mail messages that pass through the nodes of the interagency electronic interaction system are considered, as well as the features of digital signatures and official digital signature authority usage by interagency electronic interaction participants.

The electronic document protection includes technology protection using cryptographic information protection.

Key words: digital signature, qualified key certificate, interagency electronic interaction, data protection.

L. Voronova, A. Trunov, V. Voronov

DEVELOPMENT OF PARALLEL CALCULATION METHODS OF CORRELATED MANY-PARTICLE SYSTEMS ON THE GPU

The article considers the development of high-performance computing methods, implemented in network computing resources in RSUH (information and research system of IMS «MD-Slag-Melt»), allowing to explore the structure and properties of correlated many-particle systems using molecular dynamics. The model elements of heterogeneous distributed descriptors for MD-modelling, on which the methods of computing data flows allocation are based, are provided. Detailed description of the balanced calculators load method and of the parallel calculation method of the correlated N-particle system on the GPU using technologies like MPI and CUDA, is considered.

In conclusion, the test results of computer experiments are presented.

Key words: parallel algorithms, high performance computing, automated research systems, molecular dynamics, slag melts.

V. Zabotkina

INTEGRATION CHALLENGE IN COGNITIVE SCIENCE: POSSIBLE SOLUTIONS

In the article the basic cognitive science concepts, the cognitive science formation process and the Russian scientists contribution, as well as the main challenges facing researchers are considered. The models for solving problems in single framework development, which will determine the relationship between the various disciplines pertaining to cognitive sciences, are proposed.

Key words: cognitive science, integration, interdisciplinary, knowledge generation model, cognition.

S. Zheltov

ADAPTATION OF DISCRETE LOGARITHM PROBLEM SOLUTION BY POLLARD ρ-METHOD TO THE COMPUTING ARCHITECTURE CUDA

The article is devoted to some aspects of organizing parallel computing and the GPGPU technology usage for the discrete logarithm problem solving in a finite field. The main sections are devoted to the review of adaptation Pollard ρ-method for parallel computing on devices with heterogeneous architectures.

Key words: parallel computing, discrete logarithm, architecture CUDA.

Сведения об авторах

Аносов Антон Евгеньевич – аспирант кафедры компьютерной безопасности Института информационных наук и технологий безопасности при Российском государственном гуманитарном университете (ИИНиТБ РГГУ), anosov@rnt.ru.

Баранович Андрей Евгеньевич – доктор технических наук, профессор кафедры компьютерной безопасности ИИНиТБ РГГУ, barae@rambler.ru.

Березовский Сергей Валентинович – преподаватель кафедры организационно-правовой защиты информации ИИНиТБ РГГУ, berezovskiysv@mail.ru.

Воронов Вячеслав Игоревич – кандидат технических наук, доцент кафедры математических методов обработки информации ИИНиТБ РГГУ, vorvi@mail.ru.

Воронова Лилия Ивановна – доктор физико-математических наук, профессор, завкафедрой математических методов обработки информации ИИНиТБ РГГУ, voronova2001@mail.ru.

Григорьев Виталий Робертович – кандидат технических наук, главный научный консультант ЗАО «РНТ», grigorjev_vr@mail.ru.

Желтов Сергей Александрович – старший преподаватель кафедры компьютерной безопасности и математических методов управления Тверского государственного университета, zheltov_s@mail.ru.

Заботкина Вера Ивановна – доктор филологических наук, профессор, проректор по инновационным международным проектам РГГУ, zabotkina@rggu.ru.

Иглицкая Софья Михайловна – аспирант кафедры общей информатики ИИНиТБ РГГУ, sofa.sofa@mail.ru.

Казарин Олег Викторович – доктор технических наук, ведущий научный сотрудник отдела математических проблем информационной безопасности Института проблем информационной безопасности МГУ им. М.В. Ломоносова, okaz2005@yandex.ru.

Кондратьев Дмитрий Вениаминович – кандидат химических наук, председатель правления АНО «Центр поддержки общественных инициатив и социального партнерства “Экклезия”», otdelro.kdv@gmail.com.

Кузнецов Владимир Сергеевич – аспирант МГТУ МИРЭА, kuznecov.vladimir.00@mail.ru.

Ларин Дмитрий Александрович – кандидат технических наук, доцент кафедры интеллектуальных технологий и систем МГТУ МИРЭА, greattzar@yandex.ru.

Лекае Владимир Алексеевич – кандидат химических наук, доцент, завкафедрой информационных технологий факультета информатики ИИНиТБ РГГУ, valek41@yandex.ru.

Морозова Лидия Владимировна – слушатель богословских курсов Высоко-Петровского ставропигиального мужского монастыря, krona-12@mail.ru.

Ненашев Александр Николаевич – кандидат юридических наук, помощник министра культуры Российской Федерации, nan@mkrf.ru.

Никитин Никита Олегович – аспирант кафедры общей информатики ИИНиТБ РГГУ, nikita-fin@yandex.ru.

Новиков Андрей Алексеевич – кандидат технических наук, старший научный сотрудник, генеральный директор ЗАО «РНТ», novikov_an@rnt.ru.

Паждин Михаил Юрьевич – старший преподаватель МГТУ МИРЭА, rescue44@mail.ru.

Петров Сергей Томасович – главный редактор журнала «Цифровое наследие», 5008604@gmail.com.

Платонова Алла Сергеевна – соискатель кафедры «Физика и прикладная математика» Муромского института (филиала) Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых, allaplatonova@inbox.ru.

Познякова Екатерина Игоревна – аспирант кафедры компьютерной безопасности ИИНиТБ РГГУ, e.poznyakova@gmail.com.

Сатунина Анна Евгеньевна – кандидат экономических наук, ведущий научный сотрудник, декан факультета информатики ИИНиТБ РГГУ, aesat@mail.ru.

Сысоева Леда Аркадьевна – кандидат технических наук, доцент, директор Центра дистанционных технологий обучения РГГУ, leda@rggu.ru.

Тарасов Александр Алексеевич – доктор технических наук, профессор, директор Института информационных наук и технологий безопасности РГГУ, aa_tarasov@list.ru.

Трунов Артем Сергеевич – аспирант кафедры общей информатики ИИНиТБ РГГУ, greek17@yandex.ru.

Ханковский Дмитрий Борисович – аспирант кафедры общей информатики ИИНиТБ РГГУ, viperdima89@mail.ru.

Челноков Валерий Павлович – кандидат физико-математических наук, доцент кафедры прикладного программного обеспечения МГТУ МИРЭА, chelnokov@mirea.ru

Шевцова Галина Александровна – кандидат исторических наук, доцент кафедры организационно-правовой защиты информации ИИНиТБ РГГУ, shevtsova-g@rambler.ru.

General data about the authors

Anosov Anton E. – postgraduate student, Department of Computer Security, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, anosov@rnt.ru.

Baranovich Andrey E. – Ph.D. in Engineering, professor, Department of Computer Security, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, barae@rambler.ru.

Berezovsky Sergey V. – lecturer, Department of Organizational and Legal Information Protection, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, berezovskiysv@mail.ru.

Chelnokov Valery P. – Ph.D. in Physics and Mathematics, associate professor, Department of Application Software, Moscow State Technical University of Radio Engineering, Electronics, and Automation, chelnokov@mirea.ru.

Grigoriev Vitaly R. – Ph.D. in Engineering, main scientific consultant, RNT cjsc, grigorjev_vr@mail.ru.

Iglitskaya Sofya M. – postgraduate student, Department of General Informatics, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, sofa.sofa@mail.ru.

Kazarin Oleg V. – Dr. in Engineering, leading researcher, Department of Mathematical Problems of Information Security, Institute for Information Security Issues, Lomonosov Moscow State University, okaz2005@yandex.ru.

Khankovsky Dmitry B. – postgraduate student, Department of General Informatics, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, viperdima89@mail.ru.

Kondratiev Dmitry V. – Ph.D. in Chemistry, chief, Autonomous non-profit organisation «Center for Support of Public Initiatives and Social Partnership "Ecclesia"», otdelro.kdv@gmail.com.

Kuznetsov Vladimir S. – postgraduate student, Moscow State Technical University of Radio Engineering, Electronics, and Automation, kuznecov.vladimir.00@mail.ru.

Larin Dmitry A. – Ph.D. in Engineering, associate professor, Department of Intellectual Technologies and Systems, Moscow State Technical

University of Radio Engineering, Electronics, and Automation, greattzar@yandex.ru.

Lekae Vladimir A. – Ph.D. in Chemistry, associate professor, head, Department of Information Technologies, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, valek41@yandex.ru.

Morozova Lidia V. – theological courses listener, High Monastery of St. Peter, krona-12@mail.ru.

Nenashev Alexander N. – LLM, assistant of Minister of culture of the Russian Federation, nan@mkrf.ru.

Nikitin Nikita O. – postgraduate student, Department of Computer Science, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, nikita-fin@yandex.ru.

Novikov Andrey A. – Ph.D. in Engineering, senior researcher, general director, RNT cjsc, novikov_an@rnt.ru.

Pazhdin Mikhail Yu. – senior lecturer, Moscow State Technical University of Radio Engineering, Electronics, and Automation, rescue44@mail.ru.

Petrov Sergey T. – editor-in-chief, magazine «Digital Heritage», 5008604@gmail.com.

Platonova Alla S. – applicant, Department "Physics and Applied Mathematics", Murom Institute (branch), Vladimir State University named after Alexander and Nikolay Stoletovs, allaplatonova@inbox.ru.

Poznyakova Ekaterina I. – postgraduate student, Department of Computer Security, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, e.poznyakova@gmail.com.

Satunina Anna E. – Ph.D. in Economics, leading researcher, dean, Faculty of Computer Science, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, aesat@mail.ru.

Shevtsova Galina A. – Ph.D. in History, associate professor, Department of Organisational and Legal Information Protection, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, shevtsova-g@rambler.ru.

Sysoeva Leda A. – Ph.D. in Engineering, associate professor, director, Center for Distance Learning Technologies, Russian State University for the Humanities, leda@rggu.ru.

Tarasov Alexander A. – Dr. in Engineering, professor, director, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, aa_tarasov@list.ru.

Trunov Artem S. – postgraduate student, Department of General Informatics, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, greek17@yandex.ru.

Voronov Vyacheslav I. – Ph.D. in Engineering, associate professor, Department of Mathematical Methods of Information Processing, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, vorvi@mail.ru.

Voronova Lylia I. – Dr. in Physics and Mathematics, professor, head, Department of Mathematical Methods of Information Processing, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, voronova2001@mail.ru.

Zabotkina Vera I. – Dr. in Philology, professor, vice-rector for International Innovative Projects, Russian State University for the Humanities, zabotkina@rggu.ru.

Zheltov Sergey A. – senior lecturer, Department of Computer Security and of Mathematical Methods of Management, Tver State University, zheltov_s@mail.ru.

Заведующая редакцией *И.В. Лебедева*

Художник *В.В. Сурков*

Художник номера *В.Н. Хотеев*

Корректор *О.Н. Картамышева*

Компьютерная верстка *Н.В. Москвина*

Формат 60×90 1/16
Усл. печ. л. 16,5. Уч.-изд. л. 17,3.
Тираж 1050 экз. Заказ № 183

Издательский центр
Российского государственного
гуманитарного университета
125993, Москва, Миусская пл., 6
www.rggu.ru
www.knigirggu.ru