СИСТЕМЫ ВЫСОКОЙ ДОСТУПНОСТИ

№ 4, т. 13, 2017

Highly available systems

Журнал включен в перечень ВАК

Журнал издается под научно-методическим руководством Федерального исследовательского центра «Информатика и управление» Российской академии наук.

СОДЕРЖАНИЕ

Ресурсно-сервисная модель эксплуатации информационно-телекоммуникационных систем ***Быстров И.И., Радоманов С.И., Сычев В.Н.***	**3**	**12**
Автоматическое выявление угроз обществу и государству в социальных сетях и средствах массовой информации ***Захаров В.Н., Садовников Д.А., Смирнов М.В., Хорошилов А.А.***	**13**	**17**
Оценка эффективности использования методов интеллектуального анализа данных при обеспечении информационной безопасности облачных вычислительных сред ***Борохов С.В., Кейер П.А.***	**18**	**24**

CONTENTS

Resource-service model of the information and telecommunication systems maintenance ***Bystrov I.I., Radomanov S.I., Sychev V.N.***	**3**	**12**
Automatic detection of threats to society and the state in social networks and the media ***Zakharov V.N., Sadovnikov D.A., Smirnov M.V., Khoroshilov A.A.***	**13**	**17**
Estimation of the effectiveness of using methods of data mining with the provision of information security of cloud computing environments ***Borokhov S.V., Keyer P.A.***	**18**	**24**

Применение технологии блокчейна и криптовалюты для обеспечения работ по государственному оборонному заказу ***Правиков Д.И., Щербаков А.Ю.***	**25**	**30**	The use of blockchain and cryptocurrency technology to support work on the state defense order ***Pravikov D.I., Scherbakov A.Yu.***
Синтез универсальной изолированной криповалютной сети ***Домашев А.В., Щербаков А.Ю.***	**31**	**38**	Synthesis of universal isolated cryptocurrency network ***Domashev A.V., Scherbakov A.Yu.***
Способ управления доступом к системе обработки больших данных на основе использования маркера потока в заголовке IP-пакета шестой версии ***Будзко В.И., Мельников Д.А., Фомичев В.М.***	**39**	**48**	The mechanism of access control to big data processing system based on using the IPv6 header «flow label» field ***Budzko V.I., Melnikov D.A., Fomichev V.M.***
Проблемы использования оптической и радиолокационной информации (ОРИ), интегрированной в ХОРИАЗ, и пути их решения ***Будзко В.И., Беленков В.Г., Сметанин Н.Н., Улитенков М.В., Зеленикин А.А.***	**49**	**58**	Problems of the integrated into ORISAZ optical and radar information (ORI) use and their solutions ***Budzko V.I., Belenkov V.G., Smetanin N.N., Ulitenkov M.V., Zelenikin A.A.***
Подходы к стабилизации систем с периодическими коэффициентами ***Фомичев В.В.***	**60**	**67**	Approaches to stabilization of systems with periodic coefficients ***Fomichev V.V.***
Результаты анализа перспектив развития геоинформационных систем ***Воронин А.В.***	**68**	**75**	Results of analyzing geoinformation systems perspectives ***Voronin A.V.***
Выбор архитектуры системы хранения данных при создании информационного комплекса «Специализированная информационная среда «Биоресурсные Коллекции» на основе критерия обеспечения высокой доступности ***Мальцев Д.А., Галимов Ю.Ю., Сигаев Д.В., Луньков С.В.***	**76**	**80**	Choice of the architecture of the data storage system when creating the information complex «Specialized information environment «Bioresource Collections» on the basis of the criterion of ensuring high availability ***Maltsev D.A., Galimov Yu.Yu., Sigaev D.V., Lunkov S.V.***

Все статьи, представленные в данном выпуске журнала, соответствуют номенклатуре специальностей научных работников (Приказ Минобрнауки РФ от 11.08.2009 № 294) по отраслям технических наук.

Journal «Sistemy' vy'sokoj dostupnosti» («Highly available systems»).
The journal covers scientific and engineering problems of ensuring confidentiality, availability, and integrity for the class of information-telecommunication systems of high availability (HA ITS), which contain such critical technologies of development

Необходимую информацию о журнале и полный список опубликованных статей, а также аннотации к ним Вы найдете на нашем сайте http://www.radiotec.ru

Учредитель: ООО «Издательство «Радиотехника».

Лицензия № 065229. Свидетельства о регистрации ПИ № ФС 77-25037 от 12 июля 2006 г.
Сдано в набор 25.08.2017 г. Подписано в печать 28.09.2017 г.
Печ. л. 10. Тираж 400 экз. Изд. № 118.
Адрес Издательства «Радиотехника»: 107031, Москва, К-31, Кузнецкий мост, д. 20/6. Тел./факс 621-4837.
E-mail: info@radiotec.ru
http: // www. radiotec.ru /

Дизайн и допечатная подготовка ООО «САЙНС-ПРЕСС».
Отпечатано в ФГУП Издательство «Известия». 127254, ул. Добролюбова, д. 6. Контактный телефон (495) 650-38-80. Заказ №.

ISSN 2072-9472

УДК 004

Ресурсно-сервисная модель эксплуатации информационно-телекоммуникационных систем

И.И. Быстров – д.т.н., профессор, зав. отделом, Институт проблем информатики ФИЦ ИУ РАН (Москва)
E-mail: ibystrov@ipiran.ru
С.И. Радоманов – науч. сотрудник, Институт проблем информатики ФИЦ ИУ РАН (Москва)
E-mail: radomanov@list.ru
В.Н. Сычев – к.в.н., профессор, гл. специалист, центр научно-технической поддержки,
АО «НИИАА» им. В.С. Семенихина (Москва)
E-mail: svn.niiaa@yandex.ru

Рассмотрены концептуальные основы применения ресурсно-сервисной модели (РСМ) для создания системы эксплуатации (СЭ) современных мультисервисных информационно-телекоммуникационных систем (ИТС), а также основные проблемы деятельности ИТ-служб по реализации этой модели на базе «лучших мировых практик». Предложен подход, закладывающий методологическую основу повышения деятельности автоматизированных коммерческих, финансовых, военных и государственных органов управления за счет создания в их инфраструктуре эффективной РСМ СЭ, которая обеспечивает поддержку соответствия ИТ-услуг изменяющимся потребностям управления в различных условиях обстановки.

Ключевые слова: *информационно-телекоммуникационная система (ИТС), ресурсно-сервисная модель системы эксплуатации, системно-процессный подход, контент ИТ-сервиса, поддержка эксплуатации ИТС, поддержка ИТ-услуг, эксплуатационные риски, ИТ-служба.*

This article discusses the conceptual basis for the use of the resource and service model (RSM) to create a system for modern multiservice telecommunication systems (ITS) maintenance, and the main problems of IT-services for the implementation of this model based on «global best practices». The proposed approach creates the methodological basis of improvement of the commercial, financial, military and public administration organs automated activities through the creation in their infrastructure some effective resource and service system of operation (RS MS), which provides support for matching of IT-services with the changing needs of management in various conditions.

Keywords: *information and telecommunications system (ITS), resource-service maintenance, system and process approach, IT-service content, IT-services support, operational risks, IT-service.*

Ц е л ь р а б о т ы – рассмотреть концептуальные основы применения ресурсно-сервисной модели (РСМ) для создания системы эксплуатации (СЭ) современных мультисервисных информационно-телекоммуникационных систем (ИТС).

Концептуальные основы создания ресурсно-сервисной модели системы эксплуатации информационно-телекоммуникационных систем

Появление современных информационных технологий (ИТ) и высоконадежной элементной базы привело к созданию нового класса АСУ типа мультисервисных ИТС, которые интегрируют в себя информационные и телекоммуникационные составляющие различных систем и сетей с опорой на взаимосвязанную совокупность центров обработки информации (ЦОИ) с предоставлением широкого спектра ИТ-услуг пунктам управления, ситуационным центрам и конечным пользователям для выполнения ими своих функциональных обязанностей. Эти системы получают широкое распространение во всех крупных коммерческих, финансовых, военных и государственных органах управления. С каждым годом возрастает роль и парадигма использования ИТС в деятельности этих органов. В зависимости от уровня зрелости они все больше и больше превращаются в автоматизированные органы (АО), когда количество и качество информационных и телекоммуникационных ИТ-услуг ИТС становится критическим фактором эффективности их деятельности. Это приводит к тому, что применение средств автоматизации выходит за границы традиционного подхода, связанного с решением отдельных информационно-аналитических задач. ИТС становится неотъемлемой частью и важным инструментом достижения целей органов управления. От эффективности применения ИТС стала зависеть вся жизнедеятельность органов управления. Переход к «ручным» методам управления становится проблематичным. Конечным продуктом разработки и применения ИТС становятся ИТ-услуги, которые система способна предоставить конечным пользователям в процессе ее эксплуатации. Повышается взаимосвязь между подразделениями информатизации и функциональными подразделениями

органов управления. Все это приводит к возрастанию роли СЭ в жизнедеятельности АО, на нее ложится вся ответственность за использование ИТС по назначению.

В настоящее время в организациях РФ реализуется ресурсная модель управления эксплуатацией ИТС. В этой модели основное внимание уделяется поиску и устранению неисправностей в техническом и программном обеспечении, приводящих к возникновению сбоев и нештатных ситуаций (НШС), нарушающих функциональные процессы систем (сетей) и подсистем, а также процессы решения функциональных задач. Данная модель в силу целого ряда обстоятельств не может в полной мере обеспечить процесс поддержки АО на базе современных мультисервисных систем, реализующих концепцию РСМ. При ресурсной модели эксплуатации ИТС из сферы эксплуатации выпадает ответственность за непрерывность поддержки эксплуатации процессов предоставления и контроля доступа пользователей к ИТ-сервисам и ИТ-услугам. Возникает объективная необходимость создания в АО интегрированной организационно-технической инфраструктуры, объединяющей в единое целое процессы функциональной деятельности органов управления, процессы использования ресурсно-сервисных возможностей ИТС и организацию их эффективной эксплуатации. Одним из путей решения этой проблемы является переход от ресурсной модели эксплуатации к РСМ эксплуатации ИТС. Главная цель перехода на РСМ заключается в том, чтобы в максимальной степени использовать информационный и технологический потенциал ИТС для удовлетворения профессиональной деятельности органов управления. РСМ позволяет описывать взаимосвязь между ресурсно-сервисными возможностями ИТС и потребностями органов управления в ИТ-сервисах и ИТ-услугах (далее сервисы и услуги). Она создает основу для построения современной РСМ СЭ ИТС, обеспечивающей управление процессами формирования, предоставления и контроля услуг на всем жизненном цикле применения ИТС. Принципиальное отличие РСМ эксплуатации от ресурсной заключается в том, что она преследует цель комплексной поддержки эксплуатации ИТС, то есть обеспечивает пользователю требуемый уровень услуг от точки контакта с ним до технической поддержки работоспособности всех составных частей (компонентов) ИТС, участвующих в формировании сервисов, на базе которых реализуются услуги. Переход от существующей системы ресурсной модели эксплуатации к СЭ ИТС на базе РСМ позволяет с учетом имеющегося опыта ресурсной эксплуатации АСУ строить комплексный процесс ресурсно-сервисной технической поддержки жизненного цикла ИТС в соответствии с требованиями «лучших мировых практик» типа Information Technology Infrastructure Library (ITIL), Microsoft Operations Framework (MOF) и международных стандартов обеспечения непрерывности и доступности услуг [1−3].

РСМ СЭ представляет собой взаимосвязанную совокупность методов, средств и эксплуатационного персонала, обеспечивающего оперативно-техническое управление (ОТУ) и техническую поддержку эксплуатации (ТПЭ) информационных, вычислительных, телекоммуникационных ресурсов ИТС, формируемых на их основе сервисов и предоставляемых пользователям услуг для обеспечения непрерывной доступности услуг пользователям АО, выполняющим задачи своей профессиональной деятельности. РСМ СЭ ИТС обеспечивает решение следующих задач:

поддержание единой точки контакта между конечными пользователями ИТС, специалистами, обеспечивающими ОТУ и ТПЭ, и ресурсно-сервисными возможностями системы;

ОТУ процессами непрерывной доступности предоставления, контроля и эксплуатации ресурсов, сервисов и услуг пользователям на всем этапе жизненного цикла деятельности АО;

техническая поддержка эксплуатации ИТС и ее составных частей с целью восстановления функциональности прерванных процессов бесперебойного обслуживания пользователей при возникновении деструктивных факторов и чрезвычайных ситуаций;

организационно-техническая минимизация рисков, порождаемых ИТС в деятельности АО.

РСМ СЭ создается с учетом следующих принципов [4]:

системотехническое объединение функциональности процессов формирования сервисов для предоставления контента услуг профессиональным потребностям пользователей;

создание единой информационно-технической среды управления АО и ИТС;

максимальное соответствие инфраструктуре ИТС и ресурсным возможностям ее компонент с учетом их территориально-распределенного размещения;

применение в процессе эксплуатации комплексной централизованной технологии, объединяющей функции управления ИТС, формирования сервисов, поставщика услуг, ОТУ непрерывностью функцио-

нирования, технической поддержкой эксплуатации систем (сетей), подсистем и технических средств и программных средств (продуктов), средств по обеспечению безопасности ИТС и защите информационных и технических ресурсов;

координация эксплуатационной деятельности основных и резервных объектов и субъектов деятельности ИТС;

применение в процессе эксплуатации ИТС общесистемной методики централизованного мониторинга, комплексного тестирования, анализа состояния систем, ресурсов, сервисов и услуг;

прогнозирование возникновения деструктивных факторов (угроз) и порождаемых ими рисков для ИТС и ее компонентов и осуществление организационно-технических мероприятий, исключающих вероятности их воздействия на процесс предоставление услуг;

ОТУ поддержанием в актуальном состоянии процессов перевода систем и средств «холодного», «теплого» и «горячего» резервирования объектов эксплуатации составных частей ИТС в рабочее состояние;

применение комплекса мер по внедрению и использованию современных методик обеспечения отказо- и катастрофо-устойчивости ИТС на основе рекомендаций отечественных и международных стандартов в области менеджмента непрерывности функционирования АО.

Создаваемая на базе РСМ СЭ ИТС должна удовлетворять следующим требованиям:

обеспечивать соответствие всех процессов эксплуатации рекомендациям международных и национальных стандартов по обеспечению непрерывности функционирования ИТС с учетом требований АО;

обеспечивать непрерывную ресурсно-сервисную поддержку доступности услуг, предоставляемых сервисами ИТС конечным пользователям, функциональным подразделениям и эксплуатационному составу системы;

обеспечивать эксплуатационную поддержку и контроль состояния резервных процессов, составных частей технической, информационной инфраструктуры, резервных объектов и субъектов управления;

обеспечивать мониторинг и постоянный контроль состояния средств противодействия угрозам, нарушающим отказо- и катастрофо-устойчивость ИТС;

осуществлять непрерывное ОТУ состоянием и готовностью систем (сетей), подсистем, технических и программных средств (основных и резервных) по ресурсно-сервисному обеспечению услуг в различных условиях обстановки;

обеспечивать ТПЭ аппаратно-программных средств, процессов технологической, информационной и операционной безопасности предоставляемых услуг конечным пользователям;

осуществлять ликвидацию сбоев, НШС и восстановление штатного режима функционирования составных частей ИТС в установленные сроки.

Учитывая, что процесс создания РСМ СЭ носит практический прикладной характер и основывается в значительной мере на существующих подходах построения ИТС и нормативных источниках (стандартах, рекомендациях и т.п.), сначала дадим несколько частных определений понятиям РСМ СЭ. ИТС состоит из следующих основных функциональных компонент, на базе которых формируются сервисы: информационные системы, транспортные системы прикладного уровня, телекоммуникационные системы, вспомогательные системы, системы контроля и управления, системы безопасности и защиты, СЭ. Аппаратно-программное информационно-лингвистическое наполнение компонентов ИТС представляет собой ресурс, который можно определить как совокупность технических, программных средств, средств информационного обеспечения, функциональных процессов и всего, что может способствовать формированию сервисов в интересах пользователей системы. Сервис является базовым понятием РСМ СЭ и представляет собой логически завершенную совокупность ресурсов и технологических процессов, которые могут быть предоставлены пользователям АО как результат функционирования ИТС для восприятия его пользователем в виде услуги. При этом следует различать несколько видов сервисов:

системные сервисы, на базе которых формируются информационные и технологические услуги, предоставляемые внутренним и внешним пользователям функциональных подразделений АО;

управленческие сервисы, на базе которых формируются услуги в интересах управления составными частями ИТС;

технологические сервисы, определяющие методы и средства обеспечения технической эксплуатации ресурсов, процессов функционирования компонентов ИТС и ОТУ системой поддержки эксплуатации (этот вид сервисов ориентирован на эксплуатацию компонентов, процессов формирования сервисов и зависит от инфраструктуры ИТС, ее проектных и эксплуатационных активов).

В качестве услуги рассматривается конечный продукт реализации сервисных возможностей ИТС, используемых пользователями и эксплуатирующим персоналом для удовлетворения потребностей профессиональной деятельности. В частности, основными услугами, формируемыми на базе сервисов, для большинства органов управления являются: электронная почта, локальные вычислительные сети, процессы хранения и резервирования информации, широкий спектр приложений (моделей и задач), процессы сбора и обработки данных, знаний, запросов, заказов, терминальный доступ, удаленный защищенный доступ, сервис сетевой печати, файловые ресурсы и т.п. Каждая услуга имеет свое смысловое содержание (контент), определяемое информационным и техническим наполнением на базе сервисов. Сервис и услуга рассматриваются как товарный продукт использования ИТС по предназначению. Часто в технических материалах эти понятия рассматриваются как синонимы, и используется универсальный термин сервис, исходя из того, что английское слово «service» переводится на русский и как «сервис», и как «услуга». Однако между ними есть различие: сервис – это потенциальная возможность системы, а услуга – реализованный (воспринятый) пользователем сервис для удовлетворения своих профессиональных потребностей. В тексте будем употреблять термины сервис и услуга с учетом изложенного различия между ними.

Основными объектами РСМ СЭ являются ресурсы систем (сетей), подсистем, программно-технических комплексов (ПТК), комплексов средств автоматизации (КСА), средств защиты информации (СЗИ), сервисов и процессов поддержки услуг, функциональность которых приводит к нарушению непрерывности и доступности услуг, их устойчивости, а также порождению эксплуатационных рисков СЭ и рисков в деятельности органов управления. Субъектами РСМ СЭ являются поставщики ресурсов, сервисов и услуг ИТС. В качестве субъектов выступают специалисты подразделений информатизации, осуществляющих управление жизненным циклом ИТС на этапе ее эксплуатации. При формировании облика РСМ СЭ учитываются следующие особенности объектов эксплуатации ИТС и требования органов управления:

иерархическая организация ИТС, в которой централизованная обработка и единое управление ресурсами на верхнем уровне сочетаются с распределенной обработкой на нижнем;

модульное построение ИТС, предполагающее существование множества различных типов архитектурных решений в рамках единого комплекса;

экономия ресурсов системы (в самом широком понимании этого термина) за счет централизации хранения и обработки данных на верхних уровнях иерархии;

наличие эффективных централизованных средств сетевого и системного администрирования, позволяющих осуществлять сквозной контроль за функционированием сети и управление на всех уровнях иерархии, а также обеспечивающих необходимость, гибкость и динамическое изменение конфигурации системы;

территориальная распределенность объектов эксплуатации ИТС, топологическая структура которой включает центральный и региональный уровни, причем региональный уровень включает в себя системы (сети), подсистемы, технические и программные средства ИТС, которые могут быть распределены по любым регионам страны;

тенденция к использованию универсальных сетевых платформ, уникального многофункционального оборудования и к эффективной модернизации устаревшего;

постоянное расширение видов, количества и качества сервисов и услуг;

преимущественное использование в существующих системах различных аппаратно-программных средств зарубежного производства и конструктивного построения;

широкий спектр систем и средств связи;

сокращение жизненного цикла оборудования в связи с моральным старением или снятием с производства.

Основными ресурсами ИТС, требующими эксплуатационной поддержки, являются:

информационные активы и функциональные процессы АО;

системные ресурсы функциональных систем, подсистем и КСА ИТС;

ресурсы наземных первичных сетей связи, спутниковых сетей связи, системы документального обмена, сетей ведомственной телефонной связи, систем видеоконференцсвязи, региональных систем связи и передачи данных и др.;

ресурсы основной и резервной систем управления, центров и пунктов управления ИТС;

ресурсы системы обеспечения безопасности и защиты информации;

ресурсы системы эксплуатации, КСА системы эксплуатации;

ресурсы вспомогательных систем: вентиляции и кондиционирования воздуха, гарантированного и бесперебойного электроснабжения, пожаротушения, оповещения, пожарной сигнализации и др.

Центральное место при переходе к РСМ СЭ широкомасштабных мультисервисных ИТС занимают вопросы семантической и технической интероперабельности ресурсов разнородных аппаратно-программных платформ многофункциональных систем и сетей и их интеграции в единый сервис. Ключевым моментом в определении уровня интеграции разнородных ресурсов в единый сервис является фактор углубления и системотехнического объединения функциональных процессов и компонентов ИТС в единое целое за счет применения системно-процессуального подхода посредством согласования технических и функциональных характеристик, входной и выходной информации. Несмотря на то, что конкретный набор сервисов и услуг всегда зависит от особенностей построения ИТС, потребностей органов управления, его возможностей и уровня автоматизации, тем не менее, можно выделить базовые характеристики общей оценки процессов их формирования. В частности, к ним относятся:

функциональность, связанная с предметной областью автоматизации органа управления и решаемыми задачами;

производительность, характеризующая то, насколько сервис соответствует требованиям оперативности и масштабу предоставляемых услуг;

непрерывность, характеризующаяся средним временем наработки сервиса на отказ, то есть временем между двумя сбоями или отказами;

доступность – период времени, в течение которого услуга, сформированная на базе данного сервиса, реально работает;

время обслуживания – период времени, в течение которого подразделения эксплуатации несут ответственность за работу сервиса и предоставление пользователю услуги;

контентность сервиса (услуги) – степень соответствия содержания сервиса (услуги) потребностям пользователя;

конфиденциальность – вероятность несанкционированного доступа к ресурсам, данным и средствам защиты с использованием сервиса;

масштабность сервиса, характеризующаяся объемом и сложностью работ по формированию сервиса и поддержки услуг на базе ресурсных возможностей ИТС;

затраты – стоимость всех ресурсов ИТС, задействованных для формирования и оказания услуг, а также минимизации рисков, порождаемых сбоями и отказами в их предоставлении.

Функционально-структурная организация ИТ-службы при ресурсно-сервисной модели системы эксплуатации информационно-телекоммуникационных систем

Для решения задач, стоящих перед АО, в составе РСМ СЭ создается специальная ИТ-служба, объединяющая сотрудников, занимающихся формированием сервисов, предоставлением пользователям услуг и ТПЭ ИТС. Создание ИТ-службы при РСМ СЭ ИТС предполагает выполнение целого комплекса работ, связанных с централизованным характером задач, решаемых органами управления и СЭ. ИТ-служба организует свою работу по следующим функциональным направлениям:

планирование и организация ОТУ процессами ресурсно-сервисной эксплуатации ИТС;

предоставление и сопровождение услуг в соответствии с требованиями пользователей к уровню обслуживания (Service level agreement – SLA) на базе единой точки контакта;

координация и разрешение конфликтов, ликвидация сбоев, НШС и предотвращение рисков, порождаемых нарушениями процессов эксплуатации ИТС;

прогнозирование появления уязвимых мест в инфраструктуре ИТС, угроз и различных видов кибератак на процессы непрерывности и доступности сервисов и услуг.

Существует д в а в а р и а н т а организационного построения ИТ-службы в условиях конкретного АО:

выполнение всего комплекса работ по созданию РСМ СЭ ИТС силами собственной ИТ-службы органа управления;

делегирование части функций ИТ-службы, в основном по технической эксплуатации, специализированным организациям, имеющим опытный персонал, тестовые стенды и инструментарий для определения и устранения сбоев, НШС и отказов в технических и программных средствах системы.

В связи с широким спектром задач, которые необходимо решать СЭ автоматизированных ОВГУ в свете требований международных и национальных стандартов, ИТ-служба при организации РСМ СЭ ИТС строится на трех организационно-функциональных уровнях.

1. *Уровень поддержки функциональной деятельности АО*. Подразделения эксплуатации этого уровня призваны обеспечить гарантированную и бесперебойную интеллектуальную поддержку точки контакта между ИТС и потребителями в процессе повседневного использования услуг. Создаваемые на этом уровне подразделения ИТ-службы представляют собой Центр интеллектуальной поддержки (ЦИП) услуг. ЦИП придается статус Центра диспетчеризации и компетенции, обеспечивающего в АО единую ресурсно-сервисную политику использования ИТС и контроль процессов сбора информации, необходимой для формирования контента услуг. В общем случае ЦИП является функционально-структурной единицей, интегрированной в инфраструктуру органа управления и предназначенной для предоставления услуг и обработки обращений пользователей к единой точке контакта с ресурсно-сервисными возможностями ИТС, которая выступает в роли поставщика сервисов. Впервые идея такого центра была описана в рекомендациях библиотеки ITIL в виде центра поддержки услуг для пользователей по технологии Service Desk [1].

2. *Уровень ОТУ сервисами и услугами*. Подразделения этого уровня призваны обеспечить ОТУ процессами устойчивости систем (сетей), подсистем, технических и программных средств и средств превентивной защиты к непрерывному предоставлению сервисов в ЦИП с минимизацией эксплуатационных рисков, связанных с предупреждением и разрешением локальных сбоев, НШС и аварий, порождаемых операционными нарушениями пользователей. Подразделения ИТ-службы на этом уровне осуществляют сервисную поддержку деятельности ЦИП, координацию взаимодействия всех ИТ-служб в процессе восстановления сервисов и проведения работ на ресурсах ИТС с использованием методик комплексного управления сервисами и ИТС, а также поддержку превентивной защиты ИТ-сервисного контента. Их деятельность строится на базе концепции и модели управления качеством сервисов по технологии Information Technology Service Management (ITSM).

3. *Уровень технической эксплуатации ресурсов ИТС*. Подразделения этого уровня осуществляют техническую поддержку надежности функционирования технических и программных средств ИТС, КСА, их техническое обслуживание, ремонт, сопровождение программных средств по обеспечению непрерывного формирования сервисов. Главной целью подразделений технической эксплуатации является предотвращение потерь, связанных с системными простоями и неполадками в инфраструктуре ИТС (заражение вирусами, потеря данных, неполадки в технических средствах, компьютерах, серверах, сбои во вспомогательных средствах, нарушения в работе баз данных, приложениях, процессах формирования сервисов и т.д.) [5].

На рисунке представлена схема структурно-функциональной организации ИТ-службы ИТС АО с учетом перечисленных выше уровней эксплуатации.

Принципиальным в схеме является организационное разделение РСМ СЭ по функциям поддержки деятельности АО и технической поддержки разработки и эксплуатации сервисов, услуг и ресурсов ИТС. Однако существующая функциональная модель организации ИТ-службы ИТС имеет существенные недостатки, порождаемые, прежде всего, несоответствием между функциями ИТ-службы и функциональными процессами органа управления, так как каждый процесс управления определяется несколькими функциями ИТ-службы и может поддерживаться многими сервисами и услугами, что затрудняет оценку их качества. Недостатки структурно-функциональной организации деятельности ИТ-службы могут быть преодолены при внедрении в работу РСМ СЭ системно-процессного подхода. Суть данного подхода состоит в том, что функциональная деятельность органа управления и ИТС рассматривается как совокупность сбалансированных взаимосвязанных процессов. В ходе работы ИТ-службы по этой схеме системно-процессная модель ИТС и функциональная структура организации взаимодействуют между собой и повышают эффективность управления всеми процессами предоставления и поддержания услуг на каждом уровне. Это обстоятельство создает условия для использования типовых процессов в деятельности ИТ-службы на основе рекомендаций «лучших практик» в области управления сервисами, организации

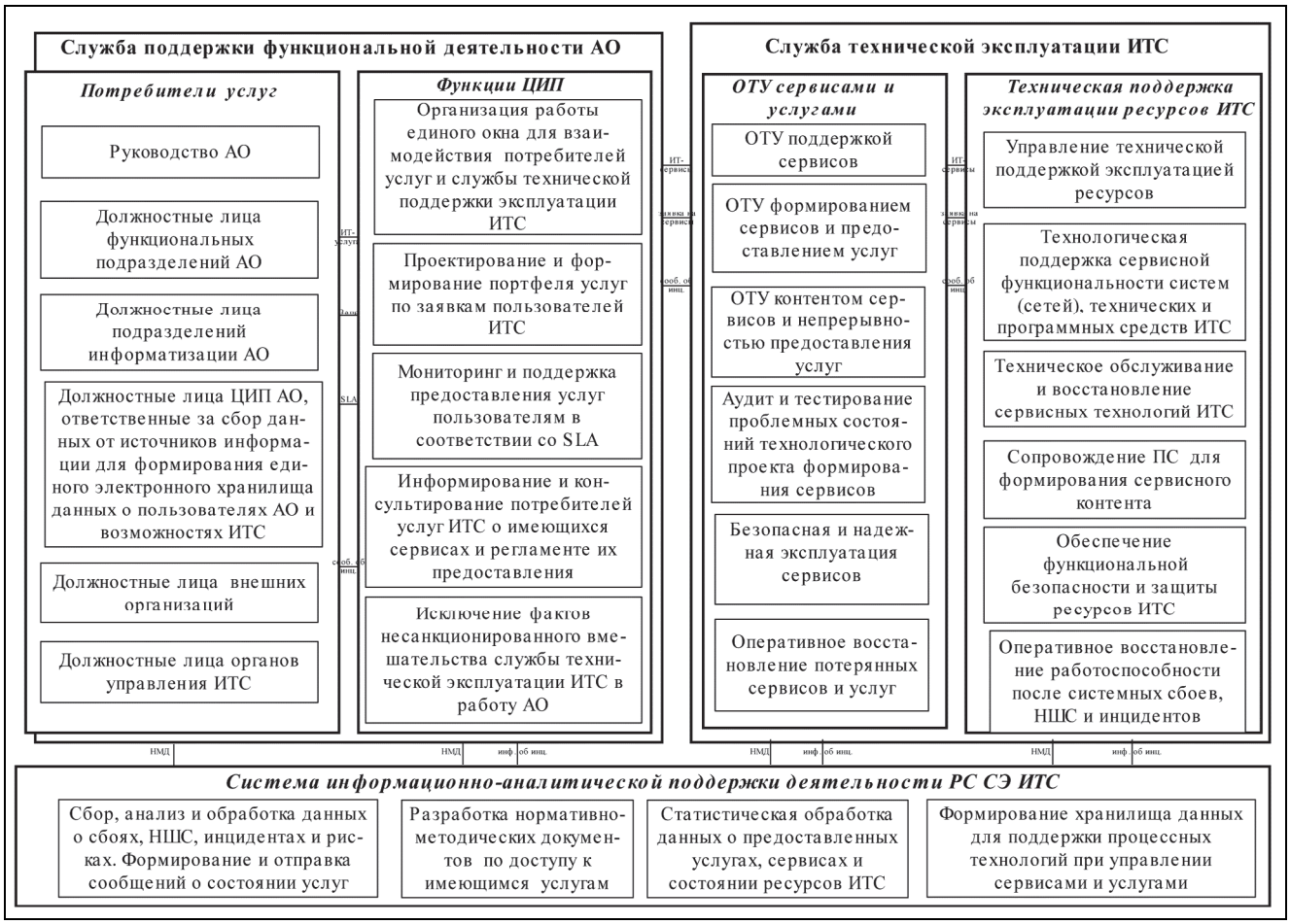


Схема структурно-функциональной организации ИТС АО

ИТ-службы и функционирования АО. В настоящее время наибольшее распространение получила методология управления на базе библиотеки ITIL. Практическая ценность предполагаемой методологии состоит в том, что специалисты органа управления при РСМ СЭ получают доступ к единому понятийному аппарату и к управлению типовыми процессами ИТ-службы.

Здесь важно заметить, что для внедрения системно-процессного подхода необходимо на каждом уровне иметь некоторые управленческие функции, для которых главными в их реализации являются процессы, обеспечивающие достижение целей управления. Библиотека ITIL включает в себя описание процессов: планирования управления услугами; управления приложениями; управления инфраструктурой информационно-коммуникационных технологий; управления безопасностью; управления конфигурациями с учетом влияния ИТ-инфраструктуры на бизнес компании. При этом процессы делятся на две группы: группу *поддержки услуг* и группу *предоставления услуг*.

К первой группе относятся процессы управления уровнем услуг, мощностью, доступностью, непрерывностью, финансами и безопасностью.

Ко второй группе относятся процессы управления инцидентами, проблемами, конфигурациями, изменениями и релизами. В работе [1] подробно рассмотрено содержание этих процессов и методика их применения.

Возможно, стоит отметить, что библиотека ITIL не дает специалистам ИТ-службы и органам управления окончательных и однозначных рекомендаций как должна строиться их деятельность. Этот вопрос решается с учетом целей и задач органа управления и доступных ресурсов ИТС, а также с учетом специфики внутренней и внешней среды и приемлемого уровня риска.

Служба ОТУ сервисами и услугами предназначена для обеспечения непрерывности предоставления сервисов и доступности услуг, а также для устранения локальных сбоев, отказов (инцидентов) и нарушений безопасности сервисов. Служба ОТУ сервисами и услугами является основным связующим тех-

ническим звеном между службой ЦИП и службой ТПЭ ресурсов ИТС. Для служб ЦИП она предоставляет информацию о сервисах, их состоянии, техническом и контентном содержании. Для службы ТПЭ ИТС она определяет требования к сервисам и восстановлению системных НШС и инцидентов. Служба ОТУ организуется в соответствии с особенностями построения ИТС, объемом и сложностью решаемых задач АО, степенью уязвимости компонентов ИТС, нормативной и оперативно-технической документацией по использованию ресурсов, наличием и уровнем зрелости оперативно-технического персонала СЭ. Служба ТПЭ ресурсов ИТС обеспечивает надежность и устойчивость функционирования технических, программных средств, сервисов, услуг, их техническое обслуживание, хранение, ремонт, безопасность и защиту ресурсов на этапе эксплуатации жизненного цикла ИТС.

Переход к РСМ от существующей ресурсной модели требует создания на базе системно-процессного подхода определенного уровня «интеллектуального» развития (зрелости) всей инфраструктуры АО. В частности, при этом подразумевается следующее:

готовность пользователей воспринимать портфель услуг как набор реализации контента управляемых сервисов;

выдвижение в SLA требований, адекватных к качеству и ресурсно-сервисным возможностям ИТС;

наличие в ИТС процессов, ресурсов и сервисов, обладающих свойством измеримости и критичности;

наличие регламентов действий в исключительных и нештатных ситуациях;

мотивация ИТ-службы к минимизации рисков, порождаемых РСМ СЭ ИТС;

готовность РСМ СЭ к совершенствованию, порождению новых сервисов вслед за изменениями потребностей АО.

В настоящее время существует ряд моделей зрелости бизнес-процессов, позволяющих оценивать степень зрелости процессной организации работ на автоматизированном предприятии и повышения эффективности ИТ-инфраструктуры. Базовым понятием модели считается зрелость по нескольким уровням. Например, в работе «Интегрированная модель зрелости процессов» (Capability Maturity Model Integration – CMMI) предлагается пять уровней зрелости [6]. Успешная эксплуатация сервисов обеспечивается соблюдением принятых уровней зрелости. На их базе определяется методология разработки информационного и технического наполнения содержания сервиса, которое определяется функциональными процессами, органами управления, ресурсами ИТС и способностью ЦИП осуществлять управление контентом услуги.

Система управления контентом строится на базе системы информационно-аналитической поддержки (СИАП) и представляет собой АПК, предназначенный для сбора, анализа и обработки данных о процессах функционирования АО, процессах управления услугами, сервисами и ресурсами ИТС. СИАП, создаваемая в инфраструктуре РСМ СЭ по ассоциации с управлением информацией рассматривает управление по операциям и задачам, приведенным на рисунке. Цель СИАП СЭ может быть сформулирована на базе рекомендаций Microsoft Operations Framework (MOF), которые базируются на принципах ITIL V.3 и стандарта ISO 15504 [7], заключающихся в предоставлении ИТ-подразделениям руководств, помогающих создавать, эксплуатировать и поддерживать услуги, обеспечивая получение ожидаемых коммерческих преимуществ от конкретных инвестиций в ИТ. СИАП призвана обеспечить информационную поддержку зрелости: модели процессов эксплуатации; модели управления точкой доступа; модели управления рисками; модели ОТУ услугами, сервисами и технической поддержкой ресурсов.

В процессе функционирования ИТ-службы осуществляется множество эксплуатационных операций, которые выполняются специалистами подразделений информатизации. Выбор возможных вариантов и организационно-технических решений осуществляется с использованием системы показателей, характеризующих свойства СЭ по обеспечению непрерывного сервисного обслуживания пользователей АО. Методический подход к определению состава показателей базируется на двух типах:

системные показатели Situation Performance Indicators (SPI), характеризующие внешнюю среду и общую ситуацию деятельности АО и функционирования ИТС, значения которых нельзя однозначно интерпретировать в отношении качества РСМ обслуживания;

ключевые показатели достижения цели обслуживания (идентификаторы результативности Key Performance Indicators (KPI)), которые характеризуют эффективность процессов и/или их качество (например, уровень доступности услуг, выполнения SLA, уровень локализации инцидентов).

Показатели KPI, как правило, выражают глубинный смысл процессов предоставления услуг, ОТУ сервисами и эксплуатации ресурсов ИТС по степени достижения требуемых эксплуатационных величин.

В свою очередь, перечисленные типы показателей в каждой системе, процессе и сервисе могут быть дополнительно структурированы. Например, при управлении инцидентами применены категории показателей достижения цели, качества процесса, качества деятельности и т.п. При решении оценки эффективности РСМ СЭ необходимо выделять две основные задачи: *поддержку непрерывности и доступности услуг ЦИП* и *задачу ОТУ с ТПЭ ресурсов ИТС*.

Первая задача направлена на оценку процессов поддержки интересов пользователей и оказывает им помощь в осуществлении непрерывного доступного интерфейса между ними и ресурсно-сервисными возможностями ИТС. Вторая задача направлена на поддержание надежной и устойчивой работоспособности ИТС. Обе эти задачи являются первоочередными при внедрении методик ITSM.

Риски, порождаемые нарушениями эксплуатации информационно-телекоммуникационных систем

Деятельность любого АО во многом зависит от эффективности РСМ СЭ и вероятности возникновения эксплуатационных рисков. Например, нарушения непрерывности ресурсно-сервисного обслуживания и доступности услуг может привести к возникновению управленческих, экономических, финансовых, репутационных и других видов рисков в деятельности АО. Под эксплуатационным риском будем понимать вероятность возникновения события, связанного с нарушениями в СЭ, приведшего к искажению ресурсно-сервисных параметров функционирования ИТС, а также к ущербу в деятельности органа управления. Риски, связанные с нарушениями в СЭ, включают в себя следующие группы:

риски, связанные с обслуживанием процессов, предоставлением информационных и телекоммуникационных сервисов и услуг;

риски, связанные с техническим обслуживанием и ремонтом (восстановлением) технических средств и сопровождением программных средств;

риски, связанные с сопровождением технологических процессов функционирования систем (сетей), подсистем, ПТК и КСА;

риски, связанные с управлением уровнем доступности услуг;

риски, связанные с ОТУ устранения сбоев, НШС и инцидентов;

ресурсные риски;

инфраструктурные риски;

риски вспомогательных систем;

риски, порождаемые действиями персонала СЭ;

прочие риски (финансовые, риски технической эстетики, эргономики, социальные, имущественные и т.п.).

В работе [8] приведен примерный перечень рисков по перечисленным группам. Процесс управления рисками в крупномасштабной ИТС является сложной и многоаспектной процедурой всех составляющих РСМ СЭ, решение которой во многом сопряжено с деятельностью специалистов ИТ-служб, их способностью оценить ситуацию, определить размер инцидента и порождаемого им риска, а также способностью системы ТПЭ ИТС минимизировать ущерб от его возникновения. В АО это специфическая деятельность, требующая глубоких знаний в области эффективной деятельности организации и эксплуатации ИТС, анализа методов и средств противодействия угрозам живучести ИТС, а также наличия в СЭ средств восстановления критически важных сервисов и услуг. Главной задачей ИТ-службы по управлению рисками, порождаемыми ИТС, является способность оценить размер всех видов нарушений, выработать эффективные согласованные с функциональными процессами организации предложения по уменьшению их воздействия и принять меры, чтобы их размер был приемлемым. Теория и практика управления рисками выработала ряд основополагающих принципов, которыми следует руководствоваться субъектам ЦИП и ОТУ сервисами ИТС [9].

- Предложенный подход создает методологическую основу повышения эффективности использования возможностей ИТС за счет создания единой процессной информационной и технологической ресурсно-сервисной архитектуры СЭ, обеспечивающей непрерывную деятельность автоматизированных ОВГУ на всем этапе эксплуатации их жизненного цикла.

Применение данного подхода позволит успешно перейти от существующей ресурсной модели СЭ ИТС к РСМ СЭ ИТС, обеспечив при этом системный технологический процесс, способный динамически поддерживать деятельность АО и повышать непрерывность функционирования ИТС и доступность услуг за счет применения методик «лучших мировых практик» в подразделениях информатизации ИТ-служб.

Литература

1. IT Infrastructure Library. Библиотека ITIL v.3. Поддержка услуг. Русский перевод. Компания «Ай-Теко». 2007.
2. ГОСТ Р ИСО/МЭК 20000.1-2010. Информационная технология. Управление услугами. Ч. 1. Требования к системе управления услугами. Спецификация.
3. ГОСТ Р ИСО 10303-239-2008. Национальный стандарт РФ. Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными. Ч. 239. Поддержка жизненного цикла изделий.
4. *Быстров И.И. и др.* Теоретические основы проектирования и эксплуатации сложных мультисервисных информационно-телекоммуникационных систем. М.: ИПИ РАН. 2014. 150 с.
5. *Оганян Г.А.*, *Мусатов А.А.*, *Баландин С.Ю.*, *Сычев В.Н.* Подсистема технической поддержки эксплуатации перспективной автоматизированной системы органов государственного управления // Научно-производственный и культурно-образовательный журнал «Качество и жизнь». 2016. Спец. выпуск. С. 19–22.
6. Интегрированная модель зрелости процессов. Институт Карнеги-Меллон (SEI). 2010. Версия 1.3.
7. ГОСТ Р ИСО/МЭК 15504-1-2009. Информационные технологии. Оценка процессов. Ч. 1. Концепция и словарь. М.: Стандартинформ. 2009.
8. *Быстров И.И.* Живучесть автоматизированных организаций. М.: Майор: Осипенко. 2016. 506 с.
9. *Вишняков Я.Д.*, *Радаев Н.Н.* Общая теория рисков. Изд. 2-е, испр. М.: Издательский центр «Академия». 2008. 368 с.

Поступила 7 декабря 2017 г.

Resource-service model of the information and telecommunication systems maintenance

I.I. Bystrov – Dr. Sc. (Eng.), Professor, Head of Department, Institute of Informatics Problems of FRC CSC RAS (Moscow)
E-mail: ibystrov@ipiran.ru
S.I. Radomanov – Research Scientist, Institute of Informatics Problems of FRC CSC RAS (Moscow)
E-mail: radomanov@list.ru
V.N. Sychev – Ph. D. (Mil.), Professor, Main Specialist, Scientific and Technical Support Centre,
SC «RIAA after V.S. Semenikhin» (Moscow)
E-mail: svn.niiaa@yandex.ru

This article discusses the conceptual basis for the use of the resource and service model (RSM) to create a system for modern multi-service telecommunication systems (ITS) maintenance, and the main problems of IT-services for the implementation of this model based on «global best practices». The proposed approach creates the methodological basis of improvement of the commercial, financial, military and public administration organs automated activities through the creation in their infrastructure some effective resource and service system of operation (RS MS), which provides support for matching of IT-services with the changing needs of management in various conditions. The application of this approach will make it possible to successfully transfer from the existing resource model of ITS to the RSM maintenance system of ITS.

References

1. IT Infrastructure Library. Biblioteka ITIL v.3. Podderzhka uslug. Russkiy perevod. Kompaniya «Ay-Teko». 2007.
2. GOST R ISO/MEK 20000.1-2010. Informatsionnaya tekhnologiya. Upravlenie uslugami. Ch. 1. Trebovaniya k sisteme upravleniya uslugami. Spetsifikatsiya.
3. GOST R ISO 10303-239-2008. Natsional'nyy standart RF. Sistemy avtomatizatsii proizvodstva i ikh integratsiya. Predstavlenie dannykh ob izdelii i obmen etimi dannymi. Ch. 239. Podderzhka zhiznennogo tsikla izdeliy.
4. *Bystrov I.I. i dr.* Teoreticheskie osnovy proektirovaniya i ekspluatatsii slozhnykh mul'tiservisnykh informatsionno-telekommunikatsionnykh sistem. M.: IPI RAN. 2014. 150 s.
5. *Oganyan G.A., Musatov A.A., Balandin S.Yu., Sychev V.N.* Podsistema tekhnicheskoy podderzhki ekspluatatsii perspektivnoy avtomatizirovannoy sistemy organov gosudarstvennogo upravleniya // Nauchno-proizvodstvennyy i kul'turno-obrazovatel'nyy zhurnal «Kachestvo i zhizn'». 2016. Spets. Vypusk. S. 19–22.
6. Integrirovannaya model' zrelosti protsessov. Institut Karnegi-Mellon (SEI). 2010. Versiya 1.3.
7. GOST R ISO/MEK 15504-1-2009. Informatsionnye tekhnologii. Otsenka protsessov. Ch. 1. Kontseptsiya i slovar'. M.: Standartinform. 2009.
8. *Bystrov I.I.* Zhivuchest' avtomatizirovannykh organizatsiy. M.: Mayor: Osipenko. 2016. 506 s.
9. *Vishnyakov Ya.D., Radaev N.N.* Obshchaya teoriya riskov. Izd. 2-e, ispr. M.: Izdatel'skiy tsentr «Akademiya». 2008. 368 s.

УДК 81.322

Автоматическое выявление угроз обществу и государству в социальных сетях и средствах массовой информации

В.Н. Захаров – д.т.н., ученый секретарь, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: vzakharov@ipiran.ru
Д.А. Садовников – сотрудник, ООО «МетаФраз»
E-mail: fos2000@yandex.ru
М.В. Смирнов – сотрудник, ООО «МетаФраз»
E-mail: smirnoff63@gmail.com
А.А. Хорошилов – к.т.н., науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: a.a.horoshilov@mail.ru

Описан метод выявления и нейтрализации угроз обществу и государству в социальных сетях и средствах массовой информации, основанный на двухэтапной обработке поступающих в систему текстов. Показано, что данный метод позволяет значительно сократить трудозатраты по выявлению деятельности киберпреступников, деятельность которых направлена на дестабилизацию обстановки в стране.

Ключевые слова: *выявление заимствований, автоматизированная обработка текстов, формализованное описание текста, смысловая структура, лингвистическое программное обеспечение, декларативные средства.*

The article describes a method for identifying and neutralizing threats to society and the state in social networks and the media. This method is based on two-stage processing of texts entering the system. This method makes it possible to significantly reduce efforts to identify the activities of cybercriminals, whose activities are aimed at destabilizing the situation in the country.

Keywords: *detection of cyberthreats, automatic detection of extremist texts, automated information systems, automated word processing, formalized text description, semantic structure, linguistic software, declarative tools.*

В настоящее время интернет стал одним из наиболее часто используемых источников информации для населения большинства стран мира и все сильнее набирает ход процесс информатизации всех сфер жизни общества. Сетевые средства массовой информации вытесняют печатные издания, общение между людьми переходит в социальные сети – все это значительно изменило образ жизни большинства жителей развитых стран. К сожалению, в ногу со временем идут и различные враждебные по отношению к современному обществу силы. Часто интернет используется террористическими и экстремистскими организациями для достижения своих целей. Поэтому одной из важнейших составляющих политики обеспечения национальной безопасности для развитых стран становится возможность отслеживания угроз, идущих из киберпространства.

Цель работы – рассмотреть метод выявления и нейтрализации угроз обществу и государству в социальных сетях и средствах массовой информации, основанный на двухэтапной обработке поступающих в систему текстов.

Состояние проблемы

В нашей стране в последнее время проводится множество исследований по изучению деятельности киберпреступников по дестабилизации обстановки в стране. Например, в 2012 г. Н.К. Воронович представил диссертационную работу по теме «Интернет как угроза информационной безопасности России» [1], в которой был рассмотрен ряд угроз, возникающих в результате широкого использования интернета. А в статье «Социальные сетевые сервисы в контексте международной и национальной безопасности» О.В. Демидова [2] описывается использование социальных сетей для организации революций и беспорядков. Также в России регулярно проходят форумы, посвященные проблеме терроризма и экстремизма в интернете. В качестве примера можно привести форум «Выбор молодежи – интернет без терроризма», где обсуждаются вопросы противодействия противоправным действиям в сети интернет. В целом, работ по такой тематике представлено довольно много, но основная проблема их заключается в том, что в публикациях не описывается методика борьбы с угрозами национальной и международной безопасности.

В настоящее время в России существует «Единый реестр запрещенной информации». Ежедневно в него попадают десятки, а иногда и сотни сайтов, содержимое которых признано «опасным», но работает эта технология в ручном режиме, эксперты определяют такую информацию по своему усмотрению. К сожалению, такая технология не позволяет охватить полностью информационное пространство, в котором содержится деструктивная информация. На данный момент единственная технология, с помощью которой фильтруется контент в интернете – это поиск по ключевым словам, что в значительной степени влияет на точность выявления угроз, идущих из киберпространства, поскольку такой метод требует значительных затрат времени экспертов.

На данный момент практически отсутствуют комплексные методы и модели, реализованные в виде программно-информационного обеспечения, которые позволяют проводить научные исследования и практические работы в области выявления угроз и противодействия им в социальных сетях и средствах массовой информации.

Общие сведения о документах экстремистской направленности

В соответствии с Федеральным законом от 25.07.2002 № 114-ФЗ (ред. от 29.04.2008) «О противодействии экстремистской деятельности» к экстремистской деятельности относятся:

насильственное изменение основ конституционного строя и нарушение целостности РФ;

публичное оправдание терроризма и иная террористическая деятельность;

возбуждение социальной, расовой, национальной или религиозной розни;

пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;

воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;

совершение преступлений по мотивам, указанным в пункте «е» части первой статьи 63 Уголовного кодекса РФ;

пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций;

публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;

публичное заведомо ложное обвинение лица, замещающего государственную должность РФ или государственную должность субъекта РФ, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением;

организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;

финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг [3].

Представленные выше выдержки дают достаточно полную картину о том, какие документы можно считать представляющими угрозу обществу и государству. В исследованиях, описанных в данной статье, авторы для выявления таких текстов используют вышеизложенные определения.

Технологии автоматической обработки текста для автоматизации процесса выявления угроз обществу и государству

Для решения задач семантической обработки разноязычных текстов в рамках процесса автоматизации выявления угроз обществу и государству предлагается использовать Лингвистическое программное обеспечение (ПО) МетаФраз. Это ПО уже было использовано в процессе разработки системы «Монито-

ринг СМИ» (СКЦ Росатома) и смысловой поисково-аналитической системы авиационной промышленности «СПАС-Авиа» (ГосНИИАС).

ПО МетаФраз обеспечивает весь технологический цикл преобразования текстового представления документа в его формализованное смысловое представление. Оно разработано в виде единого интегрированного многофункционального программного комплекса, состоящего из нескольких подсистем, предназначенных для решения отдельных функциональных задач по обработке, формализации и анализу смыслового содержания разноязычных документов. При этом в состав ПО включены также программные модули, позволяющие создавать и адаптировать декларативные средства для настройки на заданную предметную область путем быстрого автоматизированного создания словарей по корпусу текстов.

Основными инструментами, которые используются в предлагаемом подходе, являются процедуры семантико-синтаксического и концептуального анализа текстов. Центральной процедурой ПО МетаФраз является процедура семантико-синтаксического анализа текстов. В эту процедуру входит совокупность следующих базовых процедур: графематический анализ текстов; морфологический анализ слов; нормализация (лемматизация) слов; формализация и унификация наименований понятий [5]; отождествление наименований понятий [6]; семантико-синтаксический анализ предложений [7].

Весь комплекс процедур семантико-синтаксического анализа текстов базируется на использовании грамматических таблиц для морфологического и семантико-синтаксического анализа и комплекса словарей для процедур концептуального анализа и построения формализованного смыслового представления текста.

Подготовка декларативных средств для решения задачи выявления угроз обществу и государству

На начальном этапе было отобрано более 1000 текстов и новостных сообщений, связанных с деятельностью террористической организации «ИГИЛ», запрещенной на территории РФ, а также был составлен массив текстовых сообщений, состоящий из комментариев одного из запрещенных на территории РФ сайтов, а также одной из групп ВКонтакте, близкой к экстремистской организации «Правый сектор». Эти текстовые массивы были обработаны процедурой семантико-синтаксического и концептуального анализа, в результате чего были выделены отдельные слова и словосочетания различной длины и составлены частотные словари. Далее на основе лингвистического анализа частотной части этих словарей были сформированы тематические словари, относящиеся к тематикам «ИГИЛ» и «Правый сектор». Фрагмент такого словаря приведен в таблице.

Таблица. ***Фрагмент частотного словаря по тематике «Правый сектор»***

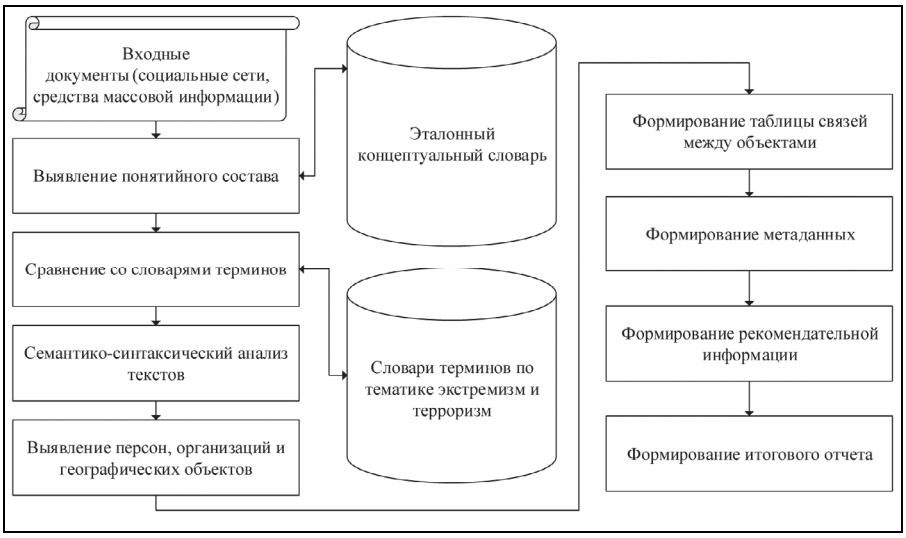
Наименование понятия	Частота
…	…
Аннексия	43
Кацап	39
Заблудившийся десантник	35
Недочеловек	33
Гебня	31
Цензор	31
…	…

Полученные словари значительно отличаются по возможностям применения. Словарь по тематике «ИГИЛ» содержит в основном термины, имеющие отношение к деятельности данной террористической организации, и может использоваться для поиска текстов, в которых описываются происшествия, связанные с их деятельностью. Второй словарь составлен с учетом лексики, используемой участниками организации «Правый сектор» и людьми, близкими к ней. Поэтому словарь может быть использован для выявления, например, обсуждений в социальных сетях, которые направлены на возбуждение национальной розни.

Метод выявления угроз обществу и государству в социальных сетях и средствах массовой информации

Далее опишем разработанный авторами метод, позволяющий производить двухэтапный анализ смыслового содержания текстов, получаемых в социальных сетях и средствах массовой информации.

На первом этапе производится отбор подозрительных текстов, требующих дополнительного исследования. Рассмотрим алгоритм первого этапа.



Общая схема работы алгоритма выявления угроз обществу и государству в социальных сетях и средствах массовой информации

Ш а г 1 . Производится графематический анализ поступившего текста.

Ш а г 2 . Производится морфологический анализ поступившего текста.

Ш а г 3 . Производится концептуальный анализ поступившего текста.

Ш а г 4 . Понятийный состав текста сравнивается с тематическими словарями (по тематикам «ИГИЛ» и «Правый сектор»).

Ш а г 5 . Если присутствуют значительные совпадения со словарями, то документ направляется для дополнительного анализа.

Н а в т о р о м э т а п е производится углубленный анализ смысловой структуры текста и выявляются необходимые данные для последующих исследований. Рассмотрим алгоритм второго этапа.

Ш а г 1 . Производится семантико-синтаксический анализ текста.

Ш а г 2 . Выявляются персоны, организации и географические объекты, описанные в тексте.

Ш а г 3 . Формируется таблица связей между персонами, организациями и объектами, выявленными в тексте.

Ш а г 4 . Устанавливается тип угрозы (формальное описание угрозы и т.д.).

Ш а г 5 . Формируются метаданные, идентифицирующие текстовые сообщения (списки персон, организаций и стран, представляющих террористическую угрозу, а также персон и стран, в отношении которых направлены эти угрозы).

Ш а г 6 . На основе метаданных формируется рекомендательная информация, касающаяся анализируемого текста (рекомендовать для изъятия из публичного доступа; рекомендовать для предоставления в правоохранительные органы; оставить без изменений).

Ш а г 7 . Если на вход подавалась группа документов, то формируется итоговый отчет, основанный на данных, полученных на шаге 5.

Этот отчет наряду со статистикой выявленных угроз также должен включать в себя информацию о степени опасности угроз (базирующуюся на семантических и статистических критериях).

На рисунке представлена общая схема работы алгоритма выявления угроз обществу и государству в социальных сетях и средствах массовой информации.

- Разработанный авторами алгоритм может быть применен для поиска угроз в социальных сетях, например, для выявления пользователей, распространяющих информацию экстремистского содержания, и их дальнейшей блокировки, а также выявления информации о деятельности экстремистских организаций и ее систематизации. Нужно отметить, что текстовые сообщения социальных сетей плохо поддаются автоматическому анализу вследствие того, что пользователи не всегда руководствуются устоявшимися правилами языка, на котором формируются сообщения. Кроме того, иногда опасаясь, что их сообщения будут удалены, пользователи, стремящиеся донести информацию экстремистской направленности, пишут свои сообщения путем их транслитерирования или сознательно включают в текст грамматические ошибки.

  Для выявления таких ситуаций требуется более детальный анализ упрощенного языка, используемого в социальных сетях, и создание словарей сленга. В настоящее время таких словарей, содержащих достаточно полную информацию, не существует. Для их формирования требуется обработка больших объемов комментариев из социальных сетей и новостных порталов. Это позволит

сформировать за короткое время достаточно качественные словари, позволяющие выполнять описанную задачу более эффективно.

Статья подготовлена при поддержке гранта РФФИ (проект №17-03-12042).

Литература

1. *Воронович Н.К.* Интернет как угроза информационной безопасности России: автореферат дис. … канд. соц. наук: 22.00.04. Краснодар: 2012. 27 с.
2. *Демидов О.В.* Социальные сетевые сервисы в контексте международной и национальной безопасности // Индекс безопасности. 2013. Т. 19. № 1(104). С. 65–86.
3. Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 29.04.2008) «О противодействии экстремистской деятельности» // Российская газета. 2002. № 138–139.
4. Свид-во о гос. регистрации программы для ЭВМ № 2014663081 от 15.12.2014. Система семантической обработки текстов МетаФраз R10 (MF Text Analyst R10) / *Никитин Ю.В.*, *Смирнов М.В.*, *Садовников Д.А.*, *Хорошилов А.А. и др.*
5. *Захаров В.Н.*, *Хорошилов Ал-др А.*, *Хорошилов Ал-ей А.* Метод автоматического выявления неявно выраженных заимствований в научно-технических текстах // Искусственный интеллект и принятие решений. 2017. № 1. С. 10–20.
6. *Хорошилов А.А.* Методы автоматического установления смысловой близости документов на основе их концептуального анализа // Труды XV Всерос. научной конф. «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» – RCDL'2013. Ярославль. 14–17 октября 2013 г. С. 369–376.
7. *Захаров В.Н.*, *Хорошилов А.А.* Автоматическое формирование визуального представления смыслового содержания документа // Системы и средства информатики. 2013. Т. 23. № 1. С. 143–158.

Поступила 7 декабря 2017 г.

Automatic detection of threats to society and the state in social networks and the media

V.N. Zakharov – Dr. Sc. (Eng.), Scientific Secretary, FRC «Computer Science and Control» RAS (Moscow)
E-mail: vzakharov@ipiran.ru
D.A. Sadovnikov – Employee, LLC MetaFraz
E-mail: fos2000@yandex.ru
M.V. Smirnov – Employee, LLC MetaFraz
E-mail: smirnoff63@gmail.com
A.A. Khoroshilov – Ph. D. (Eng.), Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: a.a.horoshilov@mail.ru

The article describes a method for identifying and neutralizing threats to society and the state in social networks and the media. This method is based on two-stage processing of texts entering the system. At the first stage, a subset of documents that require additional analysis is automatically selected using the vocabulary analysis. At the second stage, a complete semantic analysis of the texts of the selected documents takes place, and the necessary data on the texts and their fragments containing materials that threaten society and the state are identified. This method makes it possible to significantly reduce efforts to identify the activities of cybercriminals, whose activities are aimed at destabilizing the situation in the country.

References

1. *Voronovich N.K.* Internet kak ugroza informatsionnoy bezopasnosti Rossii: avtoreferat dis. … kand. sots. nauk: 22.00.04. Krasnodar: 2012. 27 s.
2. *Demidov O.V.* Sotsial'nye setevye servisy v kontekste mezhdunarodnoy i natsional'noy bezopasnosti // Indeks bezopasnosti. 2013. T. 19. № 1(104). S. 65–86.
3. Federal'nyy zakon ot 25.07.2002 № 114-FZ (red. ot 29.04.2008) «O protivodeystvii ekstremistskoy deyatel'nosti» // Rossiyskaya gazeta. 2002. № 138–139.
4. Svid-vo o gos. registratsii programmy dlya EVM № 2014663081 ot 15.12.2014. Sistema semanticheskoy obrabotki tekstov MetaFraz R10 (MF Text Analyst R10) / *Nikitin Yu.V., Smirnov M.V., Sadovnikov D.A., Khoroshilov A.A. i dr.*
5. *Zakharov V.N., Khoroshilov Al-dr A., Khoroshilov Al-ey A.* Metod avtomaticheskogo vyyavleniya neyavno vyrazhennykh zaimstvovaniy v nauchno-tekhnicheskikh tekstakh // Iskusstvennyy intellekt i prinyatie resheniy. 2017. № 1. S. 10–20.
6. *Khoroshilov A.A.* Metody avtomaticheskogo ustanovleniya smyslovoy blizosti dokumentov na osnove ikh kontseptual'nogo analiza // Trudy XV Vseros. nauchnoy konf. «Elektronnye biblioteki: perspektivnye metody i tekhnologii, elektronnye kollektsii» – RCDL'2013. Yaroslavl'. 14–17 oktyabrya 2013 g. S. 369–376.
7. *Zakharov V.N., Khoroshilov A.A.* Avtomaticheskoe formirovanie vizual'nogo predstavleniya smyslovogo soderzhaniya dokumenta // Sistemy i sredstva informatiki. 2013. T. 23. № 1. S. 143–158.

УДК 004

Оценка эффективности использования методов интеллектуального анализа данных при обеспечении информационной безопасности облачных вычислительных сред

С.В. Борохов – ст. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: sborokhov@ipiran.ru
П.А. Кейер – ст. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: pkeyer@ipiran.ru

Приведены описания методик определения эффективности использования методов интеллектуального анализа данных (ИАД) при обеспечении информационной безопасности (ИБ) в облачных вычислительных средах (ОВС).

Ключевые слова: *интеллектуальный анализ данных, информационная безопасность, облачные вычислительные среды, оценка эффективности.*

The descriptions of methods for determining the effectiveness of data mining techniques for information security in cloud computing environments are presented.

Keywords: *data mining, information security, cloud computing environments, evaluation of effectiveness.*

Проблемы обеспечения информационной безопасности (ИБ) облачных вычислительных сред (ОВС) в области практической реализации средств защиты информации обусловлены значительными объемами событий, которые необходимо анализировать и на которые требуется реагировать в реальном масштабе времени. В настоящее время в качестве комплексных решений обеспечения ИБ получили распространение универсальные шлюзы безопасности, ядро которых составляют системы обнаружения вторжений (СОВ). В работах [1, 2] показано, что имеется потенциал увеличения производительности СОВ посредством использования различных математических техник интеллектуального анализа данных (ИАД). При этом актуальным является вопрос комплексной оценки эффективности использования в СОВ различных методов ИАД.

Цель работы – рассмотреть методики оценки приведенных в [3] показателей эффективности использования методов ИАД в СОВ при обеспечении ИБ ОВС.

В [3] определены следующие группы показателей эффективности использования методов ИАД в СОВ: 1) функционирование СОВ в части выполнения основной функции; 2) функционирование СОВ в составе телекоммуникационной инфраструктуры ОВС; 3) экономические показатели СОВ.

Показатели эффективности первой группы включают в себя: метрику точности – долю событий, классифицированных СОВ в качестве атак, действительно являющихся атаками; метрику полноты – долю атак, выявленных СОВ, от всех имевших место атак; интегральную метрику гармонического среднего точности и полноты.

Показатели эффективности второй группы включают в себя производительность (пропускную способность) СОВ и определяются влиянием на показатели качества обслуживания, предоставляемого телекоммуникационной инфраструктурой ОВС.

Показатели эффективности третьей группы включают в себя: совокупную стоимость владения СОВ; величину предотвращенного СОВ ущерба.

В дополнение к перечисленным выше показателям в настоящей статье предлагается использовать интегральную оценку эффективности использования методов ИАД в СОВ при обеспечении ИБ ОВС.

Оценка эффективности используемого в СОВ метода ИАД

Оценка эффективности используемого в СОВ метода ИАД может быть осуществлена на основе следу-

ющих показателей: точность (precision, *P*), полнота (recall, *R*) и гармоническое среднее точности и полноты (*F*-мера, *F*). Данные показатели рассчитываются на основе следующих первичных показателей функционирования СОВ:

числа событий, являющихся атаками и классифицированными СОВ как атаки (true positive, *TP*);

числа событий, не являющихся атаками, но которые СОВ классифицировала как атаки (false positive, *FP*);

числа событий, не являющихся атаками и которые СОВ не классифицировала как атаки (true negative, *TN*);

числа событий, являющихся атаками, но которые СОВ не классифицировала как атаки (false negative, *FN*).

Метрика точности (precision, *P*) рассчитывается по формуле

$$P = \frac{TP}{TP + FP}. \quad (1)$$

Метрика полноты (recall, *R*) рассчитывается как

$$R = \frac{TP}{TP + FN}. \quad (2)$$

Гармоническое среднее точности и полноты (*F*-мера, *F*) находится следующим образом:

$$F = 2\frac{PR}{P + R}. \quad (3)$$

Для получения адекватных результатов при проведении сравнительной оценки эффективности использования различных методов ИАД в СОВ необходимо, чтобы сравнение осуществлялось в идентичных условиях. Это может быть достигнуто при использовании метода имитационного моделирования, при котором легко обеспечить идентичность среды и подаваемых на вход модели данных.

Процесс функционирования СОВ включает два основных этапа: обучение и функционирование непосредственно в режиме обнаружения вторжений. На первом этапе на основе обучающей выборки СОВ создает базу знаний, которая на втором этапе используется для классификации событий. Соответственно, должны быть сформированы две выборки: обучающая и оценочная. Для формирования обучающей и оценочной выборки может быть использована база сигнатур NSL KDD-2009 [4, 5].

В работе [5] методом имитационного моделирования была проведена сравнительная оценка использования в СОВ следующих методов ИАД:

опорных векторов – был реализован с помощью SVM C-SVC библиотеки LibSVM со следующими параметрами: функция ядра – радиальная базисная функция (RBF), максимальная ошибка обучения ограничена значением 10^{-5};

k-ближайших соседей – экспериментально были подобраны следующие параметры: значение *k* равное пяти, метрика – Манхэттенское расстояние;

искусственной нейронной сети – многослойного персептрона с двумя скрытыми слоями со следующими параметрами: обучение продолжительностью 1500 циклов с использованием алгоритмов обратного распространения ошибки, функция активации – сигмоидальная функция, максимальная ошибка обучения ограничена значением 10^{-7};

дерева принятия решений со следующими параметрами: минимальный порог для образования нового узла равен четырем, минимальное число листьев узла – один, максимальное число уровней – 10.

Полученные в [5] результаты приведены в таблице.

Таблица. ***Результаты сравнительной оценки использования в СОВ различных методов ИАД***

№	Метод ИАД	Точность (*P*)	Полнота (*R*)	Гармоническое среднее точности и полноты (*F*)
1	Метод опорных векторов	83,27%	83,61%	83,44%
2	Метод *k*-ближайших соседей	84,89%	84,65%	84,77%
3	Искусственная нейронная сеть	70,19%	70,38%	70,28%
4	Дерево принятия решений	79,58%	79,58%	79,58%

Отметим, что различные методы ИАД показывают различные скорости обработки событий, а также различные точность и полноту в зависимости от типа классифицируемого события (сетевой активности). При сравнительной оценке эффективности различных методов ИАД влияние этих факторов учитывается в следующих показателях: скорость обработки событий – в совокупной стоимости владения (ССВ); точность и полнота – в оценке величины предотвращенного СОВ ущерба.

Оценка влияния функционирования СОВ на телекоммуникационную инфраструктуру ОВС

При внедрении в телекоммуникационную инфраструктуру ОВС СОВ должны обеспечивать выполнение своей основной функции без ухудшения ее (телекоммуникационной инфраструктуры) показателей предоставляемого качества обслуживания. В настоящее время телекоммуникационная инфраструктура ОВС строится на базе IP-сетей, к основным показателям качества обслуживания которых относятся [6]: пропускная способность; потери; задержки передачи; готовность (доступность).

В зависимости от установленного приоритета ИБ возможны две схемы подключения СОВ:

параллельная – используется при приоритете ИБ «доступность», так как в этом случае СОВ не оказывают влияния на пропускную способность и доступность сети;

последовательная или «в разрыв» – используется при приоритетах ИБ «целостность» и «конфиденциальность».

В первом случае влияние на показатели качества обслуживания практически отсутствует, поэтому оценку влияния СОВ на телекоммуникационную инфраструктуру целесообразно проводить только при последовательной схеме подключения СОВ.

Оценка показателей качества обслуживания сети должна производиться с учетом архитектуры и используемых в сети протоколов и технологий в соответствии с разработанными программой и методиками проведения испытаний. Оценка показателей пропускной способности, потерь, задержки передачи, а также ее вариации (джиттер) может быть осуществлена как посредством свободно распространяемых утилит, так и с помощью специализированных коммерческих продуктов.

Среди свободно распространяемых утилит широкое признание получили утилиты ping и iperf [7]. Утилита ping может быть использована для измерения значения задержки передачи. Показатели качества обслуживания сети, включающие пропускную способность, потери и джиттер, могут быть измерены посредством утилиты iperf. Для этого необходимо запустить выполнение утилиты iperf на двух узлах, располагаемых на границах сети, показатели качества обслуживания которой планируется измерить. На одном узле утилита iperf должна быть запущена в серверном режиме, для этого используется ключ «-s». На втором узле утилита iperf должна быть запущена в клиентском режиме (ключ «-c») с указанием IP-адреса сервера и ключа протокола UDP (ключ «-u»). На рис. 1 показан пример вывода результатов работы утилиты iperf на стороне сервера, в котором приведены результаты измерения пропускной способности, потерь, а также джиттера.

Возможностей и точности определения утилитами ping и iperf значений показателей качества обслуживания, как правило, достаточно для небольших корпоративных сетей, характеризующихся относительно простой топологией. Для крупных, территориально распределенных сетей со сложной топологией необходимо использование специализированных коммерческих решений. На рынке присутствует достаточное число решений в этой области от различных компаний. Все они имеют развитые средства мониторинга и диагностики и позволяют оценить необходимые показатели качества обслуживания. Выбор конкретного решения должен осуществляться на основании технико-экономического обоснования, разрабатываемого для

```
------------------------------------------------------------
Server listening on 5201
------------------------------------------------------------
Accepted connection from 192.168.199.9, port 1321
[  5] local 192.168.199.2 port 5201 connected to 192.168.199.9 port 1322
[ ID] Interval           Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[  5]   0.00-1.00   sec  2.53 MBytes  21.2 Mbits/sec  4.226 ms  0/324 (0%)
[  5]   1.00-2.00   sec  3.05 MBytes  25.6 Mbits/sec  3.886 ms  0/391 (0%)
[  5]   2.00-3.00   sec  3.07 MBytes  25.7 Mbits/sec  4.702 ms  0/393 (0%)
[  5]   3.00-4.00   sec  3.06 MBytes  25.7 Mbits/sec  3.781 ms  0/392 (0%)
[  5]   4.00-5.00   sec  3.09 MBytes  25.9 Mbits/sec  4.066 ms  0/395 (0%)
[  5]   5.00-6.00   sec  3.05 MBytes  25.6 Mbits/sec  3.962 ms  0/390 (0%)
[  5]   6.00-7.00   sec  3.05 MBytes  25.6 Mbits/sec  4.065 ms  0/391 (0%)
[  5]   7.00-8.00   sec  3.05 MBytes  25.7 Mbits/sec  4.144 ms  0/391 (0%)
[  5]   8.00-9.00   sec  3.09 MBytes  25.9 Mbits/sec  4.007 ms  0/395 (0%)
[  5]   9.00-10.00  sec  3.10 MBytes  26.0 Mbits/sec  3.873 ms  0/397 (0%)
[  5]  10.00-10.18  sec   568 KBytes  25.4 Mbits/sec  4.071 ms  0/71 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[  5]   0.00-10.18  sec  0.00 Bytes  0.00 bits/sec  4.071 ms  0/3930 (0%)
------------------------------------------------------------
Server listening on 5201
------------------------------------------------------------
```

Рис. 1. Пример вывода результатов работы утилиты iperf на стороне сервера

конкретной телекоммуникационной инфраструктуры. Согласно данным Gartner Group, по состоянию на начало 2017 г. лидерами в области решений по мониторингу и диагностике сетей являются компании NetScout Systems (Fluke Networks), Riverbed и Viavi Solution (рис. 2).

Оценка экономической эффективности реализации СОВ

Экономическая эффективность реализации СОВ может быть оценена посредством следующих двух показателей: ССВ СОВ и величины предотвращенного СОВ ущерба.

В общем случае ССВ СОВ включает в себя *единовременные* и *ежегодные* затраты.

К *единовременным* относятся следующие статьи затрат:

приобретение технических средств и программного обеспечения (ПО), включая как лицензии, так и разработку заказного ПО;

работы/услуги по проектированию, включая проведение обследования, разработку концепции, проектной и эксплуатационной документации;

работы/услуги по внедрению, включая проведение строительно-монтажных и пусконаладочных работ, интеграцию в существующую подсистему обеспечения ИБ;

обучение эксплуатационного персонала.

К *ежегодным* относятся следующие статьи затрат:

техническая поддержка оборудования и сопровождение ПО;

масштабирование технических средств, развитие и совершенствование ПО;

оплата труда эксплуатационного персонала.

Для получения адекватных результатов при проведении сравнительной оценки эффективности используемых в СОВ методов ИАД сравниваемые СОВ должны обладать одинаковой производительностью. Данное условие обеспечивает учет в оценке эффективности различной скорости обработки событий различными методами ИАД, так как методы ИАД, обеспечивающие быструю обработку событий, требуют меньшей производительности технических средств, что будет учтено в их меньшей стоимости.

Величина предотвращенного СОВ ущерба может быть определена путем оценки ущерба от реализации атак, которые обнаруживает и позволяет нейтрализовать СОВ. Такой подход обеспечит учет в сравнительной оценке эффективности показателей точности и полноты различных методов ИАД в зависимости от типа классифицируемого события. В [8] предложен подход к оценке ущерба, основанный на расчете показателя ALE (Annualized Loss Expectancy). ALE – это ожидаемые годовые потери от реализации одной угрозы для одного актива. Показатель ALE рассчитывается по формуле

$$\mathrm{ALE} = \mathrm{SLE} \times \mathrm{ARO}, \qquad (4)$$

где SLE (Single Loss Expectancy) – ожидаемый ущерб от разовой реализации одной угрозы для одного актива; ARO (Annual Rate of Occurrence) – ожидаемая годовая частота реализации одной угрозы для одного актива.

Рис. 2. Схема лидеров в области решений по мониторингу и диагностике сетей

Для расчета величины предотвращенного СОВ ущерба предварительно должна быть проведена инвентаризация активов и разработана модель угроз, с использованием которых осуществлена оценка SLE. Как правило, при оценке рисков используется качественный подход, при котором SLE и ARO являются безразмерными величинами, а результаты расчетов используются для ранжирования рисков и определения их относительной величины. Для расчета величины предотвращенного СОВ ущерба такой подход не подходит, в этом случае величина SLE должна быть выражена в единицах стоимости, показывающих ущерб, причиняемый в результате реализации угрозы в отношении конкретного актива. В общем случае SLE может быть рассчитан по формуле

$$\mathrm{SLE} = \mathrm{AV} \times \mathrm{EF}, \tag{5}$$

где AV (Asset Value) – это стоимость актива; EF (Exposure Factor) – коэффициент подверженности воздействию угрозы, позволяющий через стоимость актива выразить ущерб, возникающий при реализации угрозы в отношении актива.

Способы определения значений показателей AV и EF зависят от вида актива и типа реализуемой угрозы и должны определяться для каждого случая индивидуально. Например, для угрозы недоступности web-сервера интернет-магазина в результате реализации DDoS-атаки в качестве AV может быть использована стоимость простоя за единицу времени. Значение EF в этом случае будет определяться способностью СОВ противостоять атакам DDoS и его целесообразно выразить в виде отношения времени, за которое будет устранена недоступность, вызванная DDoS-атакой, к единице времени, для которой определена стоимость простоя.

В качестве исходных данных для определения ARO следует использовать имеющуюся в организации статистику, собранную средствами обеспечения ИБ. В случае отсутствия такой статистики значения ARO могут быть определены экспертным методом.

Величина предотвращенного СОВ ущерба (ПУ) по всем угрозам (i) для всех активов (j) может быть определена так:

$$\text{ПУ} = \sum_{i,j} \mathrm{ALE}ij. \tag{6}$$

Экономическая эффективность ($Э_Э$) реализации СОВ может быть определена как разность между величиной предотвращенного ущерба и ССВ:

$$Э_Э = \text{ПУ} - \text{ССВ}. \tag{7}$$

Интегральная оценка эффективности использования методов ИАД в СОВ при обеспечении ИБ ОВС

Интегральная оценка эффективности использования методов ИАД в СОВ при обеспечении ИБ ОВС осуществляется по совокупности показателей (эффективность используемого в СОВ метода ИАД; влияние на телекоммуникационную инфраструктуру; экономические показатели) и, следовательно, относится к многокритериальной оценке эффективности.

В настоящее время на практике широкое распространение получили следующие методы многокритериальной оценки [9]: среднего взвешенного; Парето; последовательных уступок; анализа иерархий; анализа среды функционирования (DEA-АСФ).

Отдельные показатели, используемые для интегральной оценки эффективности использования методов ИАД в СОВ при обеспечении ИБ ОВС, как это было показано выше, могут быть оценены количественно. В интегральной оценке данные показатели должны быть учтены в соответствии с определенными для них весовыми коэффициентами или степенью важности. Для такого класса задач наиболее часто используется метод среднего взвешенного [10, 11]. В этом случае интегральная оценка рассчитывается по следующей формуле:

$$Э = \sum_{i=1}^{n} \alpha_i w_i, \tag{8}$$

где n – число выбранных показателей системы; α_i – весовые коэффициенты, сумма которых равняется единице; w_i – нормированные показатели системы.

Весовые коэффициенты, как правило, определяются экспертным методом. Достоинством метода среднего взвешенного, прежде всего, является простота формализации. К недостаткам метода относятся [9]: субъективность экспертов при определении весовых коэффициентов; неявная взаимная компенсация показателей; использование постоянных весовых коэффициентов, не зависящих от значения показателей.

В работе [9] показано, что влияние недостатков метода среднего взвешенного на получаемую интегральную оценку может быть снижено при использовании метода анализа иерархий [12−14], применяющего метод среднего взвешенного в качестве основы.

- При оценке эффективности применения методов ИАД в СОВ при обеспечении ИБ ОВС целесообразно использовать следующие группы показателей эффективности применения методов ИАД в СОВ: 1) функционирование СОВ в части выполнения основной функции; 2) функционирование СОВ в составе телекоммуникационной инфраструктуры ОВС; 3) экономические показатели СОВ.

  Для оценки *функционирования СОВ в части выполнения основной функции* (первая группа показателей) в статье предложено использование показателей эффективности работы метода ИАД, включающих точность (precision, *P*), полноту (recall, *R*) и гармоническое среднее точности и полноты (*F*-мера, *F*). В статье приведены формулы для расчета этих показателей и даны рекомендации по методике определения на основе имитационного моделирования первичных показателей, используемых в формулах расчета. Также приведены значения показателей точности, полноты и гармонического среднего, полученные в работе [5] по результатам имитационного моделирования СОВ, использующей следующие методы ИАД: опорных векторов; *k*-ближайших соседей; искусственную нейронную сеть; дерево принятия решений.

  Для оценки *функционирования СОВ в составе телекоммуникационной инфраструктуры ОВС* (вторая группа показателей) в статье предложено использование показателей качества обслуживания IP-сетей, включающих: пропускную способность; потери; задержки передачи; готовность (доступность). Даны рекомендации по методике оценки предложенных показателей как с использованием свободно распространяемых утилит, так и специализированных коммерческих решений.

  Для оценки *экономических показателей СОВ* (третья группа показателей) в статье предложено использование показателей ССВ СОВ и величины предотвращенного СОВ ущерба. Даны рекомендации по методике оценки предложенных показателей, включая алгоритм и формулы расчета величины предотвращенного СОВ ущерба и экономической эффективности СОВ.

  Для получения интегральной оценки эффективности использования методов ИАД в СОВ при обеспечении ИБ ОВС, учитывающей показатели всех трех групп, предложено использование метода среднего взвешенного.

Статья подготовлена в рамках работ, проводимых при поддержке РФФИ по теме № 15-29-07981 «Разработка и исследование методов искусственного интеллекта для обеспечения информационной безопасности в облачных вычислительных средах».

Литература

1. *Грушо А.А.*, *Забежайло М.И.*, *Зацаринный А.А.*, *Писковский В.О.*, *Борохов С.В.* О возможностях приложений интеллектуального анализа данных в задачах обеспечения информационной безопасности облачных сред // НТИ. Сер. 2. Информационные процессы и системы. 2015. № 11.
2. *Грушо А.А.*, *Забежайло М.И.*, *Зацаринный А.А.* Контроль и управление информационными потоками в облачной среде // Информатика и ее применение. 2015. Т. 9. № 9. С. 91−97.
3. *Борохов С.В.*, *Кейер П.А.* К вопросу выбора показателей эффективности использования методов интеллектуального анализа данных при обеспечении информационной безопасности облачных вычислительных сред // Системы высокой доступности. 2016. Т. 12. № 4. С. 54−59.
4. The NSL-KDD Data Set [Электронный ресурс]. University of New Brunswick. URL = http://www.unb.ca/cic/datasets/nsl.html (дата обращения 05.07.2017).
5. *Шарабыров И.В.* Система обнаружения атак в локальных беспроводных сетях на основе технологий интеллектуального анализа данных. Дис. … канд. техн. наук. Уфимский государственный авиационно-технический университет. Уфа: 2016.
6. Recommendation ITU-T Y.1541. Internet protocol aspects – Quality of service and network performance. Network performance objectives for IP-based services [Электронный ресурс]. International Telecommunication Union. URL = http://www.itu.int/rec/T-REC-Y.1541-201112-I/en (дата обращения 14.08.2017).

7. Программное обеспечение iperf [Электронный ресурс]. Energy Sciences Network. URL = http://software.es.net/iperf/ (дата обращения 16.08.2017).
8. *Разумов М.* Обоснование расходов на системы обнаружения вторжений [Электронный ресурс]. URL = https://www.securitylab.ru/analytics/216222.php (дата обращения 04.09.2017).
9. *Зацаринный А.А.*, *Ионенков Ю.С.* Некоторые аспекты оценки эффективности автоматизированных информационных систем на различных стадиях их жизненного цикла // Системы и средства информатики. 2016. Т. 26. № 3. С. 123–136.
10. *Окунев Ю.Б.*, *Плотников В.Г.* Принципы системного подхода к проектированию в технике связи. М.: Связь. 1976. 183 с.
11. *Саркисян С.А.*, *Голованов Л.В.* Прогнозирование развития больших систем. М.: Статистика. 1975. 192 с.
12. *Саати Т.*, *Кернс К.* Аналитическое планирование. Организация систем. М.: Радио и связь. 1991. 224 с.
13. *Саати Т.* Принятие решений. Метод анализа иерархий. М.: Радио и связь. 1993. 278 с.
14. *Саати Т.* Принятие решений при зависимостях и обратных связях. Аналитические сети. М.: ЛКИ. 2008. 360 с.

Поступила 7 декабря 2017 г.

Estimation of the effectiveness of using methods of data mining with the provision of information security of cloud computing environments

S.V. Borokhov – Senior Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: sborokhov@ipiran.ru
P.A. Keyer – Senior Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: pkeyer@ipiran.ru

The problems of providing information security of cloud computing environments in the field of practical implementation of information security tools are caused by significant volumes of events that need to be analyzed and reacted in real time. In the article methods of an estimation of efficiency of use of data mining techniques in IDS at maintenance of information security of cloud computing environments are considered.

References

1. *Grusho A.A.*, *Zabezhajlo M.I.*, *Zaczarinny'j A.A., Piskovskij V.O.*, *Boroxov S.V.* O vozmozhnostyax prilozhenij intellektual'nogo analiza danny'x v zadachax obespecheniya informaczionnoj bezopasnosti oblachny'x sred // NTI. Ser. 2. Informaczionny'e proczessy' i sistemy'. 2015. № 11.
2. *Grusho A.A.*, *Zabezhajlo M.I.*, *Zaczarinny'j A.A.* Kontrol' i upravlenie informaczionny'mi potokami v oblachnoj srede // Informatika i ee primenenie. 2015. T. 9. № 9. S. 91–97.
3. *Boroxov S.V.*, *Keyer P.A.* K voprosu vybora pokazatelej ehffektivnosti ispolzovaniya metodov intellektualnogo analiza dannyh pri obespechenii informacionnoj bezopasnosti oblachnyh vychislitelnyh sred // Sistemy vysokoj dostupnosti. 2016. T. 12. № 4. S. 54–59.
4. The NSL-KDD Data Set [Ehlektronnyj resurs]. University of New Brunswick. URL = http://www.unb.ca/cic/datasets/nsl.html.
5. *Sharabyrov I.V.* Sistema obnaruzheniya atak v lokalnyh besprovodnyh setyah na osnove tekhnologij intellektualnogo analiza dannyh. Dis. … kand. tekhn. nauk. Ufimskij gosudarstvennyj aviacionno-tekhnicheskij universitet. Ufa: 2016.
6. Recommendation ITU-T Y.1541. Internet protocol aspects – Quality of service and network performance. Network performance objectives for IP-based services [Ehlektronnyj resurs]. International Telecommunication Union. URL = http://www.itu.int/rec/T-REC-Y.1541-201112-I/en.
7. Programmnoe obespechenie iperf [Ehlektronnyj resurs]. Energy Sciences Network. URL = http://software.es/net/iperf/.
8. *Razumov M.* Obosnovanie raskhodov na sistemy obnaruzheniya vtorzhenij [Ehlektronnyj resurs]. URL = https://www.securitylab.ru/analytics/216222.php.
9. *Zaczarinny'j A.A.*, *Ionenkov Y.S.* Nekotorye aspekty ocenki ehffektivnosti avtomatizirovannyh informacionnyh sistem na razlichnyh stadiyah ih zhiznennogo cikla // Sistemy i sredstva informatiki. 2016. T. 26. № 3. S. 123–136.
10. *Okunev Y.B. and Plotnikov V.G.* Printcipy sistemnogo podhoda k proektirovaniyu v tekhnike svyazi. M.: Svyaz`. 1976. 183 p.
11. *Sarkisjan S.A. and Golovanov L.V.* Prognozirovanie razvitija bol'shih system. M.: Statistics Publs. 1975. 192 p.
12. *Saati T. and Kerns K.* Analiticheskoe planirovanie. Organizatciya sistem. M.: Radio i svyaz'. 1991. 224 p.
13. *Saati T.* Priniatie resheniy. Metod analiza ierarhiy. M.: Radio i svyaz'. 1993. 278 p.
14. *Saati T.* Priniatie reshenij pri zavisimostyakh i obratnykh svyazyakh. Analiticheskie seti. M.: LKI Publ. 2008. 360 p.

УДК 004.6.056: 004.75

Применение технологии блокчейна и криптовалюты для обеспечения работ по государственному оборонному заказу

Д.И. Правиков – к.т.н., ст. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: d_pravikov@mail.ru
А.Ю. Щербаков – д.т.н., профессор, гл. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: x509@ras.ru

Изложены основные принципы и подходы к использованию технологии распределенного реестра (блокчейна) и цифрового актива (криптовалюты) для обеспечения работ по гособоронзаказу.

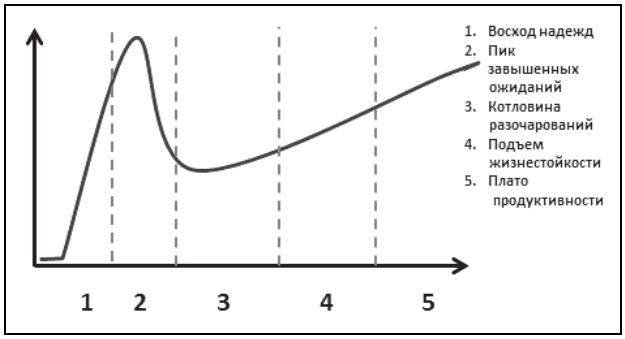
Ключевые слова: *криптовалюта, блокчейн, гособоронзаказ.*

The main principles and approaches to the use of technology distributed register (blockchain) and digital assets (cryptocurrencies) to provide works on the state defense order.

Keywords: *cryptocurrency, blockchain, state defense order.*

В последнее время в различных источниках активно обсуждаются криптовалюты и блокчейн как пример перспективной информационной технологии.

Напомним, что в научно-популярной литературе очень часто приводят эмпирическую зависимость степени позитивного отношения к новой технологии (см. рисунок).



Этапы развития информационно-коммуникационных технологий (ИКТ)

Весьма возможно, что на текущий момент в отношении блокчейна и криптовалют мы находимся на второй стадии – пике завышенных ожиданий, поскольку пока неизвестны широко используемые сервисы или услуги, применяющие данные технологии.

Для того чтобы избежать «котловины разочарования», необходимо выбрать области применения, на которых будут продемонстрированы очевидные для конечных пользователей и других заинтересованных сторон преимущества новой технологии по сравнению с существующими традиционными решениями.

По мнению экспертов – специалистов в области экономики[1] – технологии блокчейна и криптовалют интересны, исходя из следующих позиций: «Во-первых, электронный рубль нужен для удобства проведения транзакций в цифровых системах с помощью специальных кошельков или программных устройств, позволяющих хранить деньги, пополнять счета и производить покупки через интернет без задействования основного банковского счета, что делает такие операции более удобными и безопасными… Во-вторых, вся дискуссия вокруг национальной электронной валюты выглядит как отчаянная попытка уговорить Центральный банк увеличить монетизацию экономики, страдающей от кредитного сжатия, или хотя бы вывести часть денежного оборота за пределы банковской системы, внутри которой сейчас происходит оседание финансовых ресурсов, и дать дополнительную свободу движению капитала внутри страны. В частности, предлагается сделать небольшую эмиссию добавочной электронной валюты, чтобы запустить рост хотя бы в цифровом сегменте российской экономики…»

С точки зрения неэкономиста вышесказанное можно, конечно, весьма огрублено, проиллюстрировать игрой в преферанс, где по ходу игры все считается в вистах (аналог криптовалюты), которые при

[1] Тайный рубль: зачем российской экономике национальная криптовалюта. http://www.rbc.ru/opinions/economics/23/10/2017/59edb53a9a79477502fc7ee1

подведении итогов игры и подтверждении правильности расчетов переводятся в реальные деньги.

С точки зрения технического специалиста явными преимуществами блокчейна и криптовалют являются: 1) возможность трассировки использования каждой криптомонеты; 2) децентрализация (а точнее, полицентрализация) контроля транзакций.

Исходя из мнения экономистов и описанных свойств, использование криптовалюты, на взгляд авторов, лучше всего подходит для осуществления расчетов при реализации государственного оборонного заказа.

Ц е л ь р а б о т ы – изложить основные принципы и подходы к использованию технологии распределенного реестра (блокчейна) и цифрового актива (криптовалюты) для обеспечения работ по гособоронзаказу.

Концепция проекта

В настоящее время определенный контроль за движением финансовых средств, выделенных по государственному оборонному заказу, согласно ФЗ-275, возлагается на уполномоченные банки, которые фактически должны отслеживать всю цепочку платежей, осуществляемых при исполнении каждого государственного контракта. При этом они должны обеспечить как валидацию, так и возможность контроля при проведении финансовых транзакций. Необходимо отметить, что в случае создания сложных изделий, предусматривающих кооперацию значительного числа предприятий, цепочка платежей (с обязательным приложением копий подтверждающих документов) может быть очень большой и практически не доступной для контроля и анализа в ручном режиме. По мнению финансово-экономических работников подрядных организаций, существующие механизмы проведения расчетов при реализации гособоронзаказа достаточно обременительны с точки зрения трудозатрат и, в конечном итоге, приводят к увеличению стоимости поставляемой продукции за счет увеличения накладных расходов.

Для выработки предложений по внедрению новых технологий рассмотрим подробнее, для каких целей был принят Федеральный закон от 29.12.2012 № 275-ФЗ (текущая ред. от 29.07.2017) «О государственном оборонном заказе».

Для начала вспомним в качестве полушуточного примера сцену из мультфильма «Золотая антилопа». Бедняк приходит к радже и демонстрирует ему свои золотые монеты, полученные из нового центра эмиссии – золотой антилопы. Раджа берет их для «сравнения», относит в сокровищницу и «временно» помещает в хранилище вместе со своими золотыми. На просьбу бедняка отдать ему его монеты раджа отвечает, что он не может отличить их от своих и был бы рад отдать, но вдруг с монетами бедняка он отдаст свою монету, а это будет неправильно.

Данный пример демонстрирует одно из свойств современных фиатных денег – обезличенность. Монеты, безналичные счета, даже купюры обезличены с точки зрения того, что невозможно проследить историю каждой единицы валюты в произвольно выбранной транзакции. Да, в отдельных случаях используются номера купюр и специальные пометки, но, как известно из сводок новостей, это относится к оперативно-розыскной деятельности, а не к денежному обращению.

До 2013 г. в случае заключения предприятием нескольких контрактов по государственному оборонному заказу с использованием одного расчетного счета образовывался «общий котел». Как следствие, при осуществлении контроля возникали сложности с точки зрения проверки правильности расходования средств гособоронзаказа, что создавало предпосылки для возможных экономических злоупотреблений.

В качестве организационно-экономической меры противодействия таким возможным злоупотреблениям был принят закон ФЗ-275. Данный закон выделяет группу уполномоченных банков, которые под реализацию каждого государственного контракта открывают отдельный счет. При этом деньги, перечисленные заказчиком на этот счет, могут быть реализованы только для обеспечения выполнения соответствующего государственного контракта (см. главу 3.1 ФЗ-275).

Технические показатели предлагаемого подхода

Несмотря на возможные возражения финансовых специалистов, попытаемся оценить возможное число транзакций, которые будут записываться в проектируемый блокчейн. С учетом разъяснения МО, кото-

рое не находит в законе запрета на оплату командировочных расходов, сырья и комплектующих, амортизации и ремонта основных средств и т.п., возможное число транзакций может составлять несколько сотен, а в случае крупных контрактов с большим числом исполнителей второго и третьего уровня несколько тысяч на один контракт.

Вместе с тем, как представляется, число транзакций целесообразно оценивать применительно не к одному контракту, а к некоему усредненному предприятию, причем за единицу измерения целесообразно брать не рабочий день или неделю, а месяц. Такой подход обусловлен тем, что на таком предприятии существуют обязательные ежемесячные платежи, связанные с обслуживанием здания (арендой помещений), обслуживанием основных средств, оплаты услуг связи, уплаты налогов и сборов, выплаты заработной платы сотрудников и т.п. Как следствие, число транзакций в месяц N будет пропорционально количеству основных средств B, количеству ежемесячно потребляемых услуг S, количеству персонала P, числу n и сложности c_i заключенных контрактов:

$$N = f_1(B,S,P) + f_2\left(\sum_{i=0}^{n} c_i\right).$$

Практический опыт работы компаний по гособоронзаказу показывает, что среднее число финансовых транзакций за рабочий день не превышает нескольких десятков, а пиковые значения не превышают 10^2. Исходя из опыта создания различных баз данных, можно предположить, что с учетом размера одного блока в блокчейне (от одного килобайта) объем хранимых данных при современных объемах хранилищ вряд ли будет каким-либо сдерживающим фактором внедрения технологии.

Более существенным моментом, на взгляд авторов, может явиться пропускная способность каналов связи, а также порядок транзакций – поступления должны опережать расход финансовых средств.

Реализация концепции

Теперь предположим следующую ситуацию. В соответствии с установленными законодательством процедурами, уполномоченным юридическим лицом заключается государственный контракт с поставщиком продукции. Под данный контракт на основании его электронной формы центром эмиссии выпускается криптовалюта, которая в рамках как авансирования, так и окончательного расчета перечисляется подрядчику. Данные о генерации криптовалюты содержат сведения о конкретном государственном контракте, и предполагается, что выпущенная валюта будет обеспечена товаром, поставленным по гособронзаказу.

Данные средства подрядчик может использовать для следующих целей: уплаты налогов и обязательных платежей; расчетов с другими субподрядчиками в рамках выполнения конкретного государственного контракта; выплаты заработной платы работникам предприятия; других необходимых выплат.

Понятно, что вся цепочка транзакций по конкретному государственному контракту отражается в копиях блокчейна, которые могут храниться, в первую очередь, в контрольных и правоохранительных органах. ФНС может проверить, со всех ли выплат по контракту заплачены налоги и обязательные платежи. Правоохранительные органы могут полностью проверить не только факт расходования средств по конкретному государственному контракту, но и его обоснованность, так как каждая транзакция должна будет иметь в блокчейне копию подтверждающих документов (или ее функцию от их цифрового образа). Отдельно стоит отметить пока детально не проработанный механизм перевода крипторублей в реальные рубли для выплаты заработной платы. Как представляется, введение отдельной системы контроля за этой операцией позволит снизить возможные коррупционные риски.

Вышеописанное предложение может быть реализовано на базе схемы, описанной в [1]. Данную схему предлагается доработать следующим образом. Выпуск монет осуществляется только центром эмиссии под заключенные контракты. Для осуществления обращения выработанная монета, стоимость которой изначально равна стоимости контракта, должна внутри системы иметь возможность быть разделенной на более мелкие по стоимости монеты с целью оплаты поставок субподрядчиков. Деление монеты возможно как центром эмиссии, так и участниками работ по проектам (по разрешению центра эмиссии).

Область хранения – блокчейн – распределен в центре эмиссии, фискальных и контролирующих государственных органах, уполномоченных банках и подрядных организациях. С целью разграничения доступа каждое звено (а, возможно, и каждый атом блокчейна) должен иметь метку конфиденциальности, которая позволит реализовать политику безопасности как в интересах заказчика, так и в интересах подрядчиков, которые могут быть заинтересованы в сокрытии своих субподрядчиков и поставщиков. Блокчейн может быть реализован в рамках национального оператора, который выполняет подключение всех участников и обеспечивает доступ к звеньям и атомам блокчейна в соответствии с правами доступа и ролями участников работ.

Исходя из [2], можно выделить следующие группы требований к блокчейну, используемому для хранения информации о работах по гособоронзаказу.

1. *Структурные*, касающиеся наличия в звеньях блокчейна тех или иных типов данных (атомов) для обеспечения работы заданных технологий. В частности, в звеньях блокчейна должны храниться все транзакции по делению «контрактной монеты», кроме того, наличие звеньев типа Y, связанных с необходимостью гарантированного по длительности времени перебора значений, могут быть использованы для реализации конкурсных процедур или открытия условий и результатов конкурсов в заданные сроки.

2. *Организационные*, связанные с национальным криптографическим регулированием и предполагающие применение национальных, рекомендованных или сертифицированных криптографических средств для формирования и обработки атомов блокчейна. Кроме того, данная группа может включать требования, связанные с национальными или ведомственными нормативами в областях применения – налоговая сфера, конкурсные процедуры, корпоративный документооборот и т.д.

3. *Технологические*, связанные с надежностью хранения звеньев блокчейна, что должно обеспечивать заданные регуляторами соответствующих отраслей, в которых используется блокчейн, параметры надежности хранения и доступности этих звеньев. Кроме того, технологические требования должны описывать требования к производительности операций со звеньями и предельные объемы их накопления и хранения.

4. *Требования доверия*, имеющие четкую структуру блокчейна, регламентированные технологии работы со звеньями, а также интерфейс для выполнения операций над звеньями. Для обеспечения высокого доверия все прикладные интерфейсы должны быть стандартизованы и доступны в исходных кодах. Кроме того, технология может быть формально верифицирована с помощью математических моделей. Возможные технологии верификации описаны в [3].

Более подробная схема может быть проработана как результат выполнения поручений Президента РФ по итогам совещания по вопросу использования цифровых технологий в финансовой сфере, состоявшегося 10 октября 2017 г.

Технико-экономические показатели

Проведем технико-экономический анализ по следующим направлениям использования предлагаемой технологии: стоимость хранения информации; объем трафика; скорость транзакций; архитектура хранения данных и транзакций; сохранение инвестиций в ИТ-проект.

Стоимость хранения информации. В настоящее время средняя стоимость хранения информации в ЦОД общего назначения в России составляет около 30…40 руб. за Гб в месяц[2]. В корпоративных ЦОД эта сумма увеличивается в 3…5 раз. На данный момент по оценкам зарубежных экспертов цена хранения 1 Гб данных при пропускной способности в 30 Гб в месяц обходится в $1,51[3]. С учетом более компактного хранения информации в разрабатываемом отечественном прототипе распределенного реестра объем хранения может быть уменьшен в 2…2,5 раза, соответственно, во столько же раз снизится стоимость хранения информации.

Объем трафика. За счет оптимизированной структуры данных и использования предельных оптимизаций криптографических алгоритмов приблизительно в 1,7 раза уменьшен объем служебного трафика. Кроме того, межведомственное использование распределенного реестра позволит избежать дублиро-

[2] Рекомендации по выбору ЦОД в России. https://habrahabr.ru/post/246419/

[3] Распределенное хранение данных: от облака до блокчейна. https://forklog.com/raspredelennoe-hranenie-dannyh-ot-oblaka-do-blokchejna/

вания трафика для почтовых рассылок и доступа к базе данных. Экспертная оценка дает значение уменьшения в среднем порядка 4,8 раза.

Скорость транзакций. Современная оценка скорости транзакций биткоина – 7 транзакций в секунду, у Ethereum – 15. Причем эта оценка распространяется на всю сеть, поскольку каждый узел полностью реплицирует другие узлы[4]. Добавление нового узла повышает устойчивость системы, но никоим образом не увеличивает скорость ее работы или максимальный объем хранения данных. То есть изменение данных (каждое изменение данных в блокчейне – это транзакция) является абсолютно минимизирующим фактором.

Отечественный прототип может быть лишен этого недостатка, в настоящее время скорость транзакций даже без применения специализированных аппаратных платформ составляет до 3000 транзакций в секунду, то есть это более чем в 100 раз выше, чем Ethereum и Masterchain. Это позволяет не только получить стратегический эксплуатационный выигрыш, но и расширить поле применения отечественной технологии, в частности, для платежных систем реального времени.

Архитектура хранения данных и транзакций. Как отмечает источник [4], состояние блокчейна является базой данных «ключ-значение», она достаточно примитивна. Поиск в такой базе данных возможен только по первичному ключу, объем хранимых данных очень ограничен. Для серьезных приложений этого явно недостаточно. Таким образом, при разработке приложений на блокчейнах, например, для Ethereum и Masterchain, проблема хранения и обработки данных стоит очень остро. Сейчас нет удовлетворительных способов ее решения.

Предлагаемая технология будет содержать универсальные интерфейсы формирования данных и доступа к ним, которые могут быть встроены в любое приложение и обеспечить работу аналитических и управленческих систем государственного уровня, минимизировав затраты в них на этапе разработки и внедрения. По оценкам экспертов, применение стандартизованных интерфейсов снижает стоимость разработки, владения, сопровождения и обучения примерно на 25…30%.

Кроме того, в отечественный прототип будут встроены методы обеспечения информационной безопасности (ИБ) в соответствии с требованиями национальных регуляторов. По оценкам экспертов, затраты на ИБ составляют 7…9% стоимости ИТ-проекта[5], соответственно, настолько же можно дополнительно минимизировать стоимость проектов.

Сохранение инвестиций. Предлагаемая концепция обеспечит совместную работу уже созданных ведомствами ИТ-систем, минимизировав затраты в них на этапе разработки и внедрения. Рассматриваемый проект не требует дополнительных инвестиций в аппаратные платформы и их сопровождение, снижает требования к объемам хранения и трафику.

- Принципиальными преимуществами изложенного подхода являются:

  1) отсутствие необходимости появления новой фиатной валюты, сохранение центра эмиссии в руках государства (выигрыш регулятора);

  2) повышение контроля за использованием средств, выделенных на реализацию государственного заказа; повышение эффективности исполнения требований ФЗ-275 (выигрыш контролирующих и фискальных органов);

  3) возможность государственного контроля при отработке технологии блокчейн (выигрыш разработчиков технологий);

  4) возможность снижения непроизводственных затрат у поставщиков госзаказчиков (выигрыш конечных пользователей).

  По мнению авторов, общий экономический эффект проекта может составить не менее половины от сумм на формирование, реализацию и поддержку ИТ-проектов государственного уровня, а также в несколько раз (до десяти) минимизировать затраты на обеспечение гособоронзаказа.

[4] Где хранить данные децентрализованным приложениям на блокчейне? https://habrahabr.ru/post/327836/

[5] Оценка затрат компании на ИБ. http://bre.ru/security/18881.html

Литература

1. *Щербаков А.Ю.* Синтез универсальной архитектуры и протокола криптовалюты в рамках национального проекта // Системы высокой доступности. 2017. Т. 13. № 3. С. 15–18.
2. *Биктимиров М.Р.*, *Домашев А.В.*, *Черкашин П.А.*, *Щербаков А.Ю.* Блокчейн: универсальная структура и требования // НТИ. Сер. 2. Информ. процессы и системы. 2017. № 11. С. 1–4.
3. *Домашев А.В.*, *Грунтович М.М.*, *Попов В.О.*, *Правиков Д.И.*, *Щербаков А.Ю.* Программирование алгоритмов защиты информации: Учеб. пособие. М.: Нолидж. 2001. 552 с.
4. *Black F.* Banking and interest rates in a world without money: the effects of uncontrolled banking // Journal of Bank Research. 1970. № 1(Autumn). P. 9–20.
5. *Fama E.F.* Banking in the theory of finance // Journal of Monetary Economics. 1980. № 6. P. 39–57.
6. *Hall R.E.* Monetary trends in the United States and the United Kingdom: a review from the perspective of new developments in monetary economics // Journal of Economic Literature. 1982. № 20. P. 1552–1556.
7. *Kareken J. and Wallace N.* On the indeterminacy of equilibrium exchange rates // Quarterly Journal of Economics. 1981. № 96(2). P. 207–222.
8. *Meiklejohn S.*, *Pomarole M.*, *Jordan G.*, *Levchenko K.*, *McCoy D.*, *Voelker G.M. and Savage S.* A fistful of Bitcoins: characterizing payments among men with no names // Proc. of the 2013 Conference on Internet Measurement.
9. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org. 2008.
10. *Wallace N.* A legal restrictions theory of the demand for 'money' and the role of monetary policy // Federal Reserve Bank of Minneapolis Quarterly Review. 1983. № 7. P. 1–7.
11. *Russinovich M.* Introducing Azure confidential computing. 2017. URL = https://azure.microsoft.com/ru-ru/blog/introducing-azure-confidential-computing/.

Поступила 7 декабря 2017 г.

The use of blockchain and cryptocurrency technology to support work on the state defense order

D.I. Pravikov – Ph. D. (Eng.), Senior Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: d_pravikov@mail.ru
A.Yu. Scherbakov – Dr. Sc. (Eng.), Professor, Main Research Scientist,
FRC «Computer Science and Control» RAS (Moscow)
E-mail: x509@ras.ru

The main principles and approaches to the use of technology distributed register (blockchain) and digital assets (cryptocurrencies) to provide works on the state defense order are described. The overall economic effect of the project may amount to at least half of the sums for the formation, implementation and support of state-level IT projects, and also to several times (up to ten) minimize the costs of securing the state defense order.

References

1. *Shherbakov A.Yu.* Sintez universal'noj arxitektury' i protokola kriptovalyuty' v ramkax naczional'nogo proekta // Sistemy' vy'sokoj dostupnosti. 2017. T. 13. № 3. S. 15–18.
2. *Biktimirov M.R.*, *Domashev A.V.*, *Cherkashin P.A.*, *Shherbakov A.Yu.* Blokchejn: universal'naya struktura i trebovaniya // NTI. Ser. 2. Inform. proczessy' i sistemy'. 2017. № 11. S. 1–4.
3. *Domashev A.V.*, *Gruntovich M.M.*, *Popov V.O.*, *Pravikov D.I.*, *Shherbakov A.Yu.* Programmirovanie algoritmov zashhity' informaczii: Ucheb. posobie. M.: Nolidzh. 2001. 552 s.
4. *Black F.* Banking and interest rates in a world without money: the effects of uncontrolled banking // Journal of Bank Research. 1970. № 1(Autumn). P. 9–20.
5. *Fama E.F.* Banking in the theory of finance // Journal of Monetary Economics. 1980. № 6. P. 39–57.
6. *Hall R.E.* Monetary trends in the United States and the United Kingdom: a review from the perspective of new developments in monetary economics // Journal of Economic Literature. 1982. № 20. P. 1552–1556.
7. *Kareken J. and Wallace N.* On the indeterminacy of equilibrium exchange rates // Quarterly Journal of Economics. 1981. № 96(2). P. 207–222.
8. *Meiklejohn S.*, *Pomarole M.*, *Jordan G.*, *Levchenko K.*, *McCoy D.*, *Voelker G.M. and Savage S.* A fistful of Bitcoins: characterizing payments among men with no names // Proc. of the 2013 Conference on Internet Measurement.
9. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org. 2008.
10. *Wallace N.* A legal restrictions theory of the demand for 'money' and the role of monetary policy // Federal Reserve Bank of Minneapolis Quarterly Review. 1983. № 7. P. 1–7.
11. *Russinovich M.* Introducing Azure confidential computing. 2017. URL = https://azure.microsoft.com/ru-ru/blog/introducing-azure-confidential-computing/.

УДК 004.6.056: 004.75

Синтез универсальной изолированной криповалютной сети

А.В. Домашев – начальник отдела, НТЦ «Атлас»
E-mail: domix@stcnet.ru
А.Ю. Щербаков – д.т.н., профессор, гл. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: x509@ras.ru

Предложено понятие изолированной криптовалютной сети (ИКВС). Изложены принципы и подходы к синтезу универсальной архитектуры и протокола ИКВС.

Ключевые слова: *криптовалюта (КВ), электронная подпись (ЭП), удостоверяющий центр (УЦ), криптовалютный кошелек (КВК), криптовалютная сеть, изолированная криптовалютная сеть (ИКВС).*

Proposed the concept of an isolated cryptocurrency network, the principles and approaches to the synthesis of a generic architecture and protocol of the isolated cryptocurrency network.

Keywords: *cryptocurrency (CC), digital signature (DS), certification authority (CA), cryptocurrency wallet (CCW), cryptocurrency network, isolated cryptocurrency network (ICCN).*

Возрастающее влияние криптовалют (КВ) и связанных с ними технологий (в частности, блокчейна) в национальных экономиках ставят актуальную задачу синтеза решений, одинаково приемлемых как для бизнеса, так и для государственных структур и регуляторов экономики [1−3, 8].

Основной экономический и регулятивный смысл использования КВ в государственной экономике состоит в обеспечении тех же институциональных принципов использования криптофинансов, как и обычных денежных средств в сфере обмена, накопления и платежа. Это означает, в первую очередь, установление одних и тех же правил обработки транзакций для различных КВ, изоляцию контура обращения КВ от других платежных систем, обеспечение контроля транзакций и выполнение других требований, которые выдвигает национальный регулятор платежной системы.

Как в классической компьютерной безопасности обеспечение гарантированных политик безопасности возможно только в изолированной среде программных субъектов, так и для криптовалютной системы выполнение вышеприведенных требований возможно только при организации изолированной сети транзакций.

Ц е л ь р а б о т ы – рассмотреть технологию, позволяющую реализовать в рамках практически любой криптовалютной среды изолированную сеть (изолированную криптовалютную сеть – ИКВС), в которой гарантируется циркуляция транзакций только в рамках централизованно регулируемой клиентской базы.

Терминология

Перед тем как перейти к подробному рассмотрению протокола ИКВС, зафиксируем общие и специальные используемые термины и сокращения.

Общие термины и сокращения: ЭП – электронная подпись; HSM – Hardware Security Module; УЦ – удостоверяющий центр; БД – база данных.

Специальные термины и сокращения: ИКВС – изолированная криптовалютная сеть; ГУЦ – головной УЦ; КВ – криптовалюта; КВК – криптовалютный кошелек; ОКВК – оператор КВК; ОИКВС – оператор ИКВС; УЦ УК – УЦ управления клиентами; КВС – криптовалютная сеть; АВ КВК – агент восстановления КВК; БД АВ КВК – база данных АВ КВК.

Концепция изолированной криптовалютной сети

Одним из главных условий практической значимости реализации ИКВС является независимость функционирования данной среды от особенностей реализации протоколов и форматов конкретной КВ. На практике это означает, что при реализации не должны использоваться, например, возможности

смарт-контрактов, реализованных в среде Ethereum, или multisignature сценариев Bitcoin. Технология изолированности среды должна быть реализована полностью «наложенными» средствами.

Для того чтобы реализовать концепцию изолированности клиентов ИКВС, введем промежуточное звено (назовем его оператором КВК) между клиентом и криптовалютной средой, в которой он намерен осуществлять операции. Данное промежуточное звено должно осуществлять следующие основные операции:

создание КВК по соответствующему запросу клиента;

возвращение клиенту набора данных, необходимых для проведения дальнейших транзакций для созданного КВК (переданный клиенту набор данных КВК не должен позволять ему самостоятельно проводить операции с КВК);

проведение транзакций по соответствующему запросу клиента, в котором он предоставляет ранее полеченные данные КВК.

Как известно, в КВС кошелек – это ключевая пара (то есть закрытый (секретный) и соответствующий ему открытый ключ), а возможность проведения транзакций основывается на владении секретным ключом пары и, соответственно, возможностью сгенерировать валидную ЭП. Таким образом, задача реализации ОКВК сводится к построению криптографической схемы, в которой для проведения транзакции необходимо участие как клиента, так и оператора.

Необходимым условием, дающим клиенту возможность обращаться к ОКВК, примем получение клиентом сертификата у специального оператора, управляющего допуском к ИКВС (назовем его ОИКВС). Использование сертификатов позволяет построить схему регистрации и работы операторов и клиентов на стандартных компонентах и протоколах, которыми являются УЦ и программное обеспечение, поддерживающее работу с ними.

Очевидно, что ОИКВС может быть несколько, каждый из которых поддерживает независимые бизнес-процессы. Однако при этом нет необходимости в том, чтобы каждому ОИКВС соответствовал свой ОКВК. ОКВК может представлять из себя независимый сервис, поддерживающий по договоренности работу с несколькими ОИКВС.

В общем случае два этих оператора могут управляться одним и тем же органом. Однако разделение данных операторов, безусловно, рекомендуется.

Предложения по реализации изолированной криптовалютной сети

В данном разделе представлена концепция реализации ИКВС. Разумеется, описание в этом разделе представляет собой описание подхода к решению данной задачи и не учитывает многие вопросы практической реализации, которые рассмотрены в следующих разделах.

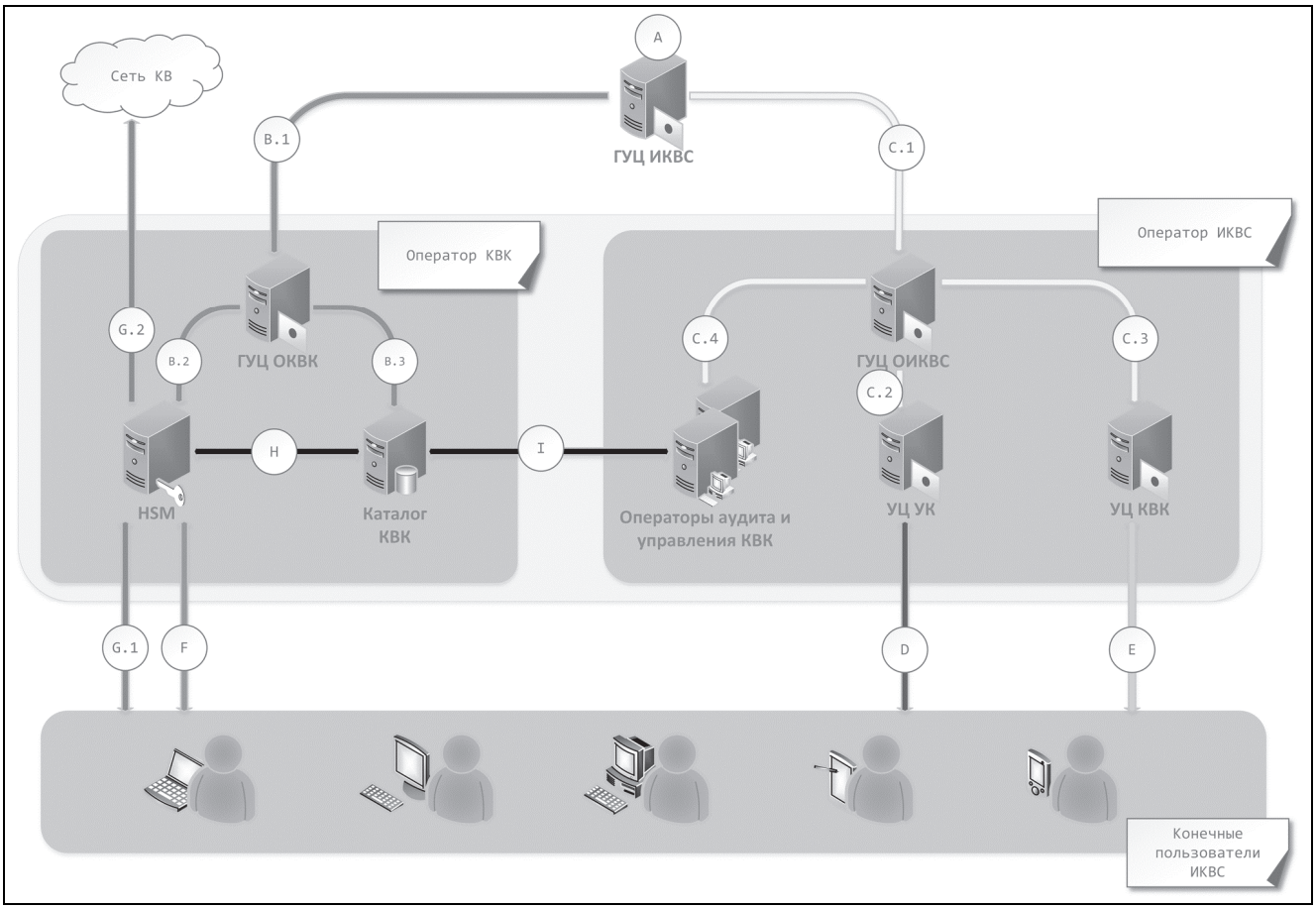
Кроме того, в представленной схеме аутентификация и авторизация конечных пользователей базируется исключительно на сертификатах и разрешениях, которые соответствующий УЦ включит в них. Данная модель является статической в том смысле, что не позволяет в динамике управлять разрешениями конечных пользователей, и поэтому на практике может быть недостаточной. Более гибкие модели управления разрешениями в среде ИКВС также рассмотрены в следующих разделах.

В процессе описания схемы работы ИКВС будут рассмотрены д в а п о д х о д а к тому, известен ли конечному пользователю его реальный адрес в среде КВ. П е р в ы й п о д х о д заключается в том, что несмотря на то, что он не может воспользоваться самостоятельно секретным ключом КВК, реальный адрес КВК конечному пользователю известен (по сути, ему известен открытый ключ КВК). В т о р о й п о д х о д , как понятно, заключается в том, что конечному пользователю неизвестен и открытый ключ КВК, то есть он не знает и адреса КВК, которым он управляет. Выбор того или иного подхода определяется исключительно характеристиками деятельности, которую хочет организовать ОИКВС. Однако очевидно, что знание пользователем его реального адреса оказывает прямое влияние на характеристики анонимности в среде ИКВС.

Общая схема предлагаемой ИКВК приведена на рисунке. Рассмотрим основные этапы инициализации и работы ИКВС.

Этап А. Инициализация ГУЦ ИКВС.

Вопрос как и откуда ГУЦ ИКВС получит свой сертификат (iccn_head_ca_cert), очевидно, не относится к концепции ИКВС и зависит от задач, поставленных перед конкретной реализацией ИКВС. В за-



Общая схема ИКВС

висимости от целей создаваемой системы ГУЦ ИКВС для своей инициализации может обратиться для получения сертификата к УЦ национального (наднационального), регионального или корпоративного уровня, обладающего необходимыми компетенциями.

Этап B. Инициализация ОКВК.

Инициализация ОКВК начинается с получения его ГУЦ сертификата (ccw_op_head_ca_cert) у ГУЦ ИКВС (шаг B.1). Шаг B.1 является регистрацией нового ОКВК в системе.

ОКВК (см. рисунок) состоит из двух основных элементов: ГУЦ и HSM. Для завершения инициализации ОКВК HSM генерирует секретный ключ (ccw_op_hsm_private_key) и получает сертификат (ccw_op_hsm_cert) открытого ключа у своего ГУЦ (шаг B.2).

Этап C. Инициализация ОИКВС.

Инициализация ОИКВС, как и ОКВК, начинается с получения его ГУЦ сертификата (iccn_op_head_ca_cert) у ГУЦ ИКВС (шаг C.1). Шаг C.1 является регистрацией нового ОИКВС в системе.

ОИКВС (см. рисунок) состоит из четырех основных элементов: ГУЦ, УЦ УК, УЦ КВК и БД АВ КВК. Для завершения инициализации УЦ УК и УЦ КВК запрашивают сертификаты открытых ключей (iccn_op_end_user_ca_cert и iccn_op_ccw_ca_cert), необходимых для их активации (шаг C.2 и шаг C.3 соответственно).

После активации всех УЦ инициализируется БД операторов восстановления. Для этого оператор (операторы) восстановления генерируют секретные ключи и запрашивают сертификаты открытых ключей у своего ГУЦ (шаг C.4).

Этап D. Регистрация клиента у ОИКВС.

Этап регистрации, как и в остальных случаях, представляет собой запрос и получение сертификата (end_user_iccn_cert) у соответствующего ОИКВС. Обработку этих запросов в рамках ОИКВС ведет УЦ УК (см. рисунок). Таким образом, клиент получает сертификат открытого ключа с включенными в него

разрешениями (end_user_iccn_perms), который он в дальнейшем будет использовать для аутентификации при обращении к сервисам ИКВС.

Какие данные клиент должен предъявить для получения сертификата, а также какие данные будут внесены в его сертификат, зависит от политики соответствующего ОИКВС. Кроме этого, важным моментом, который должен определить ОИКВС, являются параметры доступа к каталогу сертификатов. Будет ли он публичным, доступным только аутентифицированным клиентам или закрытым, также определяется текущей политикой.

Этап E. Получение сертификата КВК.

К настоящему моменту клиент, зарегистрировавшись у ОИКВС и получив соответствующий сертификат, имеет возможность обращаться к сервисам ИКВС.

Поскольку в изолированной среде клиент работает с КВК посредством ОКВК и не владеет секретным ключом кошелька, то для идентификации КВК предлагается использовать специальный сертификат, к которому ОКВК и будет привязывать реальный КВК и на котором будет производиться шифрование и ЭП информации, связанной с этим кошельком. Кроме того, использование для каждого КВК отдельного сертификата позволит ОИКВС проводить в случае необходимости целевую блокировку кошелька просто путем отзыва соответствующего сертификата.

Таким образом, на этом этапе клиент обращается к УЦ КВК, проходит аутентификацию и запрашивает сертификат КВК (end_user_ccw_cert). Аутентификация может быть проведена по протоколу TLS с использованием штатной возможности клиентской аутентификации. При обращении за сертификатом КВК клиент может указать разрешения (end_user_ccw_perms), которые он хотел бы получить. Например, тип КВ, максимальный объем кошелька, возможность обращения к внешним шлюзам ИКВС (рассматриваются далее) и др. Конкретный перечень разрешений сертификата и требования к его получению определяются политикой конкретного ОИКВС.

После успешного получения сертификата КВК клиент может обращаться с запросами к ОКВК.

Этап F. Подключение реального КВК к сертификату клиента.

На этом этапе клиент обращается к соответствующему ОКВК для создания для него КВК. Запрос подписывается на сертификате, полученном от ОИКВС на этапе F. Таким образом, ОКВК имеет возможность проверить полномочия клиента для создания КВК.

После проверки валидности запроса HSM оператора создает (или использует уже созданную) ключевую пару КВК (ccw_private_key и ccw_public_key). Из открытого ключа формируется токен открытого ключа (ccw_public_key_token), а из секретного ключа токен секретного ключа (ccw_private_key_token).

Токен ccw_private_key_token получается путем шифрования и подписи ccw_private_key на сертификате ОКВК ccw_op_hsm_cert, полученном на этапе B (шаг B.2). В состав токена также входит идентификатор сертификата конечного пользователя end_user_ccw_cert_id. Включение идентификатора необходимо, чтобы ОКВК мог при обращении проверить соответствие идентификатора сертификата конечного пользователя, который к нему обратился, и идентификатора сертификата из токена.

Токен ccw_public_key_token также может быть получен путем шифрования и подписи на сертификате ОКВК ccw_op_hsm_cert, если есть необходимость в скрытии от клиента реального адреса КВК. В противном случае достаточно только подписи. В состав ccw_public_key_token также входит идентификатор сертификата end_user_ccw_cert_id.

После этого оба токена (ccw_private_key_token и ccw_public_key_token) направляются клиенту в ответ на его запрос.

Таким образом, после этого шага клиент владеет всей необходимой информацией для осуществления криптовалютных транзакций в рамках ИКВС.

Этап G. Проведение транзакции для КВК.

Теперь для проведения транзакции клиенту необходимо сформировать параметры транзакции и подписать запрос сертификатом end_user_ccw_cert, полученным на этапе E.

Для формирования транзакции конечный пользователь должен по соответствующим каналам получить целевые адреса в виде токенов ccw_public_key_token. Получить он их может либо в результате непосредственного взаимодействия с другими пользователями (например, по электронной почте), либо если ОИКВС предусмотрит какой-либо общедоступный каталог для размещения такой информации (например, непосредственно в свойствах сертификатов в каталоге УЦ КВК).

Получив запрос, ОКВК проводит следующие действия (шаг G.2):

1) проверяет валидность подписи запроса;

2) расшифровывает (если необходимо) ccw_public_key_token отправителя транзакции;

3) проверяет подпись ccw_public_key_token отправителя транзакции;

4) расшифровывает ccw_private_key_token отправителя транзакции и получает секретный ключ КВК ccw_private_key;

5) проверяет подпись ccw_private_key_token отправителя транзакции;

6) расшифровывает (если необходимо) ccw_public_key_token получателей транзакции;

7) проверяет подпись ccw_public_key_token получателей транзакции;

8) проверяет валидность сертификатов end_user_ccw_cert получателей транзакции;

9) проверяет валидность сертификатов end_user_iccn_cert получателей транзакции;

10) формирует и подписывает запрашиваемую транзакцию на ключе ccw_private_key отправителя транзакции;

11) отправляет транзакцию с сеть соответствующей КВ;

12) отправляет конечному пользователю подписанное подтверждение проведения транзакции.

Таким образом, представленная схема гарантирует, что конечные пользователи ИКВС имеют возможность передавать транзакции только другим зарегистрированным пользователям ИКВС.

После приведения описания работы ИКВС более понятным должно стать предложенное ранее деление «полнофункционального» ОИКВС (серая область на рисунке) на два независимых компонента: собственно ОИКВС и ОКВК. В области ОКВК собраны компоненты, работающие непосредственно с транзакциями конечных пользователей и криптовалютными средами. Организация, заинтересованная в создании для каких-либо целей изолированной криптовалютной среды, может и не иметь таких специфических компетенций. Задача «малого» ОИКВС – это управление подключением конечных пользователей к изолированной среде. Кроме того, введение дополнительного независимого оператора безусловно повышает и уровень доверия конечных пользователей к системе в целом.

И еще одно замечание в отношении ОКВК. Как можно заметить из приведенного описания, ОКВК не хранит результатов своих операций. Результаты всех проведенных им операций отправляются или конечным пользователям, или в криптовалютную сеть. Это очень выгодное свойство с точки зрения простоты реализации HSM и оператора в целом. Однако, конечно, возможности такой реализации могут не удовлетворить запросы организатора ИКВС.

В следующих разделах рассматриваются дополнительные компоненты ИКВС, которые позволяют динамически управлять разрешениями конечных пользователей.

Дополнительные компоненты изолированной криптовалютной сети

При описании базовых принципов функционирования ИКВС, изложенных в предыдущем разделе, были для упрощения опущены несколько важных компонентов. Этими компонентами являются каталог КВК, а также операторы аудита и управления (см. рисунок).

Как уже отмечалось, «статическая» модель управления разрешениями, в которой разрешения конечных пользователей хранятся в сертификате и могут быть изменены только перевыпуском соответствующего сертификата, не всегда может удовлетворить запросы организатора ИКВС. Таким образом, для хранения каталога конечных пользователей, связанных с ними КВК и соответствующих разрешений вводится компонент каталог КВК. Со стороны ОИКВС текущими разрешениями, хранящимися в каталоге, управляет оператор управления КВК.

В связи с введением новых компонент этап F может быть дополнен шагом H (см. рисунок), на котором будут проверены текущие разрешения конечного пользователя на проведение запрошенной транзакции.

Помимо управления разрешениями, ОИКВС безусловно может быть заинтересован в текущем аудите транзакций конечных пользователей. Для этого оператор аудита КВК может также обратиться в каталог КВК и, получив соответствующую информацию, проводить аудит целевой криптовалютной сети.

Ну и наконец, организатор ИКВС может быть заинтересован в том, чтобы при необходимости проводить операции с КВК конечных пользователей. Это может быть прежде всего связано с необходимо-

стью обеспечения возможности возвращения средств транзакции, признанной по каким-либо причинам необходимой к отмене. Для этого оператор администрирования КВК должен иметь доступ к секретным ключам КВК. Наиболее очевидная схема реализации данного требования – это дополнение этапа F шагом создания токена секретного ключа, зашифрованного на сертификате оператора администрирования КВК, полученном на шаге С.4. Этот токен может быть в зависимости от требований оператора сохранен в каталог КВК или напрямую передан ОИКВС для хранения и использования.

Таким образом, дополненная компонентами каталога КВК и операторами аудита и администрирования ИКВС приобретает возможности динамического управления разрешениями при работе с КВК и аудита пользовательских транзакций, а также возможность возвращать полностью или частично уже проведенные транзакции.

Варианты реализации функциональности оператора криптовалютного кошелька

На схеме (см. рисунок) центральным элементом ОКВК является HSM. Основная функция данного аппаратного модуля очевидна и определяется необходимостью расшифровывать клиентские ключи и подписывать транзакции внутри HSM. Это предотвращает вероятность как случайной утечки, так и целенаправленной атаки на ключевую систему ОКВК. Данный модуль ОКВК может быть реализован как физически защищенный компьютер или специальный чип.

В качестве готового решения специального чипа могут быть использованы, например, чипы, реализующие функциональность TPM (Trusted Platform Module). Определенным недостатком такого решения является ограниченная функциональность ТР. Модуль TPM реализует только определенный набор базовых криптографических преобразований.

Более функциональным решением может являться реализация функциональности ядра ОКВК в рамках доверенной среды исполнения (Trusted Execution Environment – TEE). Примером наиболее развитой TEE является технология Intel SGX (Software Guard Extensions). Данная технология дает возможность вынести в изолированную доверенную среду исполнения не только непосредственно работу с ключами, но и полное функциональное ядро ОКВК.

Кроме того, в настоящее время крупнейшие операторы облачных сервисов предлагают возможность реализации доверенной среды исполнения в рамках облачной среды. Так компания Microsoft предлагает в рамках сервиса Azure Confidential Computing сразу два варианта реализации TEE. Кроме варианта на основе технологии Intel SGX, Microsoft предлагает также вариант программной реализации доверенной среды исполнения на основе Virtual Secure Mode [10].

Прямая передача криптовалютного кошелька как внутренняя транзакция изолированной криптовалютной сети

При всех своих достоинствах сети таких КВ, как Bitcoin и Ehtereum, обладают рядом врожденных недостатков в части проведения транзакций. Это существенное (особенно у Bitcoin) включение в блокчейн с необходимостью платить майнерам за включение в блокчейн. Необходимость платы за включение в блок приобретает большое значение в случае обмена большим числом малых по стоимости транзакций (микроплатежи), когда плата майнерам может превысить объем перевода.

В настоящее время предложен целый ряд вариантов так называемых протоколов Payment Channel, предлагающих возможность реализовать в недоверенной среде обмен транзакциями без необходимости включения их всех в блок.

В части решения данной проблемы ИКВС также может предложить оригинальное решение, базирующееся на его основополагающем свойстве. Основополагающим свойством ИКВС является то, что конечный пользователь не владеет секретным ключом КВК и оперирует кошельком посредством ОКВК. Таким образом, конечный пользователь имеет возможность просто передать посредством ОКВК свой кошелек другому конечному пользователю.

С криптографической точки зрения эта операция выглядит просто как получение от конечного пользователя, передающего КВК, токена ccw_private_key_token, расшифрование его и зашифрование с новым идентификатором end_user_ccw_cert_id конечного пользователя, получающего КВК. После это-

го в каталог КВК вносятся соответствующие изменения о владельце КВК и токены открытого и секретного ключей отсылаются новому владельцу.

В реальности, разумеется, эффективность применения данной схемы зависит от «правильного» распределения криптовалютых активов по кошелькам конечных пользователей. Поскольку если передать необходимо не все средства, которые в текущий момент имеются в кошельке, то все равно возникает дополнительная криптовалютная транзакция. Впрочем, эта проблема тоже может быть решена в среде ИКВС. Если необходимо провести «мгновенную» транзакцию, а при этом ровной суммы для перевода нет, то конечный пользователь может запросить у ОКВК операцию передачи кошелька с указанием суммы, необходимой к возврату. После этого ОИКВС может через управление каталогом КВК заблокировать указанную сумму в кошельке получателя и таким образом добиться от получателя КВК возврата «сдачи» в виде перевода или просто возврата КВК со «сдачей».

На данном примере видно, что при реализации правильно настроенной схемы динамического управления разрешениями конечных пользователей по доступу к КВК в рамках ИКВС можно реализовать схему «мгновенных» переводов криптовалютных средств, гарантированных ОИКВС.

Сценарии и смарт-контракты в среде изолированной криптовалютной сети

До настоящего момента изолированность криптовалютной сети рассматривалась только в части отправителя и получателя транзакций. Однако такого понимания изолированности достаточно, только если ИКВС ограничивает тип разрешенных транзакций лишь транзакциями, переводящими криптовалютные средства с одного адреса на другой. К таким типам транзакций можно отнести Pay-to-PubKeyHash (P2PKH) транзакцию для сети Bitcoin или Ehtereum и транзакцию с целевым адресом, являющимся адресом кошелька.

Если такое ограничение типа транзакций устраивает ОИКВС, то описанной выше схемы достаточно для выполнения поставленной задачи. Однако если в среде ИКВС предусматривается использование транзакций типа Pay-to-ScriptHash (P2SH) для Bitcoin или создание в сети Ethereum смарт-контрактов (в этом случае целевой адрес не указывается) и вызов функций смарт-контрактов (в этом случае целевой адрес транзакции – это адрес контракта), то необходимо расширить понятие ИКВС.

Расширение понятия ИКВС на сценарии и смарт-контракты приводит к тому, что по сути ИКВС становится настоящей замкнутой программной средой, применяемой для защиты информации в универсальных ОС.

В этом случае ОИКВС формирует и делает доступным для участников ИКВС перечень верифицированных и разрешенных к применению в среде смарт-контрактов и сценариев. Разница с классической ЗПС состоит в том, что разрешенные контракты и сценарии могут содержать переменные параметры, которые указываются в запросе на создание конечным пользователем. Такими переменными параметрами являются, например, наборы открытых ключей для операции OP_CHECKMULTISIG.

Конечный пользователь, например, при необходимости создать смарт-контракт, посылает запрос ОКВК с идентификатором разрешенного смарт-контракта с необходимыми параметрами. ОКВК создает соответствующую транзакцию и возвращает конечному пользователя токен адреса контракта. Данный токен, точно так же, как и в случае со стандартным токеном открытого ключа, может быть открытым или зашифрованным. Конечные пользователя, которые хотят работать с данным контрактом, должны обратиться к ОКВК для получения своего токена адреса.

Таким образом, ИКВС предоставляет возможность создать в криптовалютной среде настоящую ЗПС. Это особенно актуально, конечно, для среды Ethereum, в которой язык старт-контрактов Solidity предоставляет невероятно огромные возможности и в случае неправильного использования может привести к проблемам и потерям криптовалютных средств.

- Предложены понятие, универсальная архитектура и протокол работы ИКВС, пригодной как для децентрализованных недоверенных решений, так и для централизованных регулируемых финансовых и регистрационных процедур в рамках национального проекта. Дополнительно проект решает задачу реальной анонимности транзакций.

  Кроме того, в соединении с национальным оператором блокчейна данный проект позволит создать техническую базу проекта Единой платежной системы, в частности для Союзного государства.

Литература

1. *Щербаков А.Ю.* Синтез универсальной архитектуры и протокола криптовалюты в рамках национального проекта // Системы высокой доступности. 2017. Т. 13. № 3. С. 15–18.
2. Централизованные криптовалюты. URL = geektimes.ru/company/waves/blog/289379/.
3. *Black F.* Banking and interest rates in a world without money: the effects of uncontrolled banking // Journal of Bank Research. 1970. № 1(Autumn). P. 9–20.
4. *Fama E.F.* Banking in the theory of finance // Journal of Monetary Economics. 1980. № 6. P. 39–57.
5. *Hall R.E.* Monetary trends in the United States and the United Kingdom: a review from the perspective of new developments in monetary economics // Journal of Economic Literature. 1982. № 20. P. 1552–1556.
6. *Kareken J. and Wallace N.* On the indeterminacy of equilibrium exchange rates // Quarterly Journal of Economics. 1981. № 96(2). P. 207–222.
7. *Meiklejohn S.*, *Pomarole M.*, *Jordan G.*, *Levchenko K.*, *McCoy D.*, *Voelker G.M. and Savage S.* A fistful of Bitcoins: characterizing payments among men with no names // Proc. of the 2013 Conference on Internet Measurement.
8. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org. 2008.
9. *Wallace N.* A legal restrictions theory of the demand for 'money' and the role of monetary policy // Federal Reserve Bank of Minneapolis Quarterly Review. 1983. № 7. P. 1–7.
10. *Russinovich M.* Introducing Azure confidential computing. 2017. URL = https://azure.microsoft.com/ru-ru/blog/introducing-azure-confidential-computing/.

Поступила 7 декабря 2017 г.

Synthesis of universal isolated cryptocurrency network

A.V. Domashev – Head of Department, STC «Atlas»
E-mail: domix@stcnet.ru
A.Yu. Scherbakov – Dr. Sc. (Eng.), Professor, Main Research Scientist,
FRC «Computer Science and Control» RAS (Moscow)
E-mail: x509@ras.ru

The concept of an isolated cryptocurrency network, the principles and approaches to the synthesis of a generic architecture and protocol of the isolated cryptocurrency network are proposed. In addition, the project solves the problem of real anonymity of transactions.

References

1. *Shherbakov A.Yu.* Sintez universal'noj arxitektury' i protokola kriptovalyuty' v ramkax naczional'nogo proekta // Sistemy' vy'sokoj dostupnosti. 2017. T. 13. № 3. S. 15–18.
2. Czentralizovanny'e kriptovalyuty'. URL = geektimes.ru/company/waves/blog/289379/.
3. *Black F.* Banking and interest rates in a world without money: the effects of uncontrolled banking // Journal of Bank Research. 1970. № 1(Autumn). P. 9–20.
4. *Fama E.F.* Banking in the theory of finance // Journal of Monetary Economics. 1980. № 6. P. 39–57.
5. *Hall R.E.* Monetary trends in the United States and the United Kingdom: a review from the perspective of new developments in monetary economics // Journal of Economic Literature. 1982. № 20. P. 1552–1556.
6. *Kareken J. and Wallace N.* On the indeterminacy of equilibrium exchange rates // Quarterly Journal of Economics. 1981. № 96(2). P. 207–222.
7. *Meiklejohn S.*, *Pomarole M.*, *Jordan G.*, *Levchenko K.*, *McCoy D.*, *Voelker G.M. and Savage S.* A fistful of Bitcoins: characterizing payments among men with no names // Proc. of the 2013 Conference on Internet Measurement.
8. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org. 2008.
9. *Wallace N.* A legal restrictions theory of the demand for 'money' and the role of monetary policy // Federal Reserve Bank of Minneapolis Quarterly Review. 1983. № 7. P. 1–7.
10. *Russinovich M.* Introducing Azure confidential computing. 2017. URL = https://azure.microsoft.com/ru-ru/blog/introducing-azure-confidential-computing/.

УДК 007

Способ управления доступом к системе обработки больших данных на основе использования маркера потока в заголовке IP-пакета шестой версии

В.И. Будзко – д.т.н., Академик Академии криптографии РФ, зам. директора по научной работе, Институт проблем информатики ФИЦ ИУ РАН (Москва); профессор, Национальный исследовательский ядерный университет «МИФИ» (Москва)
E-mail: vbudzko@ipiran.ru
Д.А. Мельников – к.т.н., доцент, вед. науч. сотрудник, Институт проблем информатики ФИЦ ИУ РАН (Москва); доцент, Национальный исследовательский ядерный университет «МИФИ» (Москва)
E-mail: DAMelnikov@mephi.ru
В.М. Фомичев – д.ф.-м.н., профессор, вед. науч. сотрудник, Институт проблем информатики ФИЦ ИУ РАН (Москва); профессор, Национальный исследовательский ядерный университет «МИФИ» (Москва); профессор, Финансовый университет при Правительстве Российской Федерации
E-mail: fomichev@nm.ru

Предложен способ повышения уровня защищенности корпоративной базы данных, в основе которого лежит использование поля «Маркер потока» основного IPv6-заголовка для доставки «Маркера безопасности» (МБ). Проведен анализ реализационных аспектов указанного способа, включая некоторые общие правила и алгоритмы обработки МБ и его размещения в поле «Маркер потока» основного IPv6-заголовка. Показано, что основными компонентами, реализующими представленный способ, являются криптографический сетевой экран и локальный криптошлюз, расположенный на противоположных сторонах виртуального соединения.

Ключевые слова: *управление доступом, система обработки «больших данных», сетевой экран, аутентификация, маркер потока, IP-заголовок шестой версии.*

The offered mechanism of Access Control (AC) to Big Data processing system is based on using the IPv6 header Flow Label (FL) field to transfer security token (ST). A 20-bit IPv6 header FL can be used for delivering an additional identification/authentication parameter. Basing on the results of FL processing, a FW decides whether it grants or denies access. In such model of using FW, there arise some problems of implementation, i.e. the provision of information for identification and/or authentication, choice of access scheme and cryptographic functions by the FW itself. A few solutions of such problems are discussed.

Keywords: *access control, Big Data processing system, firewall, authentication, flow label, IPv6 header.*

Системы контроля и управления доступом (СКУД) являются наиболее важным компонентом в системе обеспечения сетевой безопасности. Средства обеспечения неприкосновенности и защищенности могут быть скомпрометированы, прежде всего, вследствие некорректной настройки политик управления доступом (УД), а также из-за сбоев в системе, реализующей криптографические алгоритмы или протоколы. Проблема обеспечения неприкосновенности и защищенности существенно усложняется вследствие того, что возрастает сложность самих комплексов программного обеспечения (КПО). Это убедительно подтверждается на примере систем обработки «больших данных» (СОБД), которые создаются для обработки больших объемов оберегаемых данных и ресурсов, образующих кластер сложной обработки [1, 2]. По существу, УД к СОБД требует взаимодействия сетевых сегментов обработки, которые должны быть защищены как вычислительные среды, состоящие из вычислительных компонентов, находящихся под защитой распределенной СКУД. Таким образом, весьма актуальной для обеспечения эффективного функционирования современных информационно-телекоммуникационных систем (ИТС) является проблема развития и совершенствования методов и программных средств накопления и обработки данных.

К настоящему времени предложено много проектов архитектуры СОБД для решения проблем их обработки. Однако большинство из них предназначалось для реализации базовых характеристик обработки данных, именуемых «VVV» («Velocity», «Volume» и «Variety» – скорость доставки, объем данных и разнообразие форматов). Основное внимание при обеспечении безопасности больших данных (БД), как правило, обращено на решение специфических проблем и исправления КПО [1, 2].

Вместе с тем, включение в некоторые современные системы БД крайне необходимых средств обеспечения безопасности и СКУД (только для авторизации) с целью защиты компонентов системы обработки БД и их пользователей от внутренних атак реализовано далеко не полностью. В [3−5] предложен способ УД общего назначения для распределенных кластеров обработки БД. Указанный способ УД ориентирован на внутреннюю структуру обработки в СОБД, полагая, что все проблемы аутентификации пользователей, запрашивающих доступ к ресурсам такой систем, решены. Он предусматривает только процедуру определения прав доступа (авторизации) к ресурсам и процедурам СОБД.

Ц е л ь р а б о т ы – предложить способ фильтрации трафика сетевым экраном (СЭ, firewall) на основе маркеров потока (МП, flow label), входящих в состав основного заголовка IP-пакета шестой версии [6]. 20-битовый МП может быть использован в качестве средства доставки дополнительного идентификационного параметра, на основании результатов обработки которого СЭ принимает решение о предоставлении или отказе доступа. При такой модели использования СЭ можно надежно решить проблемы аутентификации пользователей СОБД. Кроме того, предложены некоторые варианты решения реализационных проблем.

Общая модель системы обработки «больших данных» на примере комплекса программного обеспечения «Hadoop»

Основополагающая модель большинства существующих структур БД построена на концепции распределенной обработки [1, 3, 5] и включает в себя совокупность общих систем обработки (рис. 1).

1. ***Ведущая система*** (***Master System*** – MS) принимает данные от провайдеров, являющихся источниками БД, и определяет итерации обработки в ответ на запрос пользователя. MS реализует следующие важные функции:

функцию *распределения задачи обработки* (*Task Distribution* – TD) – эта функция отвечает за распределение процессов обработки между подчиненными системами, входящими в СОБД-кластер;

функцию *распределения данных* (*Data distribution* – DD) – эта функция отвечает за распределение данных между подчиненными системами, входящими в СОБД-кластер;

функцию *сбора и обработки результатов* (*Result Collection* – RC) – эта функция отвечает за обработку, отбор и анализ информации, предоставленной подчиненными системами, входящими в БД-кластер, а также за формирование суммарных результатов для пользователей.

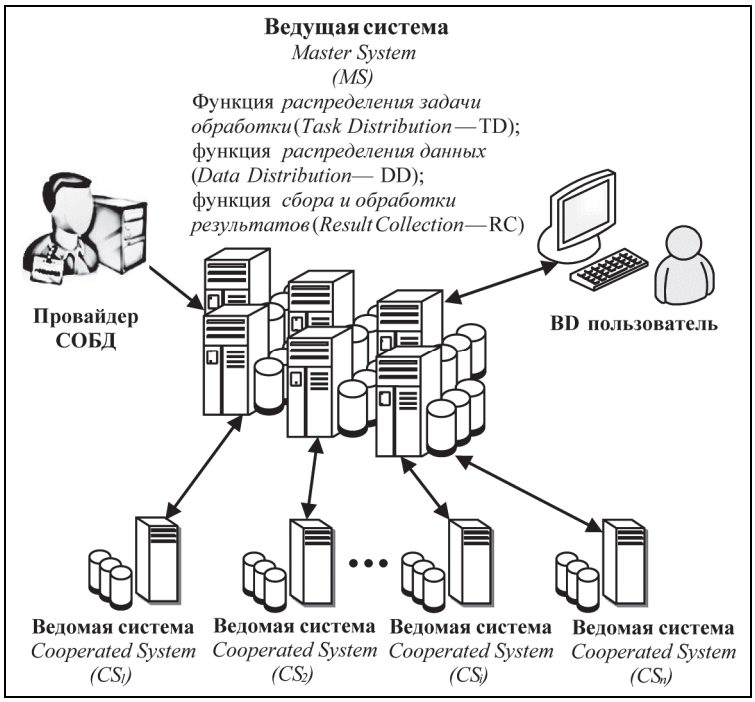


Рис. 1. Общая модель СОБД

Если нет каких-либо ограничений со стороны специализированных прикладных систем, то, как правило, указанные функции встраиваются и обслуживаются в одной и той же главной вычислительной машине (host machine) с целью упрощенной и безопасной настройки и эксплуатации.

2. ***Ведомая система*** (***Cooperated System*** – CS) назначается MS и является доверенной по отношению к MS при обработке БД. CS отчитывается за реализацию или сообщает о проблемах реализации функций TD и DD. В противном случае, CS направляет ответ с полученными результатами MS в рамках реализации функции RC.

На рис. 2 представлена общая распределенная архитектура СОБД на примере КПО с открытым исходным кодом «Hadoop» [5] американской благотворительной организации «Apache Software Foundation» (ASF), который используется во всем индустриальном секторе и прави-

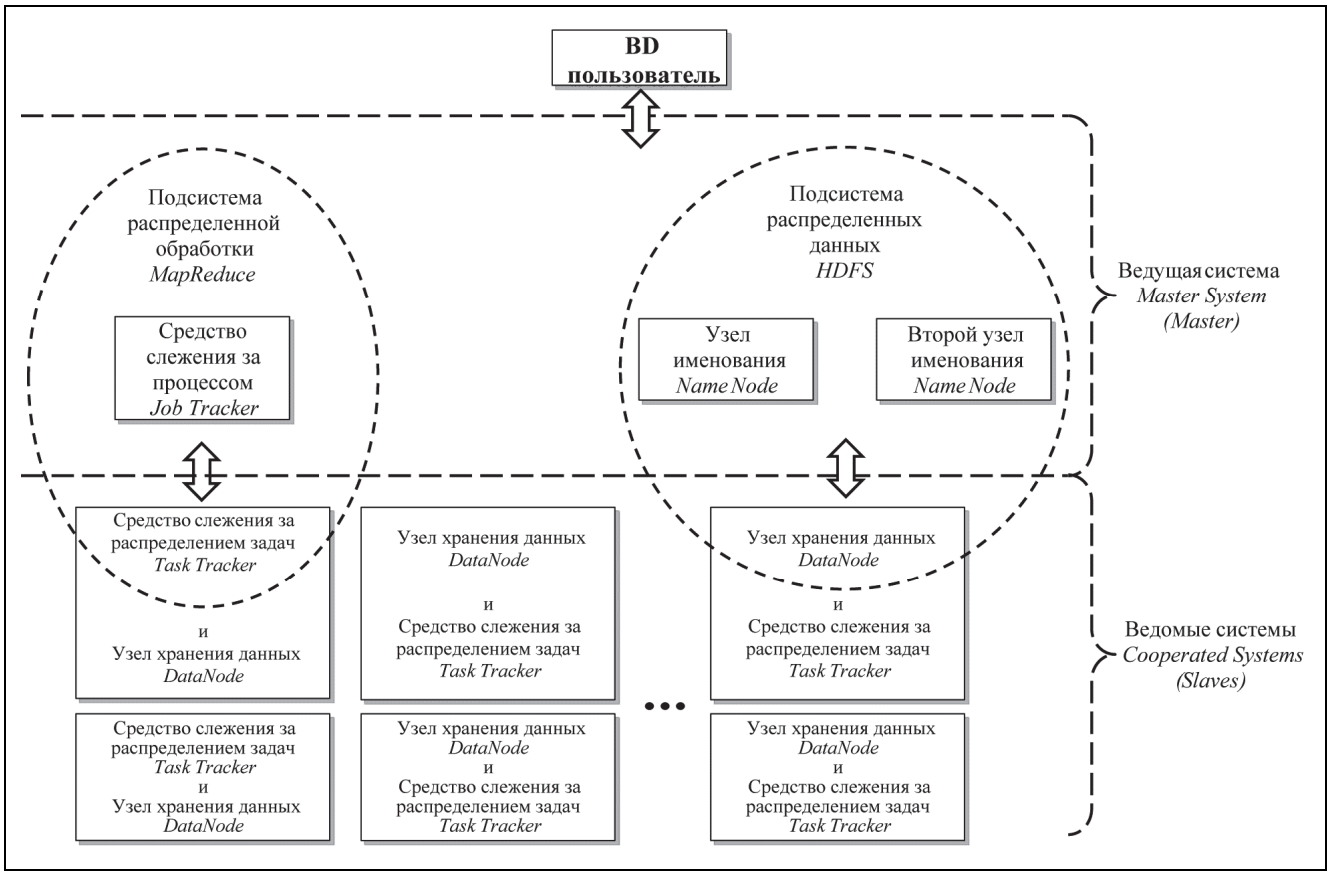


Рис. 2. Общая распределенная архитектура СОБД на основе КПО «Hadoop»

тельстве США. КПО Hadoop хранит данные и обрабатывает ресурсы, расположенные в непосредственной близости внутри кластера. Он функционирует на основе распределенной модели, состоящей из множества компьютеров (например, компьютеров с простой архитектурой и ОС Linux), в которой представлены два основных MS-компонента, TD – MapReduce и DD – File System (HDFS, Hadoop file system – файловая система), и совокупность программных средств. TD обеспечивает распределенную обработку данных по всему кластеру, а DD распределяет большие группы данных по всем серверам в кластере. CS КПО Hadoop называются «ведомыми» (*slaves*) и каждый включает в себя два компонента: средство слежения за распределением задач (*task tracker*) и узел хранения данных (*data node*). MS включает в себя два дополнительных компонента: средство слежения за процессом (*job tracker*) и узел именования (*name node*). Средства *job tracker* и *task tracker* сгруппированы в комплекс распределенной обработки MapReduce, средства *name node* и *data node* попали в комплекс распределенных данных HDFS.

КПО Hadoop сочетает в себе хранилище, серверы и сети, что позволяет ему делить данные на короткие последовательности, а также проводить обработку небольших совокупностей данных. Для каждой небольшой совокупности данных назначается процедура обработки, и поэтому вместо обработки одной большой совокупности данных проводится обработка множества мелких «порций» данных, которые требуют гораздо меньших временных затрат. После этого результаты агрегируются и отправляются обратно в прикладной процесс. Итак, КПО Hadoop обеспечивает линейную масштабируемость, используя для этого столько компьютеров, сколько необходимо. Внутри кластера между MS и CS обеспечивается связь, которая делает обычные системы обслуживания данных неспособными для обработки.

Способ авторизации в системе обработки «больших данных»

На рис. 3 представлена предложенная в [3, 4] схема (способ) УД, основанная на общей СОБД-модели, описанной в предыдущем разделе. Эта схема включает в себя компоненты УД с целью удовлетворения требований СОБД к СКУД. К таким компонентам относятся:

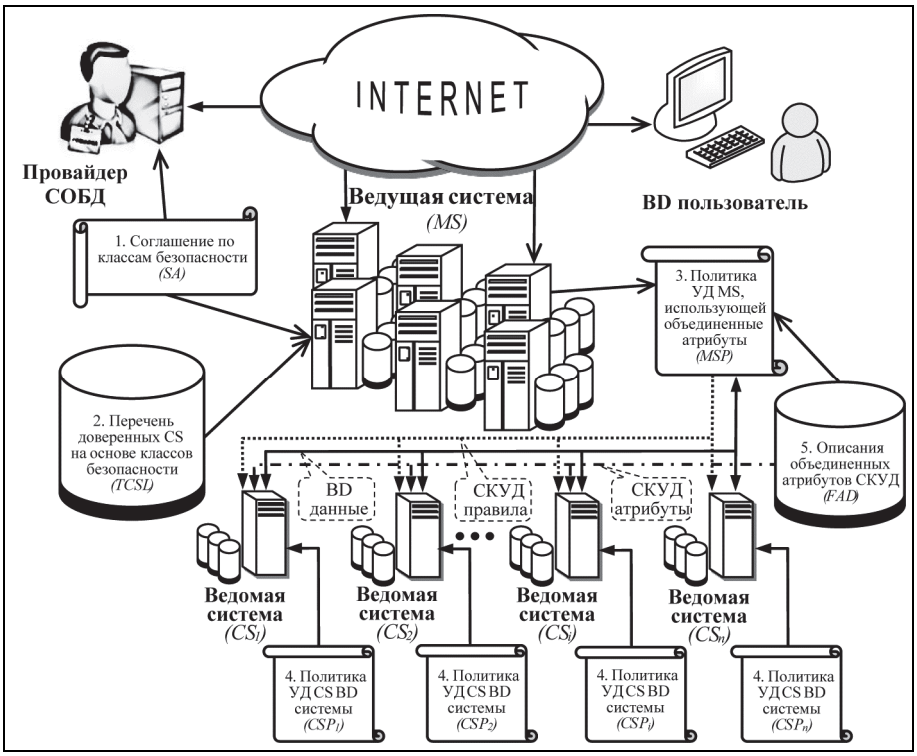


Рис. 3. Схема способа авторизации в СОБД

1. *Соглашение о безопасности* (*security agreement* – SA) – представляет собой обоюдное согласие поставщика данных в СОБД и MS с целью определения классов безопасности источников данных для СОБД. Назначение SA заключается в том, чтобы поставщики данных в СОБД и MS совместно согласовывали классы безопасности (степени защищенности) и чтобы в дальнейшем MS и CS использовали эти классы для определения уровней защищенности (или доверия) с целью определения CS, которые имели бы право на обработку соответствующих данных.

2. *Перечень доверенных* (*надежных*) *CS* (*trust CS list* – TCSL) – представляет собой список надежных CS, признанных MS. TCSL классифицирует CS по классам безопасности в соответствии с соглашениями о безопасности (SA), заключенными с поставщиками данных в СОБД. TCSL обслуживается сотрудником по безопасности MS, который основывается на собственных знаниях о присоединенных CS.

3. *Политика УД MS* (*MS AC Policy* – MSP) – обслуживается сотрудником по безопасности MS. MSP устанавливает совокупность правил УД, которые MS «принудительно навязывает» CS с целью реализации последней политики УД.

4. *Политика УД CS* (*CS AC Policy* – CSP) – обслуживается сотрудником по безопасности CS. CSP позволяет CS контролировать доступ к распределенным СОБД данным/процессам с учетом возможностей подсистемы обработки (например, загрузки системы) и требований CS по обеспечению безопасности. CSP необходима также для разрешения конфликтной ситуации, когда правила УД других локальных CS противоречат CSP-правилам.

5. *Описания объединенных атрибутов* (*Federated Attribute Definitions* – FAD) – представляют собой перечень общих атрибутов, используемых MS и CS, причем такой, что сами MSP и CSP могут быть сформированы на основе использования общих атрибутов из FAD-словаря. FAD служит объединенным словарем УД-атрибутов, которые должны быть согласованы с точки зрения их синтаксиса и семантики с MS и CS. В основе рассмотренного способа УД лежит атрибутная модель (attribute-based access control) [4].

Преодолимость сетевых экранов

Одним из основных способов парирования атак, направленных на проникновение к корпоративным ресурсам, входящим в СОБД, является применение СЭ. СЭ представляет собой «заградительную» систему обеспечения информационной безопасности (ИБ), которая реализует корпоративную стратегию УД между отдельными компьютерами и сетями, либо между двумя или более сетями (рис. 4). В широком смысле СЭ представим как пара средств, одно из которых предназначено для блокировки трафика, а второе – для пропуска разрешенного трафика[1].

[1] *Блокирующие* СЭ функционируют по принципу «блокировать только тот трафик, признаки которого указаны». А *разрешающие* СЭ функционируют по принципу «пропускать через себя только тот трафик, признаки которого указаны».

Главное предназначение СЭ – защита корпоративного сетевого сегмента, принадлежащего какой-либо организации независимо от формы собственности, от несанкционированного доступа (НСД) со стороны «внешнего мира» путем нейтрализации вредоносного трафика на основе результатов анализа адресной информации транслируемых сообщений, а также других параметров, входящих в признаковое пространство для распознавания трафика.

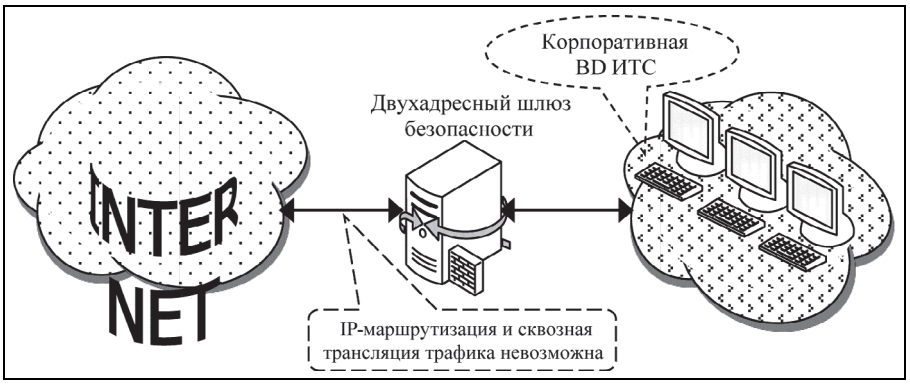


Рис. 4. Схема гибридного СЭ на основе двухадресного шлюза безопасности

С функциональной точки зрения СЭ полностью соответствует классификатору в модели системы распознавания образов. Итак, СЭ реализует функцию обнаружения, то есть «свой» или «чужой». Если он устанавливает, что IP-пакет «чужой», то последний просто уничтожается, а если «свой», то определяет его дальнейшую обработку.

На вопрос о преодолимости СЭ ответ положительный. Во-первых, сами разработчики СЭ-систем и специалисты в области ИБ говорят о возможности нелегального проникновения через такие системы. Другими словами, СЭ-системы «не всесильны» и способны защитить БД ИТС только от некоторых разновидностей атак.

Во-вторых (это «второе» объясняет «слабость» СЭ-систем по обеспечению ИБ), эти средства защиты не нарушают «прозрачность» соединения между прикладными процессами, которое идентифицируется с помощью адресной системы той или иной прикладной службы. Именно наличие прикладных адресов процесса-получателя и процесса-отправителя в транслируемом сообщении позволяет однозначно (при отсутствии ошибок) идентифицировать соединение (цель атаки) даже в условиях применения трансляторов сетевых адресов и номеров транспортных портов. Отсюда следует, что основой атак на СЭ-системы является обеспечение доступа к трафику, транслируемому через эти средства защиты. И поэтому признак классификации пакетов на «свои» и «чужие» должен быть уникальным и надежным. Такой признак должен быть неповторяемым, нерегенерируемым и случайным.

Маркер потока в заголовке IP-пакета шестой версии

На рис. 5 представлен формат заголовка IP-пакета шестой версии (IPv6-заголовок). 20-битовое поле «Маркер потока» IPv6-заголовка используется сетевым IPv6-узлом для маркирования пакетов в потоке. В данном случае под потоком понимается последовательность IP-пакетов (далее – пакет), которые были переданы соответствующим узлом/отправителем соответствующему узлу/получателю. Вообще одновременно может существовать несколько потоков пакетов от отправителя к получателю, а также иной трафик, который не связан с каким-либо потоком. Поток однозначно идентифицируется парой значений, а именно адресом отправителя пакета и ненулевым МП. Пакеты, которые не принадлежат какому-либо потоку, содержат нулевое значение в поле «Маркер потока».

Тем не менее, программно-аппаратные комплексы (ПАК) классификации пакетов (с целью определения их принадлежности к некоторому потоку) могут использовать составной вектор, включающий поля «Адрес получателя», «Номер порта отправителя» и «Номер порта получателя» помимо полей «Маркер потока» и «Адрес отправителя».

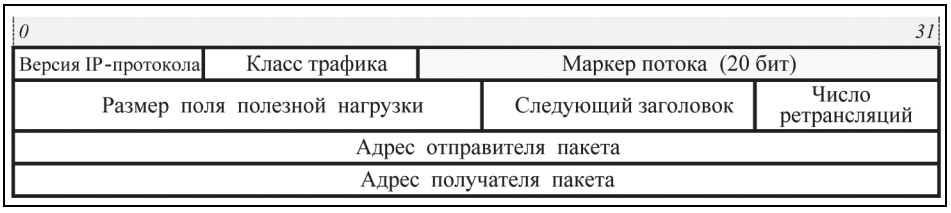


Рис. 5. Формат заголовка IPv6-пакета

Целесообразно выбирать значения МП уникальными, что достигается, например, при использовании хэш-функции, вычисляемой по последователь-

ности, которая содержит составной вектор. Промежуточные узлы не должны «догадываться» о способе формирования МП. С другой стороны, если МП содержит нулевое значение, то он должен быть доставлен в сетевой узел назначения без каких-либо изменений. Промежуточный узел обязан либо отставить МП с ненулевым значением без изменений, либо изменить его, исходя из соображений безопасности. Очевидно, что не существует способа проверки, был ли МП модифицирован, а если был, то на каком ретрансляционном участке.

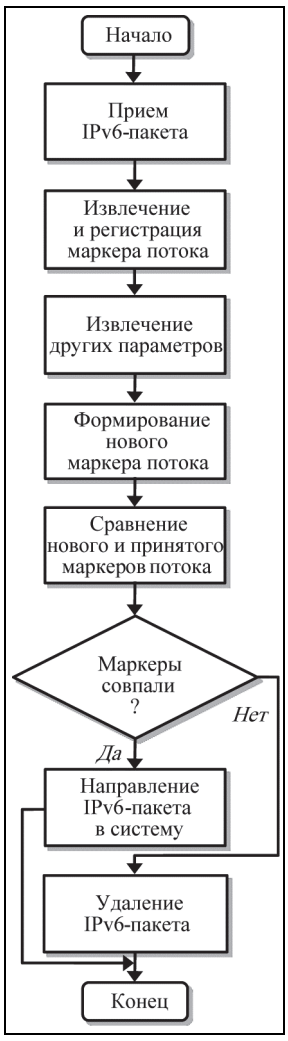


Рис. 6. Схема алгоритма проверки МП

Способ фильтрации трафика на основе маркера потока в системах управления доступом

Суть предлагаемого способа заключается в следующем [6]. СЭ корпоративной сети анализирует трафик по принципу «пропускать через себя только тот трафик, признаки которого указаны». В качестве параметра, по которому принимается решение о предоставлении или не предоставлении доступа, выступает МП. В 20-битовом поле «Маркер потока» IPv6-заголовка помещается маркер безопасности (МБ), который представляет собой результат вычисления однонаправленной функции по последовательности символов, структура которой зависит от схемы УД и криптографического преобразования, а также используемых дополнительных информационных элементов (атрибутов). При формировании запроса доступа инициатор «помещает» в поле «Маркер потока» IPv6-заголовка соответствующим образом сформированный МБ, предусматривающий собственную защиту от атак типа «маскарад» и/или «повторная передача». Другими словами, инициатор должен иметь дополнительный внутренний или внешний программный или программно-аппаратный модуль формирования МБ и размещения его в поле «Маркер потока» IPv6-заголовка.

После получения запроса доступа СЭ выполняет аналогичные действия по формированию МБ, расположенного в поле «Маркер потока» IPv6-заголовка принятого пакета. Далее он сравнивает вновь сформированный и полученный МБ, и если маркеры совпали, то принимается решение о предоставлении доступа, СЭ пропускает запрос далее в систему УД. Алгоритм проверки МП представлен на рис. 6. Последующая обработка зависит от схемы УД и «эшелонированности» системы обеспечения ИБ корпоративной сети. Функциональная блок-схема взаимодействия инициатора и СЭ представлена на рис. 7.

Многим инициаторам может понадобиться прохождение процедуры аутентификации перед тем, как им будет дозволено получение вспомогательной информации (ВИ) для контроля доступа. Эта ВИ (включенная в МБ) обеспечит доступ к ресурсам, которые являются субъектом политики УД. Соответственно служба аутентификации может предоставить результаты процедуры аутентификации службе УД для использования последней. Аннулирование аутентификационной ВИ может привести к прекращению существующего доступа.

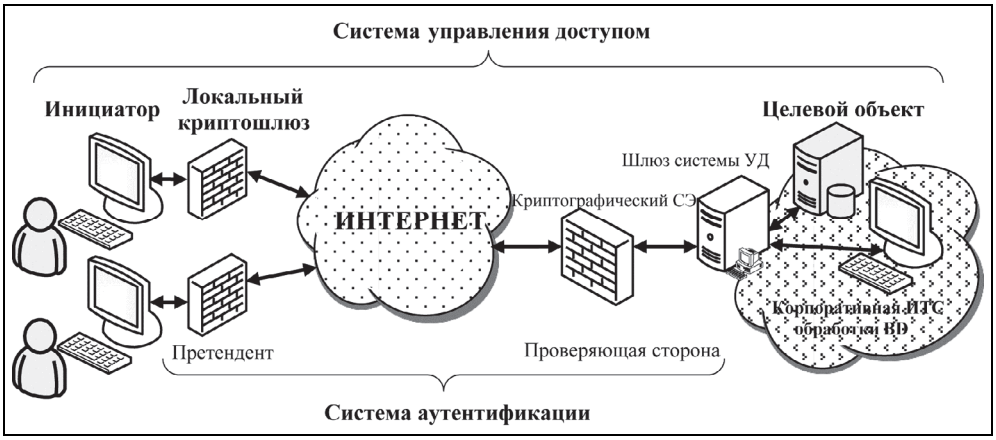


Рис. 7. Схема взаимодействия инициатора и СЭ

С точки зрения службы аутентификации СЭ выступает в роли проверяющей стороны (*verifier*), а инициатор – в роли претендента (*claimant*).

Параметром подлинности в этом случае является МБ, размещенный в поле «Маркер потока» IPv6-заголовка. Если МБ формируется с использованием криптографических функций, то и СЭ как проверяющая сторона осуществляет необходимые криптографические преобразования. То есть речь уже идет о «криптографическом» СЭ (*cryptofirewall*[2]).

Реализационные аспекты

В целях достижения максимального уровня защищенности корпоративной БД ИТС предлагаемый способ должен быть реализован с соблюдением определенных правил, которые затрагивают следующие проблемы.

Внутреннее или внешнее размещение модуля формирования и вставки МБ в IPv6-заголовок и СЭ, который принимает IPv6-заголовки и проверяет значение МБ. Программный или программно-аппаратный модуль формирования МБ и вставки его в поле «Маркер потока» IPv6-заголовка, а также СЭ на стороне целевого объекта могут быть размещены либо в составе персонального компьютера инициатора и шлюза системы УД соответственно, либо автономно. Внутреннее расположение модуля формирования МБ и СЭ с практической точки зрения почти не реализуемо. Это связано с корректировкой операционной системы (ОС), используемой в персональном компьютере инициатора и шлюзе системы УД. На сегодняшний день в условиях использования коммерческих ОС весьма трудно убедить их разработчиков в необходимости внесения дополнительных изменений, связанных с формированием и проверкой МБ, а также его вставкой в IPv6-заголовок.

Привлечение доверенной третьей стороны (ДТС, trusted third party) к процедуре аутентификации инициатора, выступающего в роли претендента. Если ДТС привлекается, то какова схема организации информационного взаимодействия между тремя сторонами? Современные стандартные модели электронной аутентификации объектов обязательно включают ДТС [7, 8]. Однако в реальной жизни условия для привлечения ДТС могут быть недостаточными. В самой простой ситуации ни претендент, ни проверяющая сторона не привлекают какую-либо третью сторону для формирования и проведения обмена ВИ и самой процедуры аутентификации. В этом случае проверочная ВИ для взаимодействующей стороны должна быть инсталлирована на проверяющей стороне.

Число итераций в процедуре аутентификации и способы защиты и привязки МБ к IPv6-заголовку. Для того чтобы взаимодействующая сторона могла аутентифицировать противоположную сторону, целесообразно, чтобы обе стороны использовали единый набор криптографических методов, способов и параметров. Стандартные способы аутентификации [7, 8] основаны на как минимум 1-итерационных или 3-итерационных процедурах обмена аутентификационной ВИ. Рассмотрим способы (рис. 8), которые обеспечивают защиту от кражи МБ (вскрытия) и атак типа «повторная передача».

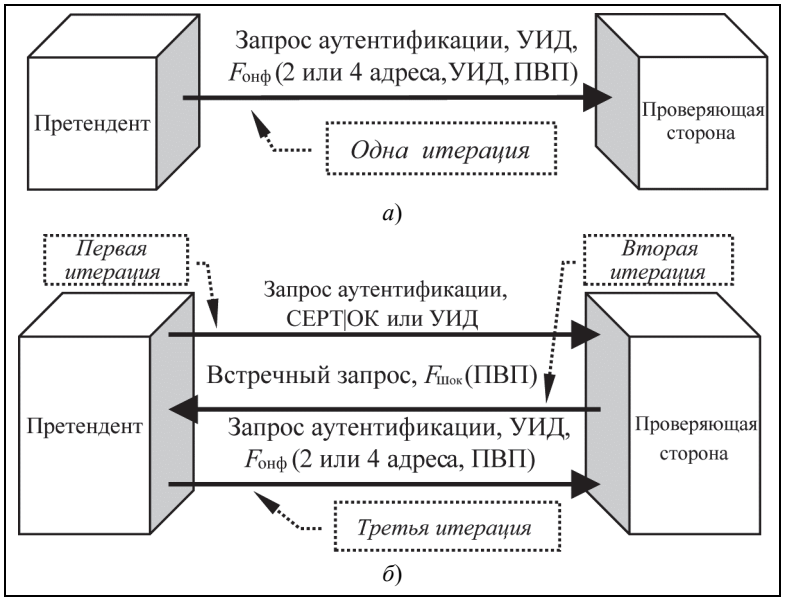


Рис. 8. Схемы 1-итерационной (*а*) и 3-итерационной (*б*) процедуры аутентификации

В обоих способах применяется переменный временной параметр (ПВП, *time variant parameter*), представляющий собой элемент данных, используемый для проверки того, что сообщение (МБ) не было передано повторно, например, случайное число, метка времени или последовательный номер. ПВП используются для контроля уни-

[2] Этот термин является торговой маркой компании «Cryptography Research» (подразделение корпорации «Rambus»). http://www.cryptography.com/technology/cryptofirewall.html.

кальности (*uniqueness*) и своевременности (*timeliness*) сообщений, которыми обмениваются взаимодействующие стороны в процедуре аутентификации. Также в этих способах используется однонаправленная функция для формирования МБ, который размещается в поле «Маркер потока» IPv6-заголовка. Необходимость трех итераций во втором способе аутентификации (рис. 8,*б*) обусловлена тем, что инициатор (претендент) не знает или не имеет возможности сформировать ПВП.

Проверяющая сторона, сформировавшая уникальный ПВП, использует открытый ключ претендента (инициатора) для зашифрования встречного запроса и своего ПВП, передаваемых во второй итерации (рис. 8,*б*). В случае если проверяющая сторона обладает сертификатом открытого ключа (СЕРТ|ОК) претендента (инициатора), то последний может в запросе аутентификации передать свой уникальный идентификатор (УИД, например, последовательный номер того же СЕРТ|ОК). Если закрытый ключ претендента (инициатора) не скомпрометирован, то только он сможет расшифровать встречный запрос с ПВП, переданный проверяющей стороной [8].

Способы формирования, хранения и распространения ПВП для защиты МБ.

Метки времени [7, 8]. Способы, предусматривающие использование меток времени, основаны на применении общего источника сигналов эталонного времени, с которым претендент и проверяющая сторона установили и поддерживают виртуальные соединения. В качестве эталонного времени рекомендуется использовать «скоординированное универсальное время» (*coordinated universal time*). Проверяющая сторона устанавливает приемлемую фиксированную длину «временного окна», с помощью которого она контролирует *своевременность* путем вычисления разницы между меткой времени, указанной в принятом и проверенном МБ, и временем, которое воспринимается проверяющей стороной как момент времени получения МБ. Если разница во времени «укладывается» во временное окно, то сообщение воспринимается как корректное. *Уникальность* может быть проверена путем регистрации и записи всех сообщений, полученных в пределах текущего временного окна, и последующего удаления (многократно) повторяющихся идентичных сообщений, также обнаруженных в пределах этого окна. Целесообразно, чтобы часы претендента и проверяющей стороны были синхронизированы достаточно точно, что существенно снижает вероятность обмана на основе атаки типа «повторная передача». Также целесообразно гарантировать, что вся информация, относящаяся к проверке меток времени, и, соответственно, к часам, к которым подсоединены взаимодействующие стороны, защищена от фальсификации. Способы, использующие метки времени, позволяют обнаруживать «вынужденные задержки» (*forced delays*), то есть задержки, вносимые противоправными действиями нарушителя в какой-либо промежуточной точке логического соединения.

Последовательные номера. Уникальность может контролироваться путем использования последовательных номеров, так как они позволяют проверяющей стороне обнаруживать повторно переданные сообщения. Претендент и проверяющая сторона заранее договариваются о политике нумерации сообщений, включая соответствующий способ нумерации. Основная идея заключается в следующем: сообщение с соответствующим номером будет восприниматься как корректное только один раз (или только однажды в течение определенного периода времени). Сообщения, принятые проверяющей стороной, в дальнейшем проверяются на предмет корректности номера в МБ в соответствии с согласованной политикой. Если же такой номер не является корректным, то сообщение удаляется. Использование последовательных номеров может потребовать от претендента и проверяющей стороны ведение дополнительной «бухгалтерии» (*book keeping*), то есть может понадобиться ведение записей о последовательных номерах, которые использовались ранее и/или которые остались действительными для дальнейшего применения.

Случайные числа. Случайные числа используются для предотвращения атак типа «повторная передача» или «чередование» (*interleaving attack*). Поэтому требуется, чтобы все случайные числа выбирались из достаточно широкого диапазона, чтобы при использовании одного и того же криптоключа вероятность их повторения была ничтожно мала и чтобы вероятность подбора некоторого числа третьей стороной (нарушителем) также была ничтожно мала. Для парирования атак типа «повторная передача» или «чередование» проверяющая сторона формирует (или получает) случайный номер, который она передает претенденту, а затем претендент отвечает путем отправки МБ, содержащего случайный номер в своей защищенной части (рис. 8,*б*). Данная процедура предусматривает обмен двумя сообщениями, содержа-

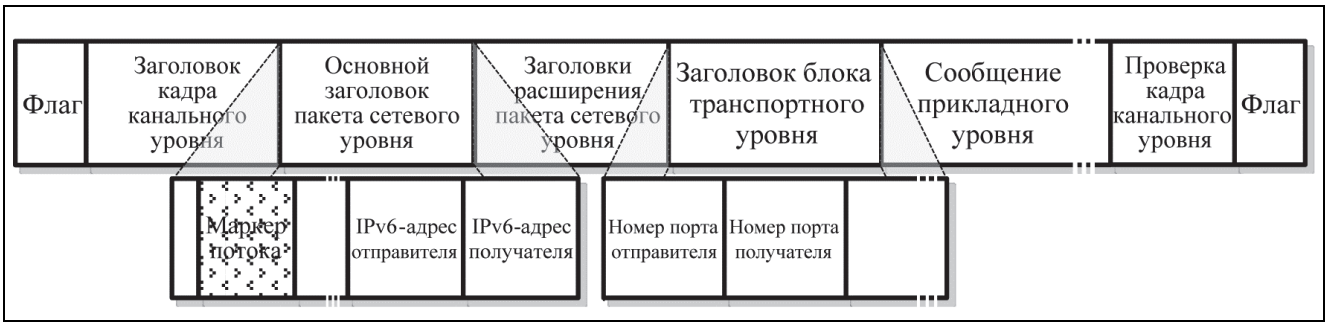


Рис. 9. Структура кадра канального уровня, поступившего на вход локального криптошлюза со стороны персонального компьютера инициатора запроса доступа

щими соответствующее случайное число. Основой парирования таких атак является строгое выполнение следующего требования: вероятность повторяемости случайного числа должна быть ничтожно мала.

Процедура вставки МБ в поле «Маркер потока» IPv6-заголовка, реализуемая локальным криптошлюзом (рис. 7), который расположен на стороне инициатора (претендента). Рассмотрим процедуру вставки МБ в поле «Маркер потока» основного IPv6-заголовка. С выхода сетевого адаптера персонального компьютера инициатора запроса доступа на вход локального криптошлюза поступает кадр канального уровня, формат которого определяется стандартом локальной вычислительной сети, в которой расположен компьютер инициатора. Общая структура такого кадра канального уровня представлена на рис. 9. В этом кадре поле «Маркер потока» основного IPv6-заголовка заполняется нулями.

Криптошлюз «запоминает» принятый кадр и выделяет в нем IPv6-адреса и номера портов отправителя и получателя. Далее, используя имеющийся у него ПВП, формирует последовательность, состоящую из двух адресов, двух номеров и ПВП (либо из двух адресов и ПВП), и вычисляет однонаправленную функцию, результатом вычисления которой и будет МБ. Далее МБ размещается в поле «Маркер потока» основного IPv6-заголовка и повторно вычисляется проверка целостности кадра канального уровня, а результат проверки вставляется в соответствующее поле.

Вставка МБ не влечет никаких изменений в форматах сетевого и канального уровней. Передаваемое прикладное сообщение, заголовок транспортного уровня, заголовки расширения IPv6-пакета, заголовок кадра канального уровня, а также все поля основного IPv6-заголовка за исключением поля «Маркер потока» остаются без изменений. Вновь вычисленная проверка целостности кадра защищает МБ от модификации.

Если же нарушитель все-таки попытается подменить МБ и пересчитать проверку кадра, то наличие ПВП позволит обнаружить подмену (модификацию). На стороне проверяющей стороны криптографический СЭ принимает кадр, проводит проверку МБ и в случае положительного результата проверки изымает МБ из поля «Маркер потока», после чего вновь пересчитывает проверку целостности кадра канального уровня и результат проверки помещает в соответствующее поле. Затем СЭ передает «очищенный» от МБ кадр в систему УД корпоративной сети для принятия окончательного решения о предоставлении доступа.

Если СЭ перешел в режим остановки и последующего рестарта (например, в результате сбоя в работе), он должен быть «внимательным», чтобы не использовать ранее назначенный МБ, время существования которого еще не закончилось. Для этого необходимо использовать процедуру записи МБ в ПЗУ, которое должно быть устойчивым при возникновении нештатных ситуаций.

- Предложен способ повышения уровня защищенности корпоративной базы данных ИТС от НСД. В основе способа лежит использование поле «Маркер потока» основного IPv6-заголовка с целью доставки МБ. Проведен анализ реализационных аспектов указанного способа, включая некоторые общие правила и алгоритмы обработки МБ и его размещения в поле «Маркер потока» основного IPv6-заголовка. Основными компонентами, реализующими представленный способ, являются криптографический СЭ и локальный криптошлюз, расположенный на противоположных сторонах виртуального соединения.

Литература

1. *Hrushikesha Mohanty, Prachet Bhuyan, Deepak Chenthati* Big Data: A Primer. Springer. India. 2015. 185 p.
2. *Sherali Zeadally, Mohamad Badra* Privacy in a Digital. Networked World. Technologies, Implications and Solutions. Springer. Switzerland. 2015. 418 p.
3. *Vincent C. Hu, Tim Grance, David F. Ferraiolo, D. Rick Kuhn* An Access Control scheme for Big Data processing // The Proc. of 10th IEEE/EAI International Conference on Collaborative Computing: Networking, Applications and Worksharing (IEEE/EAI CollaborateCom 2014) in Miami, Florida. 22–25 Oct. 2014. P. 1–7.
4. *NIST* Attribute Based Access Control Definition and Consideration. Special Publication 800-162. Jan. 2013.
5. *Smith K.T.* Big Data Security: The Evolution of Hadoop's Security Model. InfoQ. Aug. 2014. URL = http://www.infoq.com/articles/HadoopSecurityModel.
6. *Melnikov D.A., Gorbatov V.S., Durakovskiy A.P., Lavrukhin Y.N., Petrov V.R.* Access Control Mechanism Based On Entity Authentication With IPv6 Header «Flow Label» Field // The Proc. of the 3rd International Conference on Future Internet of Things and Cloud (FiCloud 2015). 2015. P. 158–164.
7. *Фомичев В.М.*, *Мельников Д.А.* Криптографические методы защиты информации: Учебник (в 2-х частях). М.: Юрайт. 2016.
8. *Мельников Д.А.* Информационная безопасность открытых систем: Учебник. М.: ФЛИНТА. Наука. 2013. 448 с.

Поступила 7 декабря 2017 г.

The mechanism of access control to big data processing system based on using the IPv6 header «flow label» field

V.I. Budzko – Dr. Sc. (Eng.), Member of Russian Cryptography Academy, Deputy Director on Research and Development, Institute of Informatics Problems of FRC CSC RAS (Moscow); Professor, National Research Nuclear University «MEPhI» (Moscow)
E-mail: vbudzko@ipiran.ru
D.A. Melnikov – Ph. D. (Eng.), Associate Professor, Leading Research Scientist, Institute of Informatics Problems of FRC CSC RAS (Moscow); Associate Professor, National Research Nuclear University «MEPhI» (Moscow)
E-mail: DAMelnikov@mephi.ru
V.M. Fomichev – Dr. Sc. (Phys.-Math.), Professor, Leading Research Scientist, Institute of Informatics Problems of FRC CSC RAS (Moscow); Professor, National Research Nuclear University «MEPhI» (Moscow);
Professor, Financial University under the Government of the Russian Federation
E-mail: fomichev@nm.ru

Access Control (AC) systems are among the most critical of network security components. It is more likely that privacy or security will be compromised due to the misconfiguration of access control policies than from a failure of a cryptographic primitive or protocol. This problem becomes increasingly severe as software systems become more and more complex such as Dig Data (BD) processing systems, which are deployed to manage a large amount of sensitive information and resources organized into a sophisticated BD processing cluster. Basically, BD AC systems require collaboration among corporate processing domains as protected computing environments, which consist of computing units under distributed AC management.
The offered mechanism of AC to BD processing system is based on using the IPv6 header Flow Label (FL) field to transfer security token (ST). Also consider are implementation aspects, including some general rules and algorithms of ST processing and their encapsulating in the IPv6 header FL field. The principal components of the mechanism under discussion include cryptofirewall and a local cryptographic gateway on opposite ends of the virtual connection.

References

1. *Hrushikesha Mohanty, Prachet Bhuyan, Deepak Chenthati* Big Data: A Primer. Springer. India. 2015. 185 p.
2. *Sherali Zeadally, Mohamad Badra* Privacy in a Digital. Networked World. Technologies, Implications and Solutions. Springer. Switzerland. 2015. 418 p.
3. *Vincent C. Hu, Tim Grance, David F. Ferraiolo, D. Rick Kuhn* An Access Control scheme for Big Data processing // The Proc. of 10th IEEE/EAI International Conference on Collaborative Computing: Networking, Applications and Worksharing (IEEE/EAI CollaborateCom 2014) in Miami, Florida. 22–25 Oct. 2014. P. 1–7.
4. *NIST* Attribute Based Access Control Definition and Consideration. Special Publication 800-162. Jan. 2013.
5. *Smith K.T.* Big Data Security: The Evolution of Hadoop's Security Model. InfoQ. Aug. 2014. URL = http://www.infoq.com/articles/HadoopSecurityModel.
6. *Melnikov D.A., Gorbatov V.S., Durakovskiy A.P., Lavrukhin Y.N., Petrov V.R.* Access Control Mechanism Based On Entity Authentication With IPv6 Header «Flow Label» Field // The Proc. of the 3rd International Conference on Future Internet of Things and Cloud (FiCloud 2015). 2015. P. 158–164.
7. *Fomichev V.M., Mel'nikov D.A.* Kriptograficheskie metody zaschity informatsii: Uchebnik (v 2-kh chastyakh). M.: Yurait. 2016.
8. *Mel'nikov D.A.* Informatsionnaya bezopasnost' otkrytykh sistem: Uchebnik. M.: FLINTA. Nauka. 2013. 448 s.

УДК 681.3

Проблемы использования оптической и радиолокационной информации (ОРИ), интегрированной в ХОРИАЗ, и пути их решения

В.И. Будзко – д.т.н., Академик Академии криптографии РФ, зам. директора по научной работе, Институт проблем информатики ФИЦ ИУ РАН (Москва)
E-mail: vbudzko@ipiran.ru
В.Г. Беленков – к.т.н., вед. науч. сотрудник, Институт проблем информатики ФИЦ ИУ РАН (Москва)
E-mail: vbelenkov@ipiran.ru
Н.Н. Сметанин – к.т.н., ген. директор, ООО «Паллада» (Москва)
E-mail: snn@geopallada.ru
М.В. Улитенков – зам. ген. директора, ООО «Паллада» (Москва)
E-mail: umv@geopallada.ru
А.А. Зеленикин – начальник отдела, «СКЦ Росморречфлота»
E-mail: aaz61@mail.ru

Рассмотрены проблемы использования оптической и радиолокационной информации (ОРИ), которая интегрирована в единое хранилище оптической и радиолокационной информации по Арктической зоне (ХОРИАЗ), а также пути их решения.

Ключевые слова: *хранилище, оптическая и радиолокационная информация, проблемы, пути решения.*

The article is devoted to problems of using optical and radar information (ORI) that is integrated into a optical and radar information Storage for the Arctic zone («ORISAZ»). The problems are discussed in conjunction with ways to address them.

Keywords: *data storage, optical and radar information, problems, solutions.*

В предыдущих статьях, подготовленных по теме № 15-29-06997, были определены пути решения проблем идентификации и сопоставления оптической и радиолокационной информации (ОРИ) и формирования хранилища ОРИ по Арктической зоне (ХОРИАЗ) [1−4], интеграции в ХОРИАЗ актуальной и ретроспективной ОРИ по объектам поиска/наблюдения Арктической зоны (АЗ), данных по месту/району/региону их нахождения и дополняющих их данных различной достоверности, актуальности и полноты, полученных из различных источников, а также данных цифровых моделей местности по районам АЗ. Были рассмотрены вопросы реализации языка изображений, позволяющего проводить описание объектов, для которых требуются в процессе загрузки ОРИ в ХОРИАЗ идентификация, сопоставление и отождествление [3], а также языка описания изображений (ЯОИ) [5], который может быть использован в более общем языке при задании условий выделения объектов при интеграции данных в ХОРИАЗ, при формировании витрин данных, а также при реализации аналитических OLAP, Data Mining подсистем и приложений.

Ц е л ь р а б о т ы – рассмотреть подход к решению проблем использования ОРИ, сохраняемой в ХОРИАЗ, для решения задач ретроспективного анализа и прогнозирования перемещения и изменения объектов поиска/наблюдения.

Задачи использования ОРИ, интегрированной в ХОРИАЗ

В предыдущих статьях [1−6] рассматривались проблемы использования ОРИ, интегрированной в ХОРИАЗ, и способы их решения, включая ретроспективный анализ и прогнозирование перемещения и изменения объектов поиска/наблюдения. Дадим им краткое описание.

Ретроспективный анализ – получение сведений об объектах поиска/наблюдения, находящихся в АЗ, за прошедшие периоды времени. Такой анализ позволяет выявить все изменения этих объектов поиска/наблюдения в качественном и количественном аспекте за определенные временные срезы, которые могут быть установлены в зависимости от тематики исследования. Ретроспективный анализ применяется при изучении по данным поиска/мониторинга текущего состояния площадных объектов, перемещения по территории объектов поиска/наблюдения для оценки динамики развития ситуации. Ретроспективный анализ любых процессов в АЗ, мониторинг которых осуществляется с использованием ОРИ, в

полном объеме может быть проведен с применением ХОРИАЗ за счет использования сохраняемых в нем поколений данных, а также описаний изменений этих данных. Ретроспективный анализ в АЗ применяют для решения следующих основных задач:

анализа изменения состояния площадных объектов, в том числе участков и территорий, акваторий и т.п., их пригодности для проведения мероприятий, работ, для использования по какому-либо назначению;

определения динамики и прогнозирования их изменения;

анализа перемещения по территории, акватории и т.п. объектов поиска/наблюдения;

определения динамики и прогнозирования их перемещения;

прогнозирования их возможного положения или места положения.

Ретроспективный анализ и прогнозирование изменения объектов наблюдения. При решении ряда задач поиска/наблюдения проведение ретроспективного анализа данных о площадных объектах, в том числе об участках и территориях АЗ, на базе обработки имеющихся данных ОРИ, например, результатов спутникового дистанционного исследования/зондирования Земли, является необходимым и безальтернативным путем получения информации об этих площадных объектах по причине отсутствия или неполноты других хранимых в фондах источников данных (статистической отчетности, описаний территорий, архивов проверок). Однако при использовании данных из фондов источников данных возникает проблема фрагментарности сохраняемых в них данных и невозможности собрать данные по полному покрытию территории, изучаемой, например, при проведении поисково-спасательных операций (работ) (ПСР). Как правило, в фондах отсутствуют корректно сравнимые пространственные данные (в том числе карты местности) с необходимой тематической информацией за требуемые для проведения ретроспективного анализа периоды времени. Применение ХОРИАЗ позволит избежать этих проблем и обеспечить специалистам и оперативным службам полное описание площадных объектов, в том числе участков и территорий АЗ, доступными и сопоставимыми данными за требуемые временные срезы.

Результатом работ по ретроспективному анализу является комплект, в том числе картографических материалов, относящихся к различным временным срезам, выполненный по единой методологии с учетом правила преемственности однотипных объектов и процессов. Результатом работ также может являться статистический качественно-количественный анализ динамики изменения объектов интереса.

К особенностям проведения ретроспективного анализа изменения площадных объектов наблюдения следует отнести то, что, как правило, визуализация пространственных представлений местности, в том числе действительного состояния местности, производится с высокими требованиями по разрешению и картографической точности, при этом собственно ретроспективное картографирование на основе выборок ОРИ осуществляется не с такими жесткими требованиями на пространственное разрешение и картографическую точность пространственно-интерпретированных тематических данных.

Виды контроля ситуации (перемещения, изменения объектов поиска/наблюдения). Задачи прогнозирования перемещения и изменения объектов поиска/наблюдения существенным образом связаны с общими процессами наблюдения/ мониторинга за АЗ, который проводится различными ведомствами с использованием многочисленных информационных систем и средств мониторинга/наблюдения и отражается в действующих в них организациях работ[1]. В число таких процессов входят:

1. *Предварительный и выборочный контроль ситуации* (условное название). Этот вид контроля проводится с целью определить фактическую ситуацию, состояние объектов поиска/наблюдения (например, подконтрольных и поднадзорных объектов в случае исполнения контрольно-надзорных функций федеральными органами исполнительной власти); оценить изменение ситуации и тенденции ее изменения; уточнить связи между параметрами, определенными разными методами с использованием различных средств и систем. Данный контроль предполагает проведение анализа общего состояния объектов поиска/наблюдения АЗ на воде и на суше, обеспечивает «реперную» привязку к конкретным условиям. Он осуществляется с комплексным применением разных методов: аэрокосмической и аэрофотосъемки, наземного визуального (например, сбор данных видеокамер и фотоматериалов) и инструментального обследования, расчетных методов. Периодичность данного вида контроля зависит от потребностей деятельности, в интересах которой он проводится, например, она может составлять как один раз в час, так и в год или период года, в несколько лет.

2. *Постоянный контроль ситуации*. Этот вид контроля позволяет выявлять проблемные зоны путем анализа происходящих изменений и отклонений от ожидаемого «поведения» и/или изменения состояния

[1] Общая структура представительной выборки таких систем приведена в [2,4].

и т.п. объектов поиска/наблюдения, от «естественного» протекания процессов и т.п. В его процессе может осуществляться краткосрочное прогнозирование этих изменений и отклонений. Краткосрочное прогнозирование может осуществляться расчетными методами с использованием ранее разработанных краткосрочных моделей. Этот вид контроля осуществляется с использованием сети стационарных наблюдательных пунктов и/или с использованием средств спутникового дистанционного исследования/зондирования Земли.

3. *Внеплановые проверки, разовые обследования* (по мере необходимости). Этот вид контроля осуществляется в зонах проведения ПСР, в проблемных зонах, в опасных очагах/участках и т.п. путем сопоставления текущих данных аэрофотосъемки с ранее накопленными, например, в ХОРИАЗ, данными по объекту интереса и зоне и т.п. Позволяет выполнить оценку сложившейся обстановки. Для проведения подобных оценок в ведомствах и организациях-участниках действуют модели, алгоритмы и регламенты. Этот вид контроля осуществляется с использованием средств аэрофотосъемки высокой разрешающей способности, позволяющих получать параметры, конкретизирующие ситуацию с объектом(ами) поиска/наблюдения. Использование ХОРИАЗ в ходе контроля этого вида создает возможности выявления дополнительных параметров оценки ситуации на основе комплексного использования всей накопленной в ХОРИАЗ информации. Однако пределы этих возможностей в данное время не проработаны и нуждаются в дальнейших исследованиях. Возможным путем решения этой проблемы могла бы быть разработка геоонтологии и классификатора, отражающего предметные области знаний об АЗ, имеющихся в совокупности отечественных и мировых информационных систем. В этом случае имелась бы возможность эффективно предлагать возможные модели оценки ситуаций на основе всей совокупности данных ОРИ, накопленной в ХОРИАЗ по данной зоне проведения ПСР, проблемной зоне, опасному очагу/участку и т.п. В качестве примера (более чем актуального для АЗ) эффективности учета данных совершенно различных областей можно привести влияние данных мониторинга траекторий движения мусора в мировом океане на поиск обломков самолета MH370 [7].

Прогнозирование ситуации (перемещения, изменения объектов поиска/наблюдения). Эта задача решается ведомствами и организациями-участницами проведения ПСР, мониторинга/контроля объектов поиска/наблюдения в зонах проведения ПСР, в проблемных зонах, в опасных очагах/участках и т.п. на основе использования постоянно действующих моделей изменения ситуации в зонах, перемещения объектов и т.п. Решение этой задачи прогнозирования опирается на ОРИ, получаемую в результате рассмотренных процессов контроля, и позволяет использовать ее для выявления участков проведения ПСР, а также проблемных участков, на которых развитие ситуации может потребовать от ведомств и организаций-участников принятия решений. Также оно позволяет реализовывать в них управление в соответствии с риск-ориентированной моделью. Реализация ведомством, организацией-участницей перечисленных видов контроля и прогнозирования позволяет им получать необходимые данные для любого объекта поиска/наблюдения в целом и для его отдельного участка; восстанавливать ряды наблюдений (например, даже при существенной фрагментарности данных наблюдений и измерений, при потере и искажении части данных или пропуске наблюдений, что является характерным именно для АЗ); контролировать все участки зоны и собирать интерпретируемые данные, сопоставимые в пространственно-временном отношении.

К особенностям представления ОРИ и результатов прогнозирования изменения ситуации следует отнести то, что, как правило, они интерпретированы и пространственно связаны с местностью, данные по которой сохраняются в ХОРИАЗ в виде ее цифровой картографической модели. Таким образом, на стадии практической реализации одним из существенных вопросов их использования становится вопрос формирования визуального интерфейса, адекватного решаемым задачам и удобного для применения пользователями. При реализации графического интерфейса в качестве него целесообразным является использование активного картографического фона.

Проблемы использования ОРИ, интегрированной в ХОРИАЗ

Решение приведенных ранее задач предполагает использование инструментов, рассмотренных в [1, 2], применение которых предусматривает решение ряда проблем использования ОРИ, интегрированной в ХОРИАЗ. Рассмотри эти проблемы и пути их решения.

Проблема разработки дополнительных процедур извлечения пространственных знаний об ОРИ по АЗ. Эта проблема порождена необходимостью идентификации и отождествления ОРИ при ин-

теграции в ХОРИАЗ. Традиционные процедуры извлечения данных объектов, содержащихся в изображениях, не всегда позволяют выполнить задачу ввиду искажений и неполноты самого изображения или искажения (частичного разрушения) объекта, зафиксированного на ОРИ, по сравнению с эталонным изображением.

В качестве пути решения этой проблемы в [3] был предложен и рассмотрен язык изображений (картинок), реализующий дополнительные процедуры формирования пространственных знаний.

Проблема достаточной математической формализации правил построения языка изображений (картинок). Эта проблема порождена использованием языка изображений (картинок), реализующего дополнительные процедуры формирования пространственных знаний. Как было показано в [6], понятия, используемые правилами вывода языка изображений (картинок), находятся в соответствии с понятиями, используемыми аппаратом пространственных вероятностных автоматов, позволяющих описывать (моделировать) изображения (картинки), в виде которых представляется ОРИ, поступающая от источников данных АЗ. Вероятностные параметры перехода автомата из состояния в состояние вырабатываются в процессе обучения извлечения образа объекта из накапливаемых данных с использованием обучающей выборки эталонов изображений, а также с учетом возможных искажений изображения. Удобной моделью графа состояний вероятностного автомата как элемента разбора (распознавания, извлечения составных частей объекта) всего изображения является нейронная сеть, коэффициенты которой определяются апостериорными вероятностями процесса обучения при сравнении с эталонами объектов. Доказано, что граф состояний и сеть идентичны.

В связи со сказанным выше в качестве решения этой проблемы представляется целесообразным обеспечить решение задачи представления описания (разбора) ОРИ средствами байесовской нейронной сети, управляющей характеристиками переходов вероятностных автоматов, выражающих правила разбора изображений языка изображений.

Байесовский подход обеспечивает возможность обучения структур управления, построенных на его основе (рассмотрен применительно к построению языка изображений (картинок) в [5]). В то же время марковские процессы, отражающие условия независимого от прошлого будущего при фиксированном настоящем, хорошо описывают ситуации, применимые в языках изображений при описании серий последовательных независимых воздействий на объект (например, разрушаемый), изображения которого при этом зависят только от своего предшествующего состояния.

Проблема управления вероятностными характеристиками переходов состояний вероятностных автоматов. Эта проблема порождена использованием вероятностных автоматов, выражающих правила разбора изображений языка изображений (картинок).

В качестве пути решения этой проблемы представляется целесообразным рассмотреть возможность создания механизма управления вероятностными характеристиками переходов автоматов из состояния в состояние на основе обучающихся нейронных сетей. Такой подход до настоящего времени практически не применялся.

В работе [8] рассмотрена обратная задача – подход к построению нейронной сети на основе двумерных клеточных марковских автоматов. Очевидно, что именно для марковских процессов прямая и обратная задачи идентичны. Таким образом, согласно этому подходу, который является обратной задачей к решаемой в рамках построения языка изображений (картинок), сначала для определения марковской системы вводится функция переходов вероятностного автомата $\alpha \rightarrow [p]\beta$, где α и β – цепочки символов в заданном алфавите; p – вероятность перехода состояний (применения функции перехода). Набор может включать в себя несколько функций переходов с одинаковой левой частью, но их суммарная вероятность не должна превышать единицы. Процесс применения функций переходов состоит в последовательном выполнении следующих шагов:

текущая цепочка случайным образом разделяется на подцепочки;

каждая полученная подцепочка заменяется на новую согласно заданному набору функций переходов с учетом их вероятностей;

все подцепочки, полученные в результате второго шага, соединяются и образуют новую текущую цепочку.

В результате выполнения этих шагов формируется марковская цепь с ограничением. На рис. 1 приведен пример представления марковской сети (цепи) с переходами в виде графа.

Если правая и левая части каждого правила заданной системы функций переходов имеют равные длины, то такую марковскую систему можно трактовать как блочный вероятностный клеточный автомат

– марковский автомат, в котором состояния клеток меняются согласованно в рамках каждого блока, а сами блоки формируются случайным образом.

На основе модели марковской системы определим понятие двумерного марковского автомата, являющегося частным случаем понятия блочного вероятностного клеточного автомата, применение которого при формировании низкоуровневых правил вывода языка изображений показано в [3]. В таких автоматах пространство клеток образует матрицу, а разбиение клеток на горизонтальные и вертикальные блоки происходит вероятностным образом.

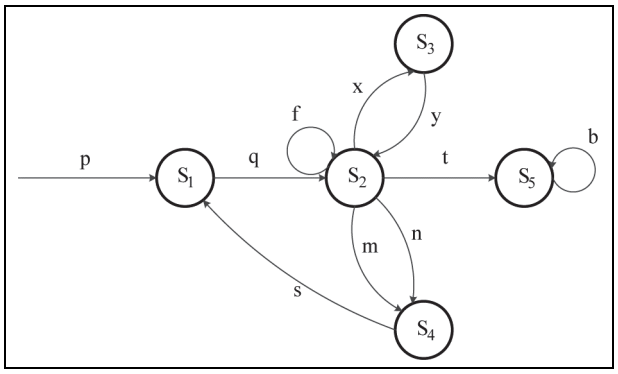


Рис. 1. Пример марковской сети (цепи) с переходами

Двумерные марковские автоматы представляют собой прямоугольную решетку (матрицу) размера $n \times m$, в каждую ячейку которой помещен символ заданного алфавита. Состояние такого автомата меняется со временем по следующему алгоритму: на каждом шаге эволюции с вероятностью 1/2 выбирается способ разбиения матрицы символов на цепочки – вертикально (на столбцы) или горизонтально (на строки), после чего каждая цепочка преобразуется стандартным (вышеописанным) образом.

В [8] было показано, что марковские автоматы являются алгоритмически универсальными системами, способными реализовывать сколь угодно сложные алгоритмы и демонстрировать упорядоченное поведение.

Простейший фрагмент нейронной сети, управляющий рассмотренными вероятностными автоматами, может быть описан следующим образом. Представим искусственный нейрон в виде двумерной области, состоящей из символов λ (возбудимая среда). Нейрон передает свое возбуждение другим нейронам с помощью аксона, представленного цепочкой символов α. Распространение сигнала по аксону описывается функциями переходов $x\alpha \to x\tilde{}x$ и $\tilde{}x\alpha \to \tilde{}x\tilde{}x$, первая из которых инициирует возбуждение аксона, а вторая отвечает за распространение возбуждения вдоль аксона. Передача возбуждения с аксона на другой нейрон выполняется с помощью синапса, представляющего собой некоторую область, отделенную от нейрона прослойкой символов s, моделирующей синоптическую щель. Синапс заполнен символами A или B, представляющими собой нейромедиаторы в неактивной форме. После того как возбуждение аксона достигло синапса, все его нейромедиаторы переводятся в активное состояние (a или b) и переносятся в нейрон через синоптическую щель, возбуждая нейрон или тормозя его возбуждение. На рис. 2 приведен пример модели нейронной сети.

Хотя нейроны в предложенной модели способны только возбуждаться, а сбрасывать возбуждение не могут, тем не менее, из таких нейронов можно строить нейронные сети прямого распространения, например, многослойные персептроны со ступенчатой функцией активации нейронов.

Это демонстрирует принципиальную схему организации нейронной сети, управляющей вероятностным автоматом. Для реализации полноценной нейронной сети, обеспечивающей глубокое обучение для предметной области «предложений» на языке изображений (картинок), дополнительно требуется уровень композиции автоматов.

Проблема проверки реализации средств языка изображений (картинок) в среде базы данных и его возможностей. Эта проблема порождена использованием языка изображений (картинок).

В качестве пути решения этой проблемы представляется целесообразным для создания инструментария, обеспечивающего реализацию средств языка изображений (картинок) и разбор входящего потока фрагментов ОРИ по АЗ, рассмотреть среду современных объектно-реляционных баз данных,

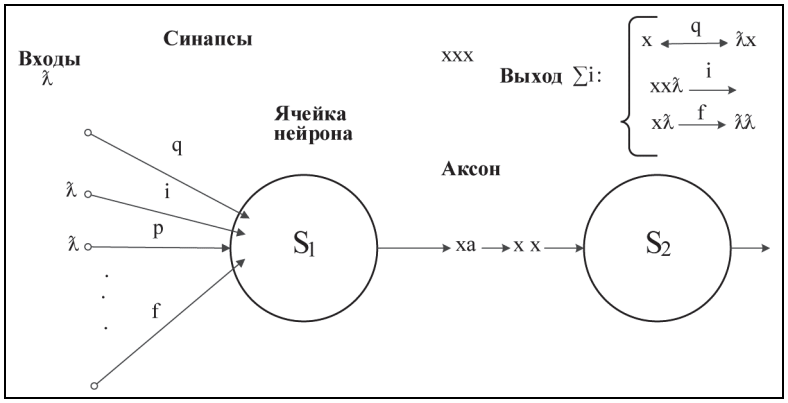


Рис. 2. Пример модели нейронной сети

например, PostgreSQL [9], и ее возможности. PostgreSQL является одной из баз данных, на которой реализованы системы для подразделений, выполняющих ПСР в морском и воздушном транспорте [6], что позволяет эффективно на реальных данных проверять разрабатываемые средства языка изображений (картинок). При реализации языка изображений (картинок) важно сделать так, чтобы имеющиеся средства представления пространственной информации были реализованы с использованием быстродействующих методов доступа к интерпретированным средствам языка изображений (картинок), то есть важно быстрое выполнение таких процедур, как поиск по набору данных ОРИ.

Имеется т р и п у т и: реализовать метод доступа, используемый языком изображений (картинок), имеющимися средствами обобщенной индексации PostgreSQL; разработать новый метод доступа (с нуля), обеспечив его реальное соответствие математической модели вероятностного представления образов ОРИ; комбинированный путь.

Реализация п е р в о г о п у т и связана с использованием имеющихся в данной СУБД *средств поиска типа GiST* (Generalized Search Tree – Обобщенное поисковое дерево), представляющих собой сбалансированное дерево поиска для типов данных типа «смеси» пространственных данных, картинок и связанных с ними описаний (текстовых документов). Для использования этих средств важны пространственные отношения или отношения, задаваемые в рамках языка изображений (картинок). Не подходят только операторы типа арифметических сравнений или сравнения текстовых строк.

Метод GiST позволяет задать принцип размещения разнообразных, в общем случае не сопоставимых корректно данных по сбалансированному дереву данных. При этом для доступа к данным может быть использован оператор, определяемый функциональными задачами, решаемыми по отношению к объектам поиска/наблюдения. Например, в качестве оператора может быть использован фотоэталон или процедура идентификации, отождествления и сопоставления ОРИ при загрузке данных в хранилище ХОРИАЗ. GiST-индекс может содержать квадро-дерево (Quad-tree), полосковое дерево (Streep tree), R-дерево[2] или RD-дерево и обеспечивает поддержку отношений (операторов) пересечения или включения [18, 22]. В [10, 11] предложена структура индекса GiST для обобщенной разновидности R-дерева, обеспечивающего реализацию стандартных методов навигации по дереву и его обновления (расщепления и удаления узлов).

Как было показано в [3], все требуемые отношения между элементами картинки, составляющей изображение ОРИ и отраженной средствами описания на языке изображений (картинок), могут быть формально «погружены в дерево» [18]. При этом реализации циклов потребуют формирования составного индекса, что приведет к дополнительным затратам памяти и загрузке процессора. Для достаточно больших структур данных [15, 24, 25], построенных с использованием языка изображений (картинок), также может потребоваться распараллеливание обработки [12, 15, 17], например, путем, который был рассмотрен в [3] на примере параллельной архитектуры графического процессора NVIDIA.

Реализация в т о р о г о п у т и связана с формированием нового метода доступа, специализированного на обработке предложений языка изображений (картинок), и соответствующего механизма пространственного и структурного индексирования (отражающего структуру объекта, содержащуюся в предложениях языка). Продвижение по этому пути также требует решения вопроса восстановления ОРИ объекта, выбранного по индексу из сохраненного в базе данных PostgreSQL, а также данных, связанных с этим индексом. Для реализации в PostgreSQL нового метода доступа «с нуля» потребуется сформировать программный интерфейс с механизмом индексирования. Для этого нужна адаптация логики вероятностных автоматов и частично компонентов нейронной сети с учетом не только логики индексации, но и страничной структуры организации памяти, эффективной реализации блокировок, поддержки журнала упреждающей записи и т.п. [17]. Реализация этого пути сопряжена с достаточно большим объемом разработки и высокой трудоемкостью реализации. Положение усугубляется необходимостью отслеживания версий открытого программного продукта PostgreSQL.

Реализация к о м б и н и р о в а н н о г о п у т и связана с формированием нового метода доступа, специализированного на обработке предложений языка изображений (картинок), средствами высокого уровня с разрешением низкоуровневых проблем средствами поиска GiST. Наличие средств поиска GiST упрощает задачу, беря на себя низкоуровневые проблемы и предоставляя свой собственный ин-

[2] В R-дереве закодированы пространственные данные, а индекс обеспечивает вычисления обычных типов пространственных отношений (операторов взаимного расположения, например: размещено по одну или другую сторону; включает, пересекает и др.) [18].

терфейс: несколько функций, относящихся не к технической сфере, а к прикладной области. В этом смысле можно говорить о том, что GiST – удобный каркас для построения метода доступа, работающего с представлениями на языке изображений (картинок).

Удобным формализмом для представления многих методов доступа в СУБД являются графы – деревья предикатов, в которых узлы-предикаты выполняются для всех ключей, содержащихся в подчиненных вершинах этого дерева. Совместно такие структуры и обеспечивают исполнение процедур хранения и выборки данных для обработки.

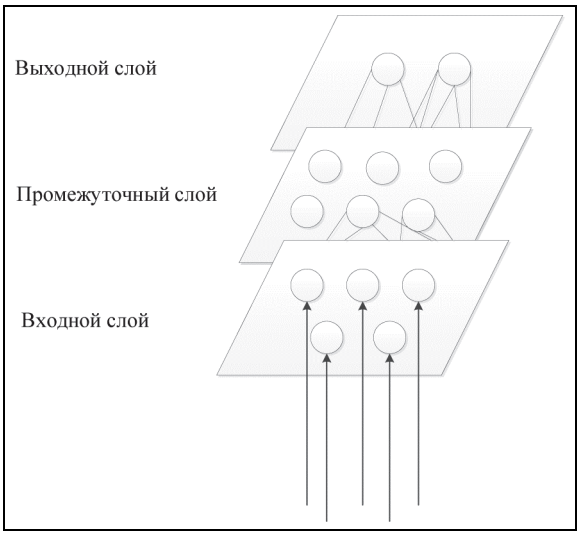


Рис. 3. Пример трехслойной нейронной сети

Представляется возможным также использовать СУБД для хранения данных нейронных сетей, используемых для управления вероятностными характеристиками переходов из состояния в состояние автоматов, выражающих правила разбора изображений языка изображений (картинок). Для этой цели разумно использовать реляционную СУБД. Реляционные СУБД традиционно применяются для хранения больших объемов данных [3]. При их использовании необходимо учитывать следующее: данные, описывающие структуру многослойного персептрона, достаточно хорошо структурированы, однако напрямую не могут быть представлены в реляционном виде (для этих целей хорошо подходят сетевые или иерархические СУБД, но такие программные средства практически не используются). Для описания структуры персептрона в терминах реляционной модели требуется ее нормализация [20]. Пример реляционной модели данных, описывающей структуру трехслойного персептрона (один слой скрытый), приведен на рис. 3.

Пример нормализованной реляционной модели данных, описывающей структуру многослойного персептрона, приведен на рис. 4. Логические связи между сущностями «слой–нейрон», «нейрон–связь», «сеть–слой», «нейрон–входная связь», «вход–входная связь», а также «сеть–вход» являются связями типа «один–ко-многим» и реализуются в БД при помощи ограничений целостности внешних ключей.

Известно, что совокупность экземпляров сущностей в реляционной БД представляет собой множество, то есть на уровне БД не может быть определен порядок следования и размещения этих экземпляров. Для нейронов и связей это не является критичным, так как результат работы сети будет определяться лишь структурой самой сети. Для входов же сети (на входном слое – input) порядок их следования и размещения является важным, так как он определяет способ взаимодействия рецепторов сети с внешней системой. Для этого в сущности «input» определен атрибут «input_seq», при помощи которого будет задаваться «порядковый номер» входа при подаче на него внешнего воздействия.

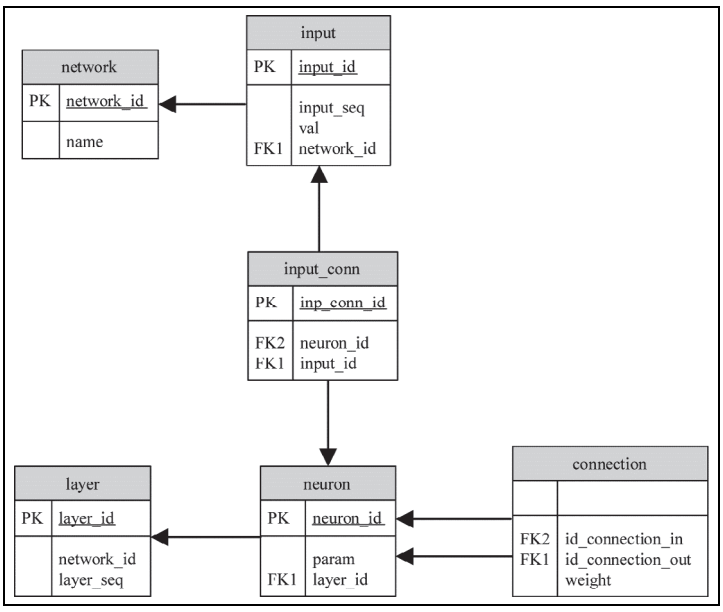


Рис. 4. Пример реляционной модели представления нейронной сети средствами реляционной СУБД

Порядок следования слоев нейронов может быть определен неявно как порядок следования входящих в слои нейронов, задаваемый направленными связями. Более того, сама сущность «слой» в некотором смысле является избыточной, так как, определив при помощи связей порядок следования нейронов, можно сделать вывод о числе слоев и о распределении нейронов по этим слоям. Тем не менее, присутствие сущности «слой» (layer) с атрибутом, определяющим порядковый номер слоя (layer_seq), в модели

желательно, так как далеко не все реляционные СУБД поддерживают рекурсивные SQL-запросы, а в отсутствии такого вида запросов нахождение в БД «цепочек» нейронов возможно только алгоритмическим (нереляционным) способом, что, очевидно, сильно снижает преимущества использования реляционного представления данных.

Предложенная реляционная модель представления многослойного персептрона может быть использована при разработке систем и средств моделировании нейронных сетей. Возможные количественные ограничения на число слоев и нейронов сети определяются только возможностями используемой СУБД. Модель инвариантна к типу применяемой реляционной СУБД.

Развитием предложенной модели является реализация дополнительных ограничений целостности, таких как, например, исключение дублирования связей, исключение связей «через слой», обратнонаправленных связей. Такие ограничения реализуются при помощи триггеров, которые поддерживаются большинством современных СУБД.

Проблема реализации средств создания и модификации структур байесовских нейронных сетей (редакторов сетей, использования наборов данных для обучения сетей). Эта проблема порождена использованием обучающихся нейронных сетей для управления вероятностными характеристиками переходов из состояния в состояние автоматов, выражающих правила разбора изображений языка изображений (картинок).

В качестве пути решения этой проблемы представляется целесообразным использовать средства создания и моделирования нейронных сетей с открытым кодом. В настоящее время имеется большое число проектов с открытым исходным кодом создания и моделирования нейронных сетей, таких как: «brain.js» (https://github.com/harthur-org/brain.js); «karpathy/convnetjs» (https://github.com/karpathy/convnetjs) и т.п. Компания Микрософт поддерживает проект с открытым исходным кодом https://azure.microsoft.com/en-us/services/cognitive-services/?v=17.29 и предлагает программный интерфейс пользователя «Computer Vision API» и «Video API» «Custom Vision Service». Обучение нейронных сетей может быть выполнено за счет использования таких наборов данных с изображениями трехмерных объектов, как «THE NORB DATASET, V1.0» (http://www.cs.nyu.edu/~ylclab/data/norb-v1.0/index.html) и аналогичных. Дополнительные изображения могут быть собраны из информационных систем поиска и спасания, где они хранятся как отчетные материалы по спасательным операциям. При этом дополнительной проработки и экспериментальной проверки требует вопрос эффективности применения и обучения таких сетей.

Проблема внедрения языков (типа OWL и т.п.) для создания онтологий предметных областей, в которых проводится решение задач обработки данных ОРИ по АЗ. Эта проблема, затронутая в [13, 14, 16], порождена использованием онтологий для кластеризации и/или доступа к ОРИ, сохраняемой в ХОРИАЗ, а также использованием активного картографического фона в качестве графического интерфейса пользователя и для визуализации ОРИ.

Пути решения этой проблемы рассмотрены в [21] применительно к визуализируемым пространственным данным.

Проблема интеграции всех типов данных в единой (как централизованной, так и распределенной) среде ХОРИАЗ и оперативного доступа к ним в ходе ПСР. Эта проблема порождена использованием ХОРИАЗ для хранения ОРИ по АЗ и его двойственной природой – централизованным хранением данных, собираемых в повседневной обстановке, а также сохраняемых по завершению конкретных ПСР (за исключением данных, относящихся к охраняемым в конкретных ведомствах и организациях) [22, 27], и децентрализованным [23, 26] хранением данных об оперативной обстановке, относящихся к конкретной ПСР и используемых в ее ходе.

Пути решения данной проблемы намечены в [4, 13, 24].

- Рассмотрены проблемы использования ОРИ, интегрированной в единое ХОРИАЗ, обусловленные решением задач ретроспективного анализа и прогнозирования перемещения и изменения объектов поиска/наблюдения. Проблемы рассмотрены совместно с путями их решения. Проблемы использования ОРИ определяются новыми способами описания (с применением языка описания изображений (картин)) и индексирования интегрированной в ХОРИАЗ информации.

  Сформулированы следующие проблемы использования ОРИ:

  проблемы разработки дополнительных процедур извлечения пространственных знаний об ОРИ по АЗ;

проблемы достаточной математической формализации правил построения языка изображений (картинок);

проблемы управления вероятностными характеристиками переходов состояний вероятностных автоматов;

проблемы проверки реализации средств языка изображений (картинок) в среде базы данных и его возможностей;

проблемы реализации средств создания и модификации структур байесовских нейронных сетей;

проблемы внедрения языков (типа OWL и т.п.);

проблемы интеграции всех типов данных в единой (как централизованной, так и распределенной) среде ХОРИАЗ и оперативного доступа к ним в ходе ПСР.

Разработан единый подход к решению указанных проблем. В основе подхода лежит применение при решении задач ретроспективного анализа и прогнозирования перемещения и изменения объектов поиска/наблюдения средств языка описания изображений (картинок), позволяющих решить задачи идентификации, отождествления и сопоставления при интеграции ОРИ по АЗ в едином ХОРИАЗ.

Показано, что применение объектно-реляционной БД позволит провести как макетирование ХОРИАЗ, так и использование доступа к сохраняемой в нем ОРИ при решении задачи идентификации, отождествления и сопоставления.

Определена математическая основа предлагаемых решений по повышению качества процессов идентификации, сопоставлению и отождествлению ОРИ с использованием методов обучения байесовских сетей, обеспечивающих «настройку» языка изображений (картинок), а также других параметров (например, метаинформации), описывающих ОРИ.

Установлено, что визуализация и создание эффективного и удобного интерфейса пользователя для решения задач поддержки процедур идентификации, отождествления и сопоставления ОРИ по АЗ, работы с эталонами изображений, спецификации изменений изображений (язык) обеспечивается применением при реализации указанных процедур средств активного картографического фона.

В рамках работ, проводимых при поддержке РФФИ по теме № 15-29-06997 «Фундаментальные проблемы идентификации, сопоставления и интеграции в единое хранилище ОРИ по Арктической зоне», было выполнено прототипирование (создана программная реализация) средств ХОРИАЗ на примере систем, решающих задачи в области ПСР. На основе прототипа были созданы дополнительные модели и подсистемы в рамках ФГИС «ИАС-Поиск» и «Поиск-Море», обеспечивающие работу координационных центров поиска и спасания в АЗ [6].

Перспективными направлениями дальнейших исследований в области обработки ОРИ при создании ХОРИАЗ являются:

повышение эффективной обработки ОРИ по АЗ;

обработка ОРИ в реальном времени поступления информации с применением методов сетевых вычислений;

совершенствование средств сбора первичной ОРИ (беспилотные системы, технологии интернета, методы сбора косвенной и неявной ОРИ по АЗ в источниках, не локализованных в странах АЗ, за счет совершенствования методов поиска в глобальных информационных ресурсах сети интернет и иных хранилищ данных).

Статья подготовлена в рамках работ, проводимых при поддержке РФФИ, по теме № 15-29-06997 «Фундаментальные проблемы идентификации, сопоставления и интеграции в единое хранилище ОРИ по Арктической зоне».

Литература

1. *Будзко В.И., Беленков В.Г., Сметанин Н.Н.* Проблемы идентификации, сопоставления и интеграции в единое хранилище оптической и радиолокационной информации по Арктической зоне // Труды Междунар. научно-технич. конф. «Информационные технологии и математическое моделирование систем 2015». Центр информационных технологий в проектировании РАН. М.: Планета. 2015. С. 133−137.
2. *Будзко В.И., Беленков В.Г., Сметанин Н.Н.* Хранилище оптической и радиолокационной информации по арктической зоне («ХОРИАЗ») // Системы высокой доступности. 2015. Т. 11. № 4. С. 3−15.

3. *Будзко В.И., Беленков В.Г., Сметанин Н.Н., Улитенков М.В.* О подходе к построению языка изображений (картинок) – Picture Language, формированию поискового образа объекта поиска и к их использованию при идентификации путем сопоставления оптической и радиолокационной информации по Арктической зоне и при ее интеграции // Системы высокой доступности. 2016. Т. 12. № 2. С. 55−63.
4. *Будзко В.И., Беленков В.Г., Сметанин Н.Н., Улитенков М.В., Зеленикин А.А.* Проблемы интеграции в единое хранилище оптической и радиолокационной информации по Арктической зоне // Системы высокой доступности. 2017. Т. 13. № 1. С. 3−21.
5. *Будзко В.И., Беленков В.Г., Сметанин Н.Н., Улитенков М.В., Зеленикин А.А.* Язык описания изображений, используемый при интеграции в хранилище оптической и радиолокационной информации по Арктической зоне // Системы высокой доступности. 2017. Т. 13. № 1. С. 22−38.
6. *Н.Н., Сметанин.* Обеспечение взаимодействия систем управления беспилотных авиационных систем, поисковых целевых нагрузок и устройств определения местоположения воздушных судов с системами информационной поддержки поисково-спасательных работ ФГИС «ИАС Поиск» // Труды научно-технич. конф. «Применение БАС для совершенствования задач поиска и спасания в интересах гражданской авиации». М.: Росавиация. 2015. URL = http://docplayer.ru/34669350-Rosaviaciya-nauchno-tehnicheskaya-konferenciya.html.
7. *Joaquin A. Trinanes, M. Josefina Olascoaga, Gustavo J. Goni, Nikolai A.* Analysis of flight MH370 potential debris trajectories using ocean observations and numerical model results // journal of Operational Oceanography. 2016. V. 9. P. 126−138.
8. *Ершов Н.М., Кравчук А.В.* Дискретное моделирование с помощью стохастических клеточных автоматов // Вестник Российского университета дружбы народов. Сер. «Математика, информатика, физика». 2014.
9. *Jayadevan Maymala* PostgreSQL for Data Architects. Discover how to design, develop, and maintain your database application effectively with PostgreSQL. Packt Publishing. 2015.
10. *Chitij Chauhan* PostgreSQL Cookbook. Over 90 hands-on recipes to effectively manage, administer, and design solutions using PostgreSQL. Packt Publishing. 2015.
11. *Krzysztof Grabczewski* Meta-Learning in Decision Tree Induction. Springer International Publishing. Switzerland. 2014.
12. *Harsh Bhasin* Algorithms: Design and Analysis. Oxford University Press. 2015.
13. *Jason Bell* Machine Learning. Hands-On for Developers and Technical Professionals. Indianapolis, Indiana: John Wiley & Sons, Inc. 2015.
14. *Miroslav Kubat* An Introduction to Machine Learning. Springer International Publishing. Switzerland. 2015.
15. *Ron Bekkerman* Scaling up Machine Learning. Parallel and Distributed Approaches. Cambridge University Press. 2012.
16. *Ajith Abraham, Crina Grosan* Intelligent Systems: A Modern Approach. Springer-Verlag. Berlin. Heidelberg. 2011.
17. *Rod Stephens* Essential Algorithms. A Practical Approach to Computer Algorithms. Morgan & Claypool. 2016.
18. *Herbert Freeman*, *Pieroni G.G.* Computer Architectures for Spatially Distributed Data. Springer Science & Business Media. 2013.
19. *Hellerstein J.M.*, *Naughton J.F. and Avi Pfeffer* Generalized search trees for database systems // In Proc. of the 21st International Conference on Very Large Data Bases. Zurich. Switzerland. 1995.
20. *Кузин Д.А.*, *Запевалов А.В.*, *Сырчин А.В.* Реляционная модель представления многослойного персептрона // Современные наукоемкие технологии. 2013. С. 45−48.
21. *Дулин С.К.*, *Дулина Н.Г.*, *Никишин Д.А.* Представление онтологий визуализируемых геоданных // Системы высокой доступности. 2016. Т. 12. № 2. С. 28−37.
22. *David Patterson, John Hennessy* Computer Organization and Design, Fifth Edition. The Hardware/Software Interface. Elsevier Inc. 2014.
23. *Frank S. Haug*, *Saeed K. Rahimi* Distributed Database Management Systems: A Practical Approach. IEEE Computer Society. John Wiley & Sons, Inc. Hoboken. New Jersey. 2010.
24. *Bahaaldine Azarmi* Scalable Big Data Architecture. A practitioners guide to choosing relevant Big Data architecture. Bahaaldine Azarmi. 2016. URL = www.apress.com.
25. *Amparo Alonso-Betanzos, Noelia Sánchez-Maroño, Verónica Bolón-Canedo* Feature Selection for High-Dimensional Data. Springer International Publishing. Switzerland. 2015.
26. *Fabrice Kordon, Laure Petrucci, Laurent Pautet, Serge Haddad* Distibuted Systems. Design and Algorithms. ISTE Ltd and John Wiley & Sons, Inc. 2011.
27. *Brice Goglin, Pascale Vicat-Blanc, Romaric Guillier, Sebastien Soudan* Computing Networks. From Cluster to Cloud Computing. ISTE Ltd and John Wiley & Sons, Inc. 2011.

Поступила 7 декабря 2017 г.

Problems of the integrated into ORISAZ optical and radar information (ORI) use and their solutions

V.I. Budzko – Dr. Sc. (Eng.), Member of Russian Cryptography Academy, Deputy Director on Research and Development, Institute of Informatics Problems of FRC CSC RAS (Moscow)
E-mail: vbudzko@ipiran.ru
V.G. Belenkov – Ph. D. (Eng.), Leading Research Scientist, Institute of Informatics Problems of FRC CSC RAS (Moscow)
E-mail: vbelenkov@ipiran.ru

N.N. Smetanin – Ph. D. (Eng.), General Director, JSC «Pallada» (Moscow)
E-mail: snn@geopallada.ru
M.V. Ulitenkov – Deputy General Director, JSC «Pallada» (Moscow)
E-mail: umv@geopallada.ru
A.A. Zelenikin – Head of Department, «RCC of Rosmorrechflot»
E-mail: aaz61@mail.ru

Problems of using optical and radar information (ORI) that is integrated into a optical and radar information Storage for the Arctic zone («ORISAZ») are considered in the article. The problems are considered on the basis of methods that have been discussed in previous articles, released as part of RFBR №15-29-06997. The problems are caused by the solution of the task of retrospective analysis and forecasting of movement and change of objects of the search/surveillance. The problems are discussed in conjunction with ways to address them. The problems of using ORI are caused by the new ways of describing (with the use of The Image (pictures) Description Language – IDL) and indexing of the integrated in the Storage («ORISAZ») information. IDL – is a formal language that provides images description, mapping and restoring. IDL specification also includes search images of objects of the search/surveillance with their etalons, considered as parameters of procedures of a more general language.

References

1. *Budzko V.I., Belenkov V.G., Smetanin N.N.* Problemy' identifikaccii, sopostavleniya i integraccii v edinoe xranilishhe opticheskoj i radiolokaccionnoj informaccii po Arkticheskoj zone // Trudy' Mezhdunar. nauchno-texnich. konf. «Informaccionny'e texnologii i matematicheskoe modelirovanie sistem 2015». Czentr informaccionny'x texnologij v proektirovanii RAN. M.: Planeta. 2015. S. 133–137.
2. *Budzko V.I., Belenkov V.G., Smetanin N.N.* Xranilishhe opticheskoj i radiolokaccionnoj informaccii po arkticheskoj zone («XORIAZ») // Sistemy' vy'sokoj dostupnosti. 2015. T. 11. № 4. S. 3–15.
3. *Budzko V.I., Belenkov V.G., Smetanin N.N., Ulitenkov M.V.* O podxode k postroeniyu yazy'ka izobrazhenij (kartinok) – Picture Language, formirovaniyu poiskovogo obraza ob"ekta poiska i k ix ispol'zovaniyu pri identifikaccii putem sopostavleniya opticheskoj i radiolokaccionnoj informaccii po Arkticheskoj zone i pri ee integraccii // Sistemy' vy'sokoj dostupnosti. 2016. T. 12. № 2. S. 55–63.
4. *Budzko V.I., Belenkov V.G., Smetanin N.N., Ulitenkov M.V., Zelenikin A.A.* Problemy' integraccii v edinoe xranilishhe opticheskoj i radiolokaccionnoj informaccii po Arkticheskoj zone // Sistemy' vy'sokoj dostupnosti. 2017. T. 13. № 1. S. 3–21.
5. *Budzko V.I., Belenkov V.G., Smetanin N.N., Ulitenkov M.V., Zelenikin A.A.* Yazy'k opisaniya izobrazhenij, ispol'zuemy'j pri integraccii v xranilishhe opticheskoj i radiolokaccionnoj informaccii po Arkticheskoj zone // Sistemy' vy'sokoj dostupnosti. 2017. T. 13. № 1. S. 22–38.
6. *N.N., Smetanin.* Obespechenie vzaimodejstviya sistem upravleniya bespilotny'x aviaccionny'x sistem, poiskovy'x czelevy'x nagruzok i ustrojstv opredeleniya mestopolozheniya vozdushny'x sudov s sistemami informaccionnoj podderzhki poiskovo-spasatel'ny'x rabot FGIS «IAS Poisk» // Trudy' nauchno-texnich. konf. «Primenenie BAS dlya sovershenstvovaniya zadach poiska i spasaniya v interesax grazhdanskoj aviaczii». M.: Rosaviacziya. 2015. URL = http://docplayer.ru/34669350-Rosaviaciya-nauchno-tehnicheskaya-konferenciya.html.
7. *Joaquin A. Trinanes, M. Josefina Olascoaga, Gustavo J. Goni, Nikolai A.* Analysis of flight MH370 potential debris trajectories using ocean observations and numerical model results // journal of Operational Oceanography. 2016. V. 9. P. 126–138.
8. *Ershov N.M., Kravchuk A.V.* Diskretnoe modelirovanie s pomoshh'yu stoxasticheskix kletochny'x avtomatov // Vestnik Rossijskogo universiteta druzhby' narodov. Ser. «Matematika, informatika, fizika». 2014.
9. *Jayadevan Maymala* PostgreSQL for Data Architects. Discover how to design, develop, and maintain your database application effectively with PostgreSQL. Packt Publishing. 2015.
10. *Chitij Chauhan* PostgreSQL Cookbook. Over 90 hands-on recipes to effectively manage, administer, and design solutions using PostgreSQL. Packt Publishing. 2015.
11. *Krzysztof Grabczewski* Meta-Learning in Decision Tree Induction. Springer International Publishing. Switzerland. 2014.
12. *Harsh Bhasin* Algorithms: Design and Analysis. Oxford University Press. 2015.
13. *Jason Bell* Machine Learning. Hands-On for Developers and Technical Professionals. Indianapolis, Indiana: John Wiley & Sons, Inc. 2015.
14. *Miroslav Kubat* An Introduction to Machine Learning. Springer International Publishing. Switzerland. 2015.
15. *Ron Bekkerman* Scaling up Machine Learning. Parallel and Distributed Approaches. Cambridge University Press. 2012.
16. *Ajith Abraham, Crina Grosan* Intelligent Systems: A Modern Approach. Springer-Verlag. Berlin. Heidelberg. 2011.
17. *Rod Stephens* Essential Algorithms. A Practical Approach to Computer Algorithms. Morgan & Claypool. 2016.
18. *Herbert Freeman*, *Pieroni G.G.* Computer Architectures for Spatially Distributed Data. Springer Science & Business Media. 2013.
19. *Hellerstein J.M.*, *Naughton J.F. and Avi Pfeffer* Generalized search trees for database systems // In Proc. of the 21st International Conference on Very Large Data Bases. Zurich. Switzerland. 1995.
20. *Kuzin D.A.*, *Zapevalov A.V.*, *Sy'rchin A.V.* Relyaccionnaya model' predstavleniya mnogoslojnogo perseptrona // Sovremenny'e naukoemkie texnologii. 2013. S. 45–48.
21. *Dulin S.K.*, *Dulina N.G.*, *Nikishin D.A.* Predstavlenie ontologij vizualiziruemy'x geodanny'x // Sistemy' vy'sokoj dostupnosti. 2016. T. 12. № 2. S. 28–37.
22. *David Patterson, John Hennessy* Computer Organization and Design, Fifth Edition. The Hardware/Software Interface. Elsevier Inc. 2014.
23. *Frank S. Haug*, *Saeed K. Rahimi* Distributed Database Management Systems: A Practical Approach. IEEE Computer Society. John Wiley & Sons, Inc. Hoboken. New Jersey. 2010.
24. *Bahaaldine Azarmi* Scalable Big Data Architecture. A practitioners guide to choosing relevant Big Data architecture. Bahaaldine Azarmi. 2016. URL = www.apress.com.
25. *Amparo Alonso-Betanzos, Noelia Sánchez-Maroño, Verónica Bolón-Canedo* Feature Selection for High-Dimensional Data. Springer International Publishing. Switzerland. 2015.
26. *Fabrice Kordon, Laure Petrucci, Laurent Pautet, Serge Haddad* Distibuted Systems. Design and Algorithms. ISTE Ltd and John Wiley & Sons, Inc. 2011.
27. *Brice Goglin, Pascale Vicat-Blanc, Romaric Guillier, Sebastien Soudan* Computing Networks. From Cluster to Cloud Computing. ISTE Ltd and John Wiley & Sons, Inc. 2011.

УДК 517.977

Подходы к стабилизации систем с периодическими коэффициентами

В.В. Фомичев – д.ф.-м.н., гл. науч. сотрудник, Центр информационных технологий в проектировании РАН (г. Одинцово, Моск. обл.)
E-mail: fomichev@cs.msu.ru

Проанализирована проблема стабилизации одного из подклассов нестационарных линейных систем управления, а именно систем с периодическими коэффициентами. Рассмотрены как общие вопросы анализа устойчивости таких систем, так и алгоритмы построения стабилизирующей обратной связи, в частности для дискретных систем. Показано, что для стабилизации системы требуется решать систему полиномиальных уравнений, при этом число переменных может быть увеличено за счет увеличения периода управления по сравнению с периодом самой системы.

Ключевые слова: *нестационарные системы, периодические системы, стабилизация.*

In article, the problem of stabilizing of one of subclasses of non-stationary linear management systems is considered. Systems with periodic coefficients are considered. In article there are studied as the general questions of the analysis of stability of such systems, and algorithms of creation of stabilizing feedback coupling. In particular, stabilizing algorithms for the discrete systems are received. It is shown that for stabilizing of system it is required to solve the system of the polynomial equations, at the same time the number of variables can be increased due to increase in the period of control in comparison with the period of the system.

Keywords: *non-stationary systems, periodic systems, stabilization.*

В настоящее время во многих инженерных задачах современной техники используются системы линейных дифференциальных уравнений с периодическими коэффициентами. Они используются для описания явлений, которые определяются величинами, периодически изменяющимися во времени или в пространстве. Например, с системами такого типа приходится встречаться при расчете периодических режимов систем автоматического регулирования, ускорителей элементарных частиц, динамической устойчивости упругих систем, линий высоковольтных передач и для решения других практически значимых задач.

Общие вопросы динамики систем с периодическими коэффициентами можно изучить по классическим монографиям: Г. Д'Анжело «Линейные системы с переменными параметрами. Анализ и синтез»; И.В. Гайшун «Введение в теорию линейных нестационарных систем» и др. [1–4]. С их помощью можно изучить общую теорию, связанную с исследованием систем линейных дифференциальных уравнений с периодическими коэффициентами, однако в них не рассматриваются вопросы управления такими системами.

Актуальность и практический аспект выбранной темы связаны с тем, что совсем не много авторов брались за стабилизацию таких систем в общем виде (хотя анализ их устойчивости изучался), и заключается в необходимости разработки рекомендаций по стабилизации систем линейных дифференциальных уравнений с периодическими коэффициентами.

Объектом исследования работы является система уравнений вида $\dot{x}(t) = \mathbf{A}(t)x(t) + \mathbf{B}(t)\mathbf{u}(t)$, где $\mathbf{A}(t+T) = \mathbf{A}(t)$, $\mathbf{B}(t+T) = \mathbf{B}(t)$ – периодические матрицы.

Относительно параметров системы предполагается, что они достаточно гладкие, а решение системы существует и единственно при $t > 0$.

Стабилизирующее управление, как правило, ищут в виде линейной обратной связи, но в случае периодических систем возможны разные варианты, например:

$\mathbf{u}(t) = -\mathbf{k}x(t)$ – стационарная обратная связь;

$\mathbf{u}(t) = -\mathbf{k}(t)x(t)$, при этом $\mathbf{k}(t+T) = \mathbf{k}(t)$ – периодическая обратная связь, тогда $\mathbf{B}(t)$ может быть не периодическая, а постоянная, а периодичность второго слагаемого получится за счет периодичности $\mathbf{k}(t)$;

для системы с выходом

$$\begin{cases} \dot{x}(t) = \mathbf{A}(t)x(t) + \mathbf{B}(t)\mathbf{u}(t), \\ y = \mathbf{C}x, \end{cases}$$

управление можно выбирать в виде $\mathbf{u}(t) = -\mathbf{k}y$ или задать более сложную связь $\mathbf{u}(t) = -\mathbf{k}(y)$ – обратную связь по выходу.

Ц е л ь р а б о т ы – проанализировать устойчивость и стабилизацию систем такого вида и найти метод исследования на устойчивость замкнутой системы дифференциальных уравнений с периодическими коэффициентами и предложение по алгоритмическому решению этой задачи.

Исследование непрерывной системы уравнений с периодическими коэффициентами на устойчивость

Рассмотрим систему $\dot{x}(t) = \mathbf{A}(t)x(t)$, где $\mathbf{A}(t+T) = \mathbf{A}(t)$ – непрерывная периодическая с периодом T матрица, $t \geq 0$.

Определение 1 [1]. Фундаментальная система решений – любой базис в пространстве решений.

Определение 2 [1]. Фундаментальная матрица – матрица, столбцы которой образуют фундаментальную систему решений.

Если $\mathbf{\Phi}(t)$ – фундаментальная матрица, то она удовлетворяет системе уравнений $\dot{\mathbf{\Phi}}(t) = \mathbf{A}(t)\mathbf{\Phi}(t)$.

Пусть $\mathbf{\Phi}(0) = \mathbf{I}$, тогда фундаментальная матрица $\mathbf{\Phi}(t)$ находится в явном виде, то есть ее можно записать в виде матричной экспоненты

$$\mathbf{\Phi}(t) = \exp\left[\int_0^t \mathbf{A}(\tau)\,d\tau\right].$$

Но несмотря на то, что существует формула Коши через матричную экспоненту, нахождение матричной экспоненты в явном виде – это в общем случае нерешенная задача.

Для анализа устойчивости периодической с периодом T системы необходима матрица $\mathbf{\Phi}(T)$. Заметим, что $x(t+T) = \mathbf{\Phi}(T)x(t)$, тогда при конкретных значениях решения через период будут отличаться друг от друга на множитель $\mathbf{\Phi}(T)$. Например, $x(0) = \mathbf{\Phi}(0)x(0) = x(0)$, $x(T) = \mathbf{\Phi}(T)x(0)$, $x(2T) = \mathbf{\Phi}(T)^2x(0)$, ….

В общем случае каждому τ из отрезка $[0;T]$ соответствует цепочка решений $x(t) = \left[\mathbf{\Phi}(T)\right]^{\left\lceil \frac{t}{T} \right\rceil} x(\tau)$, где $\tau = t - \left\lceil \frac{t}{T} \right\rceil T$.

Таким образом, для решения периодической системы необходимо найти решение только на промежутке $[0;T]$, и тогда можно будет найти решение системы в произвольный момент времени t.

Функция $x(t)$ как решение дифференциального уравнения непрерывна, значит $x(\tau)$ ограничена. Тогда устойчивость $x(t)$ определяется множителем $\mathbf{\Phi}(T)^k$. Остается решить вопрос, сходится ли к нулю последовательность $\mathbf{\Phi}(T)^k$?

Получается, что для устойчивости данной системы необходимо, чтобы собственные значения фундаментальной матрицы $\mathbf{\Phi}(T)$ (числовая матрица) принадлежали единичному кругу на комплексной плоскости C.

Стабилизация непрерывной системы уравнений с периодическими коэффициентами

Общие сведения. Одним из важных понятий при рассмотрении задач управления является стабилизируемость.

Определение 3 [2]. Управляемая система называется стабилизируемой, если существует закон управления, при котором замкнутая система асимптотически устойчива.

Рассмотрим систему $\dot{x}(t) = \mathbf{A}(t)x(t) + \mathbf{B}(t)\mathbf{u}(t)$, где $\mathbf{A}(t+T) = \mathbf{A}(t)$ непрерывная периодическая с периодом T матрица; $\mathbf{u}(t)$ – управление. Рассмотрим управление вида $\mathbf{u}(t) = -\mathbf{k}x$. Тогда система примет вид $\dot{x}(t) = \bar{\mathbf{A}}(t)x(t)$, где $\bar{\mathbf{A}}(t) = (\mathbf{A} - \mathbf{Bk})$.

Для стабилизации данной системы нужно подобрать $\mathbf{k}$ так, чтобы собственные значения фундаментальной матрицы $\bar{\mathbf{\Phi}}(T)$ принадлежали единичному кругу на комплексной плоскости C.

Исследование системы уравнений с периодическими коэффициентами с помощью перехода к дискретной системе. Сложность данной работы состоит в том, что при нахождении фундаментальной матрицы $\mathbf{\Phi}(T)$ необходимо считать интеграл от матричной экспоненты

$$\mathbf{\Phi}(t) = \exp\left[\int_0^t \mathbf{A}(\tau)\,d\tau\right],$$

но это не простая и не всегда разрешимая задача, поэтому перейдем к аналогичной дискретной системе уравнений $x^{t+1} = \mathbf{A}^t x^t + \mathbf{B}^t \mathbf{u}^t$, $\mathbf{A}^{t+T} = \mathbf{A}^t$, $t = 0, 1, 2, \ldots$, где верхние индексы относятся к значению функции в определенный момент времени. Например, x^t – значение функции x в момент времени t.

В таком случае фундаментальная матрица получается достаточно просто: $\mathbf{\Phi}^{t+1} = \mathbf{A}^t \mathbf{\Phi}^t$, $\mathbf{\Phi}^0 = \mathbf{I}$, $\mathbf{\Phi}^1 = \mathbf{A}^0$, $\mathbf{\Phi}^2 = \mathbf{A}^1\mathbf{\Phi}^1 = \mathbf{A}^1\mathbf{A}^0$, …, $\mathbf{\Phi}^T = \mathbf{A}^{T-1}\mathbf{A}^{T-2}\ldots\mathbf{A}^1\mathbf{A}^0$.

1. Возьмем простой случай системы второго порядка при $T = 2$. Тогда матрицы $\mathbf{A}^t$ представляют собой цепочку матриц $\mathbf{A}^0, \mathbf{A}^1, \mathbf{A}^0, \mathbf{A}^1, \ldots$. Пусть для простоты $\mathbf{B}$ – стационарная матрица, $\mathbf{u}^t = -\mathbf{k}^t x^t$, размерность матриц 2×2. Тогда система примет вид $x^{t+1} = \overline{\mathbf{A}^t} x^t$, где $\overline{\mathbf{A}^t} = \left(\mathbf{A}^t - \mathbf{B}\mathbf{k}^t\right)$.

Нужно подобрать значения $\mathbf{k}$ так, чтобы собственные значения $\mathbf{\Phi}(T)$ лежали внутри единичного круга.

С помощью вышеприведенной формулы найдем фундаментальную матрицу

$$\mathbf{\Phi}(T) = \left[\mathbf{A}^1 - \mathbf{B}\mathbf{k}^1\right]\left[\mathbf{A}^0 - \mathbf{B}\mathbf{k}^0\right] = \mathbf{A}^1\mathbf{A}^0 - \mathbf{A}^1\mathbf{B}\mathbf{k}^0 - \mathbf{B}\mathbf{k}^1\mathbf{A}^0 + \mathbf{B}\mathbf{k}^1\mathbf{B}\mathbf{k}^0.$$

Выпишем подробно каждую матрицу:

$$\mathbf{A}^0 = \begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \mathbf{k}^0 = \begin{bmatrix} k_0^0 & k_1^0 \end{bmatrix}, \mathbf{k}^1 = \begin{bmatrix} k_0^1 & k_1^1 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} \Phi_{11} & \Phi_{12} \\ \Phi_{21} & \Phi_{22} \end{bmatrix}.$$

Найдем матрицу $\mathbf{\Phi}(T)$ в явном виде:

$$\mathbf{A}^1\mathbf{A}^0 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}\begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix} = \begin{bmatrix} a_{11}^1 a_{11}^0 + a_{12}^1 a_{21}^0 & a_{11}^1 a_{12}^0 + a_{12}^1 a_{22}^0 \\ a_{21}^1 a_{11}^0 + a_{22}^1 a_{21}^0 & a_{21}^1 a_{12}^0 + a_{22}^1 a_{22}^0 \end{bmatrix},$$

$$\mathbf{A}^1\mathbf{B} = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_{11}^1 b_1 + a_{12}^1 b_2 \\ a_{21}^1 b_1 + a_{22}^1 b_2 \end{bmatrix},$$

$$\mathbf{A}^1\mathbf{B}\mathbf{k}^0 = \begin{bmatrix} a_{11}^1 b_1 + a_{12}^1 b_2 \\ a_{21}^1 b_1 + a_{22}^1 b_2 \end{bmatrix}\begin{bmatrix} k_0^0 & k_1^0 \end{bmatrix} = \begin{bmatrix} a_{11}^1 b_1 k_0^0 + a_{12}^1 b_2 k_0^0 & a_{11}^1 b_1 k_1^0 + a_{12}^1 b_2 k_1^0 \\ a_{21}^1 b_1 k_0^0 + a_{22}^1 b_2 k_0^0 & a_{21}^1 b_1 k_1^0 + a_{22}^1 b_2 k_1^0 \end{bmatrix},$$

$$\mathbf{B}\mathbf{k}^1 = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\begin{bmatrix} k_0^1 & k_1^1 \end{bmatrix} = \begin{bmatrix} b_1 k_0^1 & b_1 k_1^1 \\ b_2 k_0^1 & b_2 k_1^1 \end{bmatrix},$$

$$\mathbf{B}\mathbf{k}^1\mathbf{A}^0 = \begin{bmatrix} b_1 k_0^1 & b_1 k_1^1 \\ b_2 k_0^1 & b_2 k_1^1 \end{bmatrix}\begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix} = \begin{bmatrix} b_1 k_0^1 a_{11}^0 + b_1 k_1^1 a_{21}^0 & b_1 k_0^1 a_{12}^0 + b_1 k_1^1 a_{22}^0 \\ b_2 k_0^1 a_{11}^0 + b_2 k_1^1 a_{21}^0 & b_2 k_0^1 a_{12}^0 + b_2 k_1^1 a_{22}^0 \end{bmatrix},$$

$$\mathbf{B}\mathbf{k}^1\mathbf{B} = \begin{bmatrix} b_1 k_0^1 & b_1 k_1^1 \\ b_2 k_0^1 & b_2 k_1^1 \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} b_1 b_1 k_0^1 + b_1 b_2 k_1^1 \\ b_2 b_1 k_0^1 + b_2 b_2 k_1^1 \end{bmatrix},$$

$$\mathbf{B}\mathbf{k}^1\mathbf{B}\mathbf{k}^0 = \begin{bmatrix} b_1 b_1 k_0^1 + b_1 b_2 k_1^1 \\ b_2 b_1 k_0^1 + b_2 b_2 k_1^1 \end{bmatrix}\begin{bmatrix} k_0^0 & k_1^0 \end{bmatrix} = \begin{bmatrix} b_1 b_1 k_0^1 k_0^0 + b_1 b_2 k_1^1 k_0^0 & b_1 b_1 k_0^1 k_1^0 + b_1 b_2 k_1^1 k_1^0 \\ b_2 b_1 k_0^1 k_0^0 + b_2 b_2 k_1^1 k_0^0 & b_2 b_1 k_0^1 k_0^0 + b_2 b_2 k_1^1 k_0^0 \end{bmatrix},$$

$$\Phi_{11} = a_{11}^1 a_{11}^0 + a_{12}^1 a_{21}^0 - (a_{11}^1 b_1 + a_{12}^1 b_2)\boldsymbol{k}_0^0 - b_1 \boldsymbol{k}_0^1 a_{11}^0 - b_1 \boldsymbol{k}_1^1 a_{21}^0 + b_1 b_1 \boldsymbol{k}_0^1 \boldsymbol{k}_0^0 + b_1 b_2 \boldsymbol{k}_1^1 \boldsymbol{k}_0^0,$$

$$\Phi_{12} = a_{11}^1 a_{12}^0 + a_{12}^1 a_{22}^0 - (a_{11}^1 b_1 + a_{12}^1 b_2)\boldsymbol{k}_1^0 - b_1 \boldsymbol{k}_0^1 a_{12}^0 - b_1 \boldsymbol{k}_1^1 a_{22}^0 + b_1 b_1 \boldsymbol{k}_0^1 \boldsymbol{k}_1^0 + b_1 b_2 \boldsymbol{k}_1^1 \boldsymbol{k}_1^0,$$

$$\Phi_{21} = a_{21}^1 a_{11}^0 + a_{22}^1 a_{21}^0 - (a_{21}^1 b_1 + a_{22}^1 b_2)\boldsymbol{k}_0^0 - b_2 \boldsymbol{k}_0^1 a_{11}^0 - b_2 \boldsymbol{k}_1^1 a_{21}^0 + b_2 b_1 \boldsymbol{k}_0^1 \boldsymbol{k}_0^0 + b_2 b_2 \boldsymbol{k}_1^1 \boldsymbol{k}_0^0,$$

$$\Phi_{22} = a_{21}^1 a_{12}^0 + a_{22}^1 a_{22}^0 - (a_{21}^1 b_1 + a_{22}^1 b_2)\boldsymbol{k}_1^0 - b_2 \boldsymbol{k}_0^1 a_{12}^0 - b_2 \boldsymbol{k}_1^1 a_{22}^0 + b_2 b_1 \boldsymbol{k}_0^1 \boldsymbol{k}_1^0 + b_2 b_2 \boldsymbol{k}_1^1 \boldsymbol{k}_1^0.$$

Если эта система из четырех уравнений с четырьмя неизвестными $\boldsymbol{k}$ (выделены для наглядности) имеет решение, то с помощью них всегда можно получить наперед заданную фундаментальную матрицу $\mathbf{\Phi}(T)$, а значит, можно задать матрицу, у которой собственные значения будут принадлежать единичному кругу на комплексной плоскости C.

Покажем, что данную систему можно разрешить: 1) выразим из первого уравнения системы $k_0^1\ \left(k_0^0, k_1^1\right)$; 2) подставим k_0^1 в третье уравнение, в нем останутся k_0^0 и k_1^1; 3) из этого уравнения выразим $k_0^0\ \left(k_1^1\right)$; 4) подставим $k_0^0\ \left(k_1^1\right)$ обратно в $k_0^1\ \left(k_0^0, k_1^1\right)$, останется $k_0^1\ \left(k_1^1\right)$; 5) подставим $k_0^1\ \left(k_1^1\right)$ в четвертое уравнение системы, в нем останутся k_1^0 и k_1^1; 6) выразим $k_1^0\left(k_1^1\right)$; 7) подставим $k_0^1\ \left(k_1^1\right)$ и $k_1^0\left(k_1^1\right)$ в третье уравнение системы; 8) выразим k_1^1; 9) так как есть выражения $k_0^0\ \left(k_1^1\right)$, $k_0^1\ \left(k_1^1\right)$, $k_1^0\left(k_1^1\right)$, можно найти k_0^0, k_0^1, k_1^0.

Найдены все составляющие **k**, следовательно, можно подобрать управление, стабилизирующее исходную дискретную систему дифференциальных уравнений.

2. Рассмотрим дискретную систему с выходом $\begin{cases} x^{t+1} = \mathbf{A}^t x^t + \mathbf{Bu}, \\ y = \mathbf{C}x, \end{cases}$ $\mathbf{A}^{t+T} = \mathbf{A}^t$, $t = 0, 1, 2, \ldots$.

Будем выбирать управление по выходу вида $\mathbf{u}^t = -\mathbf{k}y^t$. Тогда $\overline{\mathbf{A}^t} = \left(\mathbf{A}^t - \mathbf{BCk}\right)$. Пусть $T = 2$, k – скаляр. Найдем фундаментальную матрицу по формуле

$$\mathbf{\Phi}(T) = \left[\mathbf{A}^1 - \mathbf{BC}k\right]\left[\mathbf{A}^0 - \mathbf{BC}k\right] = \mathbf{A}^1\mathbf{A}^0 - \mathbf{A}^1\mathbf{BC}k - \mathbf{BC}k\mathbf{A}^0 + \mathbf{BC}k\mathbf{BC}k.$$

То есть необходимо решить квадратное матричное уравнение $k^2\mathbf{Q} + k\mathbf{P} + \mathbf{R} = 0$, где $\mathbf{P} = -(\mathbf{A}^1\mathbf{BC} + \mathbf{BCA}^0)$; $\mathbf{Q} = \mathbf{BCBC}$; $\mathbf{R} = \mathbf{A}^1\mathbf{A}^0 - \mathbf{\Phi}(T)$.

Выпишем подробно каждую матрицу:

$$\mathbf{A}^0 = \begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} c_1 & c_2 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} \Phi_{11} & \Phi_{12} \\ \Phi_{21} & \Phi_{22} \end{bmatrix}.$$

Найдем матрицу $\mathbf{\Phi}(T)$ в явном виде:

$$\mathbf{A}^1\mathbf{A}^0 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}\begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix} = \begin{bmatrix} a_{11}^1a_{11}^0 + a_{12}^1a_{21}^0 & a_{11}^1a_{12}^0 + a_{12}^1a_{22}^0 \\ a_{21}^1a_{11}^0 + a_{22}^1a_{21}^0 & a_{21}^1a_{12}^0 + a_{22}^1a_{22}^0 \end{bmatrix},$$

$$\mathbf{A}^1\mathbf{BC}k = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\begin{bmatrix} c_1k & c_2k \end{bmatrix} = \begin{bmatrix} a_{11}^1b_1 + a_{12}^1b_2 \\ a_{21}^1b_1 + a_{22}^1b_2 \end{bmatrix}\begin{bmatrix} c_1k & c_2k \end{bmatrix} = \begin{bmatrix} a_{11}^1b_1c_1k + a_{12}^1b_2c_1k & a_{11}^1b_1c_2k + a_{12}^1b_2c_2k \\ a_{21}^1b_1c_1k + a_{22}^1b_2c_1k & a_{21}^1b_1c_2k + a_{22}^1b_2c_2k \end{bmatrix},$$

$$\mathbf{BC}k = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\begin{bmatrix} c_1 & c_2 \end{bmatrix}k = \begin{bmatrix} b_1c_1k & b_1c_2k \\ b_2c_1k & b_2c_2k \end{bmatrix},$$

$$\mathbf{BC}k\mathbf{A}^0 = \begin{bmatrix} b_1c_1k & b_1c_2k \\ b_2c_1k & b_2c_2k \end{bmatrix}\begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix} = \begin{bmatrix} b_1c_1ka_{11}^0 + b_1c_2ka_{21}^0 & b_1c_1ka_{12}^0 + b_1c_2ka_{22}^0 \\ b_2c_1ka_{11}^0 + b_2c_2ka_{21}^0 & b_2c_1ka_{12}^0 + b_2c_2ka_{22}^0 \end{bmatrix},$$

$$\mathbf{BC}k\mathbf{BC}k = \begin{bmatrix} b_1c_1kb_1c_1k + b_1c_2kb_2c_1k & b_1c_1kb_1c_2k + b_1c_2kb_2c_2k \\ b_2c_1kb_1c_1k + b_2c_2kb_2c_1k & b_2c_1kb_1c_2k + b_2c_2kb_2c_2k \end{bmatrix},$$

$$\Phi_{11} = a_{11}^1a_{11}^0 + a_{12}^1a_{21}^0 - \left(a_{11}^1b_1c_1 + a_{12}^1b_2c_1 + b_1c_1a_{11}^0 + b_1c_2a_{21}^0\right)\boldsymbol{k} + \left(b_1c_1b_1c_1 + b_1c_2b_2c_1\right)\boldsymbol{kk},$$

$$\Phi_{12} = a_{11}^1a_{12}^0 + a_{12}^1a_{22}^0 - \left(a_{11}^1b_1c_2 + a_{12}^1b_2c_2 + b_1c_1a_{12}^0 + b_1c_2a_{22}^0\right)\boldsymbol{k} + \left(b_1c_1b_1c_2 + b_1c_2b_2c_2\right)\boldsymbol{kk},$$

$$\Phi_{21} = a_{21}^1a_{11}^0 + a_{22}^1a_{21}^0 - \left(a_{21}^1b_1c_1 + a_{22}^1b_2c_1 + b_2c_1a_{11}^0 + b_2c_2a_{21}^0\right)\boldsymbol{k} + \left(b_2c_1b_1c_1 + b_2c_2b_2c_1\right)\boldsymbol{kk},$$

$$\Phi_{22} = a_{21}^1a_{12}^0 + a_{22}^1a_{22}^0 - \left(a_{21}^1b_1c_2 + a_{22}^1b_2c_2 + b_2c_1a_{12}^0 + b_2c_2a_{22}^0\right)\boldsymbol{k} + (b_2c_1b_1c_2 + b_2c_2b_2c_2)\boldsymbol{kk}.$$

Таким образом, чтобы с помощью управления вида $u = -ky$ получить наперед заданную фундаментальную матрицу, необходимо, чтобы все четыре уравнения имели одни и те же корни, что вряд ли возможно разрешить в общем случае.

При решении квадратного матричного уравнения назначается вся матрица $\mathbf{\Phi}(T)$, но для устойчивости системы требуется знать только собственные значения матрицы $\mathbf{\Phi}(T)$. Собственные значения s находятся по формуле $\det(\mathbf{\Phi} - s\mathbf{I}) = s^2 - \mathrm{tr}\mathbf{\Phi}\, s + \det\mathbf{\Phi}$. То есть можно назначить определитель и след матрицы $\mathbf{\Phi}(T)$:

$$\mathrm{tr}\,\mathbf{\Phi} = \Phi_{11} + \Phi_{22} = a_{11}^1 a_{11}^0 + a_{12}^1 a_{21}^0 + a_{21}^1 a_{12}^0 + a_{22}^1 a_{22}^0 -$$
$$-\left(a_{11}^1 b_1 c_1 + a_{12}^1 b_2 c_1 + b_1 c_1 a_{11}^0 + b_1 c_2 a_{21}^0 + a_{21}^1 b_1 c_2 + a_{22}^1 b_2 c_2 + b_2 c_1 a_{12}^0 + b_2 c_2 a_{22}^0\right)\boldsymbol{k} +$$
$$+\left(b_1 c_1 b_1 c_1 + b_1 c_2 b_2 c_1 + b_2 c_1 b_1 c_2 + b_2 c_2 b_2 c_2\right)\boldsymbol{k}\boldsymbol{k},$$
$$\det\mathbf{\Phi} = \Phi_{11}\Phi_{22} - \Phi_{21}\Phi_{12}.$$

Получилась система двух уравнений (квадратного и уравнения четвертой степени). Разрешить такую систему будет проще предыдущей.

3. Рассмотрим такую же дискретную систему с выходом $\begin{cases} x^{t+1} = \mathbf{A}^t x^t + \mathbf{B}\mathbf{u}, \\ y = \mathbf{C}x, \end{cases}$ $\mathbf{A}^{t+T} = \mathbf{A}^t$, $t = 0, 1, 2, \ldots$,

но будем выбирать управление вида $\mathbf{u}^t = -\mathbf{k}^t y^t$.

Тогда $\overline{\mathbf{A}^t} = \left(\mathbf{A}^t - \mathbf{B}\mathbf{C}\mathbf{k}^t\right)$. Пусть период системы $T = 2$, а матрица обратной связи $\mathbf{k}$ периодическая с тем же периодом $T = 2$. Найдем фундаментальную матрицу по формуле

$$\mathbf{\Phi}(T) = \left[\mathbf{A}^1 - \mathbf{B}\mathbf{C}k^1\right]\left[\mathbf{A}^0 - \mathbf{B}\mathbf{C}k^0\right] = \mathbf{A}^1\mathbf{A}^0 - \mathbf{A}^1\mathbf{B}\mathbf{C}k^0 - \mathbf{B}\mathbf{C}k^1\mathbf{A}^0 + \mathbf{B}\mathbf{C}k^1\mathbf{B}\mathbf{C}k^0.$$

Выпишем подробно каждую матрицу:

$$\mathbf{A}^0 = \begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} c_1 & c_2 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} \Phi_{11} & \Phi_{12} \\ \Phi_{21} & \Phi_{22} \end{bmatrix}.$$

Найдем матрицу $\mathbf{\Phi}(T)$ в явном виде:

$$\mathbf{A}^1\mathbf{A}^0 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}\begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix} = \begin{bmatrix} a_{11}^1 a_{11}^0 + a_{12}^1 a_{21}^0 & a_{11}^1 a_{12}^0 + a_{12}^1 a_{22}^0 \\ a_{21}^1 a_{11}^0 + a_{22}^1 a_{21}^0 & a_{21}^1 a_{12}^0 + a_{22}^1 a_{22}^0 \end{bmatrix},$$
$$\mathbf{A}^1\mathbf{B}\mathbf{C}k^0 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\begin{bmatrix} c_1 k^0 & c_2 k^0 \end{bmatrix} = \begin{bmatrix} a_{11}^1 b_1 + a_{12}^1 b_2 \\ a_{21}^1 b_1 + a_{22}^1 b_2 \end{bmatrix}\begin{bmatrix} c_1 k^0 & c_2 k^0 \end{bmatrix} = \begin{bmatrix} a_{11}^1 b_1 c_1 + a_{12}^1 b_2 c_1 & a_{11}^1 b_1 c_2 + a_{12}^1 b_2 c_2 \\ a_{21}^1 b_1 c_1 + a_{22}^1 b_2 c_1 & a_{21}^1 b_1 c_2 + a_{22}^1 b_2 c_2 \end{bmatrix} k^0,$$
$$\mathbf{B}\mathbf{C}k^1 = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\begin{bmatrix} c_1 & c_2 \end{bmatrix}k^1 = \begin{bmatrix} b_1 c_1 & b_1 c_2 \\ b_2 c_1 & b_2 c_2 \end{bmatrix}k^1,$$
$$\mathbf{B}\mathbf{C}k^1\mathbf{A}^0 = \begin{bmatrix} b_1 c_1 & b_1 c_2 \\ b_2 c_1 & b_2 c_2 \end{bmatrix}\begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix}k^1 = \begin{bmatrix} b_1 c_1 a_{11}^0 + b_1 c_2 a_{21}^0 & b_1 c_1 a_{12}^0 + b_1 c_2 a_{22}^0 \\ b_2 c_1 a_{11}^0 + b_2 c_2 a_{21}^0 & b_2 c_1 a_{12}^0 + b_2 c_2 a_{22}^0 \end{bmatrix}k^1,$$
$$\mathbf{B}\mathbf{C}k^1\mathbf{B}\mathbf{C}k^0 = \begin{bmatrix} b_1 c_1 b_1 c_1 + b_1 c_2 b_2 c_1 & b_1 c_1 b_1 c_2 + b_1 c_2 b_2 c_2 \\ b_2 c_1 b_1 c_1 + b_2 c_2 b_2 c_1 & b_2 c_1 b_1 c_2 + b_2 c_2 b_2 c_2 \end{bmatrix}k^1 k^0,$$
$$\Phi_{11} = a_{11}^1 a_{11}^0 + a_{12}^1 a_{21}^0 - \left(a_{11}^1 b_1 c_1 + a_{12}^1 b_2 c_1\right)\boldsymbol{k}^0 - \left(b_1 c_1 a_{11}^0 + b_1 c_2 a_{21}^0\right)\boldsymbol{k}^1 + \left(b_1 c_1 b_1 c_1 + b_1 c_2 b_2 c_1\right)\boldsymbol{k}^1\boldsymbol{k}^0,$$
$$\Phi_{12} = a_{11}^1 a_{12}^0 + a_{12}^1 a_{22}^0 - \left(a_{11}^1 b_1 c_2 + a_{12}^1 b_2 c_2\right)\boldsymbol{k}^0 - \left(b_1 c_1 a_{12}^0 + b_1 c_2 a_{22}^0\right)\boldsymbol{k}^1 + \left(b_1 c_1 b_1 c_2 + b_1 c_2 b_2 c_2\right)\boldsymbol{k}^1\boldsymbol{k}^0,$$
$$\Phi_{21} = a_{21}^1 a_{11}^0 + a_{22}^1 a_{21}^0 - \left(a_{21}^1 b_1 c_1 + a_{22}^1 b_2 c_1\right)\boldsymbol{k}^0 - \left(b_2 c_1 a_{11}^0 + b_2 c_2 a_{21}^0\right)\boldsymbol{k}^1 + \left(b_2 c_1 b_1 c_1 + b_2 c_2 b_2 c_1\right)\boldsymbol{k}^1\boldsymbol{k}^0,$$
$$\Phi_{22} = a_{21}^1 a_{12}^0 + a_{22}^1 a_{22}^0 - \left(a_{21}^1 b_1 c_2 + a_{22}^1 b_2 c_2\right)\boldsymbol{k}^0 - \left(b_2 c_1 a_{12}^0 + b_2 c_2 a_{22}^0\right)\boldsymbol{k}^1 + (b_2 c_1 b_1 c_2 + b_2 c_2 b_2 c_2)\boldsymbol{k}^1\boldsymbol{k}^0.$$

Получилась система из четырех уравнений с двумя неизвестными. Такая система лучше, чем система из четырех уравнений с одним неизвестным, но и она довольно сложна. Попробуем не назначать всю матрицу $\mathbf{\Phi}(T)$, а назначить только ее спектр. Для этого, как и предыдущем случае, назначим определитель и след матрицы $\mathbf{\Phi}(T)$:

$$\operatorname{tr}\mathbf{\Phi} = \Phi_{11} + \Phi_{22} = a_{11}^1 a_{11}^0 + a_{12}^1 a_{21}^0 + a_{21}^1 a_{12}^0 + a_{22}^1 a_{22}^0 -$$
$$-\left(a_{11}^1 b_1 c_1 + a_{12}^1 b_2 c_1 + a_{21}^1 b_1 c_2 + a_{22}^1 b_2 c_2\right)\boldsymbol{k}^0 - \left(b_1 c_1 a_{11}^0 + b_1 c_2 a_{21}^0 + b_2 c_1 a_{12}^0 + b_2 c_2 a_{22}^0\right)\boldsymbol{k}^1 +$$
$$+\left(b_1 c_1 b_1 c_1 + b_1 c_2 b_2 c_1 + b_2 c_1 b_1 c_2 + b_2 c_2 b_2 c_2\right)\boldsymbol{k}^1\boldsymbol{k}^0,$$
$$\det\mathbf{\Phi} = \Phi_{11}\Phi_{22} - \Phi_{21}\Phi_{12}.$$

Тогда получается система из двух уравнений с двумя неизвестными, что уже намного проще разрешить.

4. Рассмотрим еще один более интересный случай. Остается та же система с выходом

$$\begin{cases} x^{t+1} = \mathbf{A}^t x^t + \mathbf{B}\mathbf{u}, \\ y = \mathbf{C}x, \end{cases} \quad \mathbf{A}^{t+T} = \mathbf{A}^t,\ T = 1, 2, \ldots,\ \ t = 0, 1, 2, \ldots.$$

Будем выбирать управление вида $\mathbf{u}^t = -\mathbf{k}^t y^t$. Тогда $\overline{A^t} = \left(A^t - BCk^t\right)$. Пусть период системы $T_1 = 2$, а вот матрицу обратной связи $\mathbf{k}$ будем выбирать периодической с удвоенным периодом $T_2 = 4$. Тогда общий период станет равным $T = 4$. Найдем фундаментальную матрицу:

$$\mathbf{\Phi}(T) = \left[\mathbf{A}^1 - \mathbf{B}\mathbf{C}k^3\right]\left[\mathbf{A}^0 - \mathbf{B}\mathbf{C}k^2\right]\left[\mathbf{A}^1 - \mathbf{B}\mathbf{C}k^1\right]\left[\mathbf{A}^0 - \mathbf{B}\mathbf{C}k^0\right].$$

После раскрытия скобок получится система из четырех уравнений с четырьмя неизвестными. Это значит, что в этом случае возможно будет назначить не только спектр, но и всю матрицу $\mathbf{\Phi}(T)$.

Таким образом, анализ простых примеров показывает, что для управления спектром дискретной системы порядка n в общем случае желательно, чтобы период замкнутой системы был не меньше n. Если T, период матрицы $\mathbf{A}$, меньше n, то можно выбрать период управления кратным T, то есть $T_1 = pT$, при этом новый период должен быть не меньше размерности системы.

Моделирование

В предыдущем разделе рассматривалась стабилизация четырех простых дискретных систем. Для каждой из них находилось управление из условия наперед заданной фундаментальной матрицы $\mathbf{\Phi}(T)$ или ее спектра. Аналитически решить полученные уравнения сложно, но их можно решать численно, что важно при практическом применении указанного подхода. С помощью средств MATLAB найдем коэффициенты k управления каждой системы. Для этого напишем функции для решения систем нелинейных уравнений, полученных в предыдущем разделе, и найдем управления для конкретных примеров.

1. Системы второго порядка при $T = 2$, $\mathbf{u}^t = -\mathbf{k}^t x^t$, размерность матриц 2×2. Система имеет вид $x^{t+1} = \overline{\mathbf{A}^t} x^t$, где $\overline{\mathbf{A}^t} = \left(\mathbf{A}^t - \mathbf{B}\mathbf{k}^t\right)$.

$$\mathbf{\Phi}(T) = \left[\mathbf{A}^1 - \mathbf{B}\mathbf{k}^1\right]\left[\mathbf{A}^0 - \mathbf{B}\mathbf{k}^0\right] = \mathbf{A}^1\mathbf{A}^0 - \mathbf{A}^1\mathbf{B}\mathbf{k}^0 - \mathbf{B}\mathbf{k}^1\mathbf{A}^0 + \mathbf{B}\mathbf{k}^1\mathbf{B}\mathbf{k}^0.$$

Из этого уравнения найдем все коэффициенты $\mathbf{k}$ при

$$\mathbf{A}^0 = \begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \mathbf{k}^0 = \begin{bmatrix} k_0^0 & k_1^0 \end{bmatrix}, \mathbf{k}^1 = \begin{bmatrix} k_0^1 & k_1^1 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} \Phi_{11} & \Phi_{12} \\ \Phi_{21} & \Phi_{22} \end{bmatrix}.$$

Возьмем конкретный пример:

$$\mathbf{A}^0 = \begin{bmatrix} 5 & 1 \\ 6 & 1 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} 7 & 3 \\ 1 & 5 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \mathbf{k}^0 = \begin{bmatrix} k_0^0 & k_1^0 \end{bmatrix}, \mathbf{k}^1 = \begin{bmatrix} k_0^1 & k_1^1 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} 0{,}5 & 0{,}01 \\ 0{,}1 & 0{,}5 \end{bmatrix}.$$

Численно были получены коэффициенты обратной связи $k_0^0 = 2{,}506$; $k_1^0 = 2{,}262$; $k_0^1 = 0{,}542$; $k_1^1 = 1{,}674$.

2. Система с выходом $\begin{cases} x^{t+1} = \mathbf{A}^t x^t + \mathbf{B}\mathbf{u}, \\ y = \mathbf{C}x, \end{cases}$ $\mathbf{A}^{t+T} = \mathbf{A}^t$, $t = 0, 1, 2, \ldots$.

Управление вида $u^t = -ky^t$, $T = 2$, k – скаляр.

$$\mathbf{\Phi}(T) = \left[\mathbf{A}^1 - \mathbf{BC}k\right]\left[\mathbf{A}^0 - \mathbf{BC}k\right] = \mathbf{A}^1\mathbf{A}^0 - \mathbf{A}^1\mathbf{BC}k - \mathbf{BC}k\mathbf{A}^0 + \mathbf{BC}k\mathbf{BC}k,$$

$$\operatorname{tr}\mathbf{\Phi} = \Phi_{11} + \Phi_{22}, \ \det\mathbf{\Phi} = \Phi_{11}\Phi_{22} - \Phi_{21}\Phi_{12},$$

$$\mathbf{A}^0 = \begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} c_1 & c_2 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} \Phi_{11} & \Phi_{12} \\ \Phi_{21} & \Phi_{22} \end{bmatrix}.$$

Возьмем конкретный пример: $\mathbf{A}^0 = \begin{bmatrix} 5 & 1 \\ 6 & 1 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} 7 & 3 \\ 1 & 5 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 4 & 5 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} 0{,}5 & 0{,}01 \\ 0{,}1 & 0{,}5 \end{bmatrix}$.

В этом случае решений не оказалось.

Для другого примера $\mathbf{A}^0 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 1 & 1 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} 0{,}1 & 0 \\ 0 & 0 \end{bmatrix}$ коэффициенты обратной связи были найдены: $k = 1{,}158$ или $k = 0{,}8419$.

Таким образом, получаемые системы нелинейных уравнений не всегда имеют решение, или решение может быть не единственное. То есть не всегда возможно подобрать стабилизирующее управление.

3. Рассмотрим систему с выходом $\begin{cases} x^{t+1} = \mathbf{A}^t x^t + \mathbf{B}\mathbf{u}, \\ y = \mathbf{C}x. \end{cases}$

Управление вида $\mathbf{u}^t = -\mathbf{k}^t y^t$. Тогда $\overline{\mathbf{A}^t} = \left(\mathbf{A}^t - \mathbf{BC}\mathbf{k}^t\right)$. Период системы $T = 2$, $\mathbf{k}$ – периодическая матрица с периодом $T = 2$.

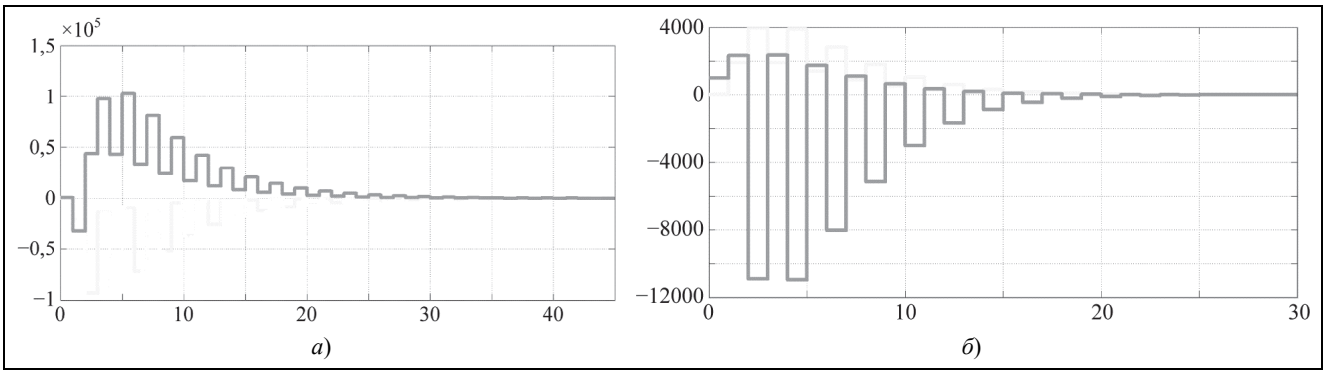
$$\mathbf{\Phi}(T) = \left[\mathbf{A}^1 - \mathbf{BC}k^1\right]\left[\mathbf{A}^0 - \mathbf{BC}k^0\right] = \mathbf{A}^1\mathbf{A}^0 - \mathbf{A}^1\mathbf{BC}k^0 - \mathbf{BC}k^1\mathbf{A}^0 + \mathbf{BC}k^1\mathbf{BC}k^0,$$

$$\mathbf{A}^0 = \begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} c_1 & c_2 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} \Phi_{11} & \Phi_{12} \\ \Phi_{21} & \Phi_{22} \end{bmatrix}.$$

Возьмем конкретный пример: $\mathbf{A}^0 = \begin{bmatrix} 5 & 1 \\ 6 & 1 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} 7 & 3 \\ 1 & 5 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 4 & 5 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} 0{,}5 & 0{,}01 \\ 0{,}1 & 0{,}5 \end{bmatrix}$.

Для периодического управления были найдены две пары решений: $k^0 = 3{,}667$ и $k^1 = 0{,}5425$; $k^0 = -0{,}14$ и $k^1 = 0{,}7562$.

Построим графики для этого примера. Система выдает два решения. Посмотрим, как ведет себя система с начальными условиями (10, 1000) при найденных коэффициентах управления. На рисунке видно, что система стабилизируется найденным управлением.



Графики поведения системы для $k^0 = 3{,}667$, $k^1 = 0{,}5425$ (*а*) и для $k^0 = -0{,}14$, $k^1 = 0{,}7562$ (*б*)

4. Система с выходом $\begin{cases} x^{t+1} = \mathbf{A}^t x^t + \mathbf{B}\mathbf{u}, \\ y = \mathbf{C}x. \end{cases}$

Управление вида $\mathbf{u}^t = -\mathbf{k}^t y^t$. Период системы $T_1 = 2$, $\mathbf{k}$ с периодом $T_2 = 4$. Общий период $T = 4$.

$$\mathbf{\Phi}(T) = \left[\mathbf{A}^1 - \mathbf{B}\mathbf{C}k^3\right]\left[\mathbf{A}^0 - \mathbf{B}\mathbf{C}k^2\right]\left[\mathbf{A}^1 - \mathbf{B}\mathbf{C}k^1\right]\left[\mathbf{A}^0 - \mathbf{B}\mathbf{C}k^0\right],$$

$$\mathbf{A}^0 = \begin{bmatrix} a_{11}^0 & a_{12}^0 \\ a_{21}^0 & a_{22}^0 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} a_{11}^1 & a_{12}^1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} c_1 & c_2 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} \Phi_{11} & \Phi_{12} \\ \Phi_{21} & \Phi_{22} \end{bmatrix}.$$

Возьмем конкретный пример: $\mathbf{A}^0 = \begin{bmatrix} 5 & 1 \\ 6 & 1 \end{bmatrix}, \mathbf{A}^1 = \begin{bmatrix} 7 & 3 \\ 1 & 5 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 2 & 3 \end{bmatrix}, \mathbf{\Phi}(T) = \begin{bmatrix} 0{,}5 & 0{,}01 \\ 0{,}1 & 0{,}5 \end{bmatrix}$.

Для управления с удвоенным периодом также были найдены два решения:
$k^0 = 118{,}1$, $k^1 = 0{,}542$, $k^2 = 3{,}804$, $k^3 = 0{,}5424$;
$k^0 = -0{,}148$, $k^1 = 0{,}7638$, $k^2 = -0{,}1487$, $k^3 = 0{,}763$.

- Проведенное моделирование показало практическую реализуемость предложенных подходов к стабилизации дискретных систем с периодическими коэффициентами. В то же время при такой реализации возникают сложности, связанные с возможной неразрешимостью полученных систем уравнений (получить условия разрешимости системы нелинейных уравнений очень сложно).

Работа выполнена по теме (проекту) 0071-2014-0019 «Синтез систем управления с учетом специфики современных средств автоматизации».

Литература

1. *Г. Д'Анжело* Линейные системы с переменными параметрами. Анализ и синтез. М.: Машиностроение. 1974. 288 с.
2. *Ким Д.П.* Теория автоматического управления. Т. 2. Многомерные, нелинейные, оптимальные и адаптивные системы. М.: Физматлит. 2004. 464 с.
3. *Гайшун И.В.* Введение в теорию линейных нестационарных систем. М.: Эдиториал УРСС. 2010. 408 с.
4. *Андреев Ю.Н.* Управление конечномерными линейными объектами. М.: Наука. 1976. 424 с.

Поступила 12 декабря 2017 г.

Approaches to stabilization of systems with periodic coefficients

V.V. Fomichev – Dr. Sc. (Phys.-Math.), Main Research Scientist, Center of Information Technologies in Design (Odintsovo, Moscow region)
E-mail: fomichev@cs.msu.ru

In article, the problem of stabilizing of one of subclasses of non-stationary linear management systems is considered. Systems with periodic coefficients are considered. In article there are studied as the general questions of the analysis of stability of such systems, and algorithms of creation of stabilizing feedback coupling. In particular, stabilizing algorithms for the discrete systems are received. It is shown that for stabilizing of system it is required to solve the system of the polynomial equations, at the same time the number of variables can be increased due to increase in the period of control in comparison with the period of the system. The simulations demonstrated the practical feasibility of the proposed approaches to the stabilization of discrete systems with periodic coefficients.

References

1. *G. D'Anzhelo* Linejny'e sistemy' s peremenny'mi parametrami. Analiz i sintez. M.: Mashinostroenie. 1974. 288 s.
2. *Kim D.P.* Teoriya avtomaticheskogo upravleniya. T. 2. Mnogomerny'e, nelinejny'e, optimal'ny'e i adaptivny'e sistemy'. M.: Fizmatlit. 2004. 464 s.
3. *Gajshun I.V.* Vvedenie v teoriyu linejny'x nestaczionarny'x sistem. M.: E'ditorial URSS. 2010. 408 s.
4. *Andreev Yu.N.* Upravlenie konechnomerny'mi linejny'mi ob^ektami. M.: Nauka. 1976. 424 s.

УДК 621

Результаты анализа перспектив развития геоинформационных систем

А.В. Воронин – к.т.н., доцент, вед. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: aleksey.v.v@mail.ru

Рассмотрены геоинформационные системы (ГИС), которые развиваются в направлении использования технологии клиент-сервер, специализированных расширений для распространенных SQL-серверов, решений на основе WEB-браузеров, открытых форматов и кодов программ, реализуя распределенные и интеллектуальные ГИС. Показано, что перспектива развития ГИС – «умные» специализированные ГИС – ИГИС для качественного решения задач управления в специализированной сфере деятельности.

Ключевые слова: *геоинформационные системы, ГИС, трансформация, визуализация, анализ, ИГИС, метод, способ.*

Geoinformation systems are developed in the direction of client-server technologies, specialized extensions for commonly used SQL-servers, WEB-browser decisions, open formats and instruction (program) codes, realizing distributed and intelligent geoinformation systems. Perspective of GIS development is eveation of intelligent GIS – IGIS for a qualitative problem of management solving in the specialized sphere.

Keywords: *geoinformation systems, GIS, transformation, visualization, analysis, IGIS, method, means.*

Качественное решение задач практически всех направлений жизнедеятельности человека на современном этапе осуществляется посредством использования центров управления (принятия решений – ситуационных центров), одним из центральных элементов которых является геоинформационная система (ГИС).

Применение ГИС обусловлено возможностью наглядного восприятия геообъектов по их управлению и контролю. Анализ системных связей, закономерностей функционирования и развития ГИС дает возможность определения функционала ГИС по анализу, трансформации и визуализации данных.

Ц е л ь р а б о т ы – определить теоретические основы, методы, способы и алгоритмическое обеспечение анализа, трансформации и визуализации информации на основе компьютерных технологий в ретроспективе развития ГИС и соответствия динамики развития современного инфокоммуникационного мира.

Перспективы развития геоинформационных систем

В документах OGC и OSGeo [1, 2] ГИС определяется как компьютерная система для сбора, хранения, проверки, интеграции, управления, анализа и отображения данных применительно к их расположению на поверхности Земли.

В работах С.П Присяжнюка, В.Н. Филатова, Федоненкова [3, 6, 7] под ГИС понимают автоматизированную систему, предназначенную для обработки пространственно-временных данных, которые позволяют расширить знания о каком-либо явлении или предмете (объекте) реального мира, при этом основой их интеграции служит географическая информация.

Автоматизированная система [3] – система, состоящая из персонала и комплекса средств автоматизации деятельности, реализующая информационную технологию выполнения установленных функций ГИС.

С точки зрения выполнения основных функций в [3] дается определение ГИС как автоматизированной системы, предназначенной для сбора, обработки, анализа, моделирования и отображения данных, а также решения информационных и расчетных задач с использованием цифровой картографической, аналоговой и текстовой информации. Данное определение созвучно с определением OGC и OSGeo.

В работах Р.М. Юсупова, В.В. Поповича, Л.С. Бернштейна, И.Н. Розенберга, С.Л. Белякова [4, 5] определение ГИС рассматривается в *широком* и *узком смыслах*: в *широком* – это система сбора, хранения, анализа и графической визуализации пространственных данных и связанной с ними информации; в *узком* – это инструмент (программный продукт), позволяющий пользователям анализировать и редактировать цифровые карты, а также дополнительную информацию об объектах.

Как видно из данных определений, ГИС – это система, реализующая информационную технологию по выполнению установленных функций ГИС: ввода, контроля целостности и хранения данных, преобразования форматов, разграничения прав доступа, выполнения геоинформационных задач, отображения

геоданных и результатов анализа данных.

Ретроспектива развития ГИС неразрывно связана с развитием информационной технологии. Рассмотрим ГИС иностранного и отечественного производства, динамично развивающиеся и представленные на рынке геоуслуг.

В [6, 7] предложена классификация ГИС по пространственной характеристике, региональной принадлежности, форме представления геоданных, используемым аппаратным средствам и области применения. Однако центральный элемент – реализуемый функционал (основные функции) – не рассматривался. Проанализируем технологии хранения данных и организации их взаимодействия, позволяющие не только предложить следующую классификацию ГИС, но и выявить достоинства и недостатки ГИС в ретроспективе их развития.

1. ГИС, состоящие из одной или нескольких программ. Данные системы просты в реализации и эксплуатации, но имеются ограничения при совместном использовании геоданных в компьютерной сети (поддерживаются, как правило, функции сетевой операционной системы). Достоинства и недостатки по используемым средствам анализа данных, их трансформации и визуализации представлены в табл. 1.

Таблица 1. ***Достоинства и недостатки ГИС, состоящих из одной или нескольких программ***

Функции ГИС	Достоинства	Недостатки
Анализ данных	Реализация уникальных алгоритмов обработки геоданных	Отсутствие возможности самостоятельной разработки уникальных алгоритмов обработки геоданных
Трансформация данных	Простая трансформация ввиду использования собственных форматов данных	Несовместимость с форматами данных других ГИС
Визуализация данных	Высокое быстродействие	–

2. ГИС, функционирующие с использованием технологии клиент-сервер. Системы предполагают наличие выделенного в сети сервера геоданных, однако его функциональность, как правило, ограничена. Сложность в эксплуатации систем требует наличия квалифицированного персонала. Достоинства и недостатки по используемым средствам анализа данных, их трансформации и визуализации представлены в табл. 2.

Таблица 2. ***Достоинства и недостатки ГИС, функционирующих с использованием технологии клиент-сервер***

Функции ГИС	Достоинства	Недостатки
Анализ данных	Реализация уникальных алгоритмов обработки геоданных	Отсутствие возможности самостоятельной разработки уникальных алгоритмов обработки геоданных
Трансформация данных	Простая трансформация в виду использования собственных форматов данных	Несовместимость с форматами данных других ГИС
Визуализация данных	Высокое быстродействие	–

3. ГИС, функционирующие с использованием технологии клиент-сервер и хранящие данные с использованием одной из распространенных систем управления базами данных (Microsoft SQL Server, Oracle, My SQL, Postgre SQL). Системы ориентированы на использование внешней СУБД и современных средств работы с ней. Следовательно, сложность в эксплуатации систем (необходимы настройки ГИС, СУБД) требует наличия квалифицированного персонала. Достоинства и недостатки по используемым средствам анализа данных, их трансформации и визуализации представлены в табл. 3.

Таблица 3. ***Достоинства и недостатки ГИС, функционирующих с использованием технологии клиент-сервер и хранящие данные с использованием одной из распространенных систем управления базами данных***

Функции ГИС	Достоинства	Недостатки
Анализ данных	–	Наличие ограничений на знание внутренней структуры СУБД
Трансформация данных	Простая трансформация в виду использования собственных форматов данных	Наличие ограничений с форматами данных других ГИС. Наличие ограничений на знание внутренней структуры СУБД
Визуализация данных	–	Снижение быстродействия ввиду необходимости передачи больших объемов данных по сети

4. ГИС, функционирующие с использованием технологии клиент-сервер и использующие в качестве хранилища геоданных специализированные расширения SQL-сервера (Oracle Locator/Spatial для Oracle SQL Server, Microsoft Spatial для Microsoft SQL Server, Post GIS для PostgreSQL). В рамках технологии предложены решения, реализующие распределенные ГИС (одно хранилище – несколько ГИС) и использующие WEB-браузер в качестве рабочего места пользователя. Системы предполагают использование программного обеспечения сторонних разработчиков (включая свободно распространяемого и распространяемого с открытым исходным кодом). Сложность в эксплуатации систем (необходимы настройки ГИС, СУБД) требует наличия квалифицированного персонала. Достоинства и недостатки по используемым средствам анализа данных, их трансформации и визуализации представлены в табл. 4.

Таблица 4. ***Достоинства и недостатки ГИС, функционирующих с использованием технологии клиент-сервер и использующие в качестве хранилища геоданных специализированные расширения SQL-сервера***

Функции ГИС	Достоинства	Недостатки
Анализ данных	Независимость структуры хранения геоданных от разработчика ГИС	–
Трансформация данных	Интеграция форматов геоданных различных ГИС	–
Визуализация данных	Возможность использования произвольного браузера при решении на базе WEB-технологии	Снижение быстродействия при решении на базе WEB-технологии

Недостаточность развития отечественных ГИС в вопросах анализа, трансформации и визуализации данных, а также санкционная политика стран Запада против РФ формируют особенность современной ситуации развития инфокоммуникационной отрасли в стране. Как следствие, требуется разработка методов и способов функционирования ГИС по анализу, трансформации и визуализации данных в отрасли. Проведем анализ методов и способов анализа, трансформации и визуализации данных, применяемых в ГИС.

Анализ методов и способов анализа, трансформации и визуализации данных, применяемых в геоинформационных системах

Под *методом* понимают единое решение задач определенного класса или способ теоретического исследования. *Способ* – действия или система действий, применяемых при исполнении работы (решении задачи).

Сводные данные по применяемым в ГИС методах и способах по анализу, трансформации, визуализации данных представлены в табл. 5−7.

При *анализе данных* в ГИС рассматриваются рассчитываемые параметры статистических характеристик выборных объектов. При этом рассчитываются: значения минимума, максимума, суммы, среднего значения данных характеристик рассматриваемых объектов.

Таблица 5. ***Методы и способы по анализу данных***

Методы	Способы
1. Регрессионный. 2. Оверлейный. 3. Элементов теории графов (сетевой). 4. С помощью искусственных нейронных сетей	1. С учетом отображения на карте и: с учетом пространственного расположения объекта; без учета пространственного расположения объекта; с расчетом плотности отображаемых геоданных на картографическом сегменте. 2. Без учета отображения на карте. 3. «Из-в», «из-через».

В ГИС применяются следующие основные методы анализа геоданных (табл. 5): регрессионный; оверлейный; сетевой; нейросетевой.

Сущность *регрессионного метода* заключается в представлении результатов анализа показателей в виде графика (диаграммы) распределения, таблицы статистических характеристик регрессии, коэффициентов корреляции. Также генерируются случайные гипотетические показатели на основе статистических моделей распределения с заданным параметром. По результатам анализа возможны: построение модели поверхности тренда на растровом изображении; расчет среднего центра для множества точек изображения; генерирование векторного файла в соответствии с выбранной схемой пространственного отбора.

Оверлейный метод основан на наложении разноименных картографических слоев и создании объектов, возникающих при их геометрическом наложении. Атрибутивная информация исходных объектов наследуется производными объектами. Используются полигональные, точечные и линейные объекты.

Цифровая обработка оверлейных операций обеспечивает нахождение ошибок геоизображения для заданной точности. Операция осуществляется, как правило, двумя слоями, реже – несколькими.

Метод элементов теории графов (сетевой метод) реализует обработку данных природного и антропогенного происхождения (реки, дороги, коммуникационные сооружения). Метод применяется при изучении топологических свойств объектов и территорий.

Метод с помощью искусственных нейронных сетей заключается в построении эмпирической зависимости без привлечения дополнительной информации для заполнения пропусков в таблице данных.

В ГИС применяются следующие основные способы анализа геоданных (табл. 5): с учетом отображения на карте и с учетом пространственного расположения объекта, без учета пространственного расположения объекта, с расчетом плотности отображаемых геоданных на картографическом сегменте; без учета отображения на карте; «из-в», «из-через».

Способы реализации методов анализа геоданных относятся к решению специализированных задач анализа. Перечисленные способы (*с учетом (без) отображения на карте* – например, районирование, типология) формализуются в задаче построения отношений на множестве объектов и построения функции по конечному набору значений.

Способы *«из-в»* и *«из-через»* реализуют метод сетевого анализа данных. Сеть – набор линий, которые имеют не более двух точек касания с другими линиями: начало, конец. Способы соединения элементов сети определяют способы анализа данных: «из-в» – соединение объекта *A* с объектом *B*; «из-через» – соединение объекта *A* через объект *C* с объектом *B*.

Под *трансформацией данных* в ГИС понимаются операции ротации геообъектов (пересчета координат пространственных объектов при их повороте, сдвиге, масштабировании осей).

Таблица 6. ***Методы и способы по трансформации данных***

Методы	Способы
1. Аффинного преобразования с применением линейного или квадратичного полинома. 2. «Резиновой» трансформации	1. Удаления (добавления) тематических слоев. 2. Удаления (добавления) элементов слоя. 3. Изменения тематического содержания с помощью генерализации данных. 4. Замены отображения тематического содержания. 5. Построения анаморфированных изображений. 6. Перехода к динамическому картографическому изображению

В ГИС применяются следующие основные методы трансформации геоданных (табл. 6): аффинного преобразования с применением линейного или квадратичного полинома; «резиновой» трансформации.

Метод *аффинного преобразования с применением линейного или квадратичного полинома* применяется при трансформации растра. Использование квадратичного полинома дает результат преобразования точнее, чем при использовании линейного полинома.

Метод *«резиновой» трансформации* заключается в том, что вместе с передвигаемым узлом сдвигаются или трансформируются все объекты в ближайшей окрестности. Такой метод применим в пределах одного покрытия.

Основные способы, реализующие методы трансформации (табл. 6): удаления (добавления) тематических слоев; удаления (добавления) элементов слоя; изменения тематического содержания с помощью генерализации данных; замены отображения тематического содержания; построения анаморфированных изображений; перехода к динамическому картографическому изображению.

Удаление или добавление тематического слоя (элемента слоя) являются простейшими способами трансформации данных.

Изменение тематического содержания приемами генерализации реализуется через утрирование, обобщение, упрощение, сглаживание, например, цветового решения карты.

Замена отображения тематического содержания является картографическим способом трансформации данных (например, замена точечного представления на ареал).

Построение анаморфированных изображений представляет собой формирование картоподобных изображений.

Использование динамического картографического изображения осуществляется посредством применения интерактивной мультипликации.

Под *визуализацией данных* понимается графическое воспроизведение, отображение, генерация изображений (в том числе картографических) и иной графики на устройствах отображения данных (экране монитора). В основе лежат преобразования исходных цифровых данных с помощью специальных алгоритмов, сокращающих размерность их описания до двух измерений. Данные изображаются в виде точек на плоскости монитора. Главная задача, решаемая при визуализации, – сохранение существенной части закономерностей, присущих геоданным. Это позволяет наглядно представить исходный набор многомерных данных и сделать вывод об их распределении.

Таблица 7. ***Методы и способы по визуализации данных***

Методы	Способы
1. Классические (например, максимума правдоподобия, вложения в многомерное пространство двумерного многообразия). 2. Комбинированные. 3. Альтернативные	1. В виде числовых значений. 2. В виде таблиц (включая атрибуты объектов). 3. Медиа (фото-, видеоизображения, анимация). 4. В виде графики: размерных символов (значков); качественного (для количественных данных) фона; точек; столбчатых и круговых локализованных диаграмм; изолиний.

В ГИС применяются следующие основные методы визуализации геоданных [8] (табл. 7): классические (например, максимума правдоподобия или вложения в многомерное пространство двумерного многообразия); комбинированные; альтернативные.

Метод вложения в многомерное пространство двумерного многообразия заключается в построении вложенного в многомерное пространство данных двумерного многообразия, которое моделирует или аппроксимирует данные (визуализирует данные в виде статической или подвижной карты). Каждому объекту из набора данных сопоставляется в соответствие пара координат, характеризующих положение образа на двумерной карте.

Альтернативный метод [9] – визуализация картографических изображений в рамках веб-ориентированных ГИС, предполагающий реализацию функциональных возможностей на клиентской или серверной сторонах веб-приложения, с использованием элемента canvas HTML5, технологий Adobe Flash и SVG.

Комбинированный метод является развитием методов генерации электронных карт и предполагает сочетание основных преимуществ классических и альтернативных методов визуализации [9].

В ГИС применяются следующие основные способы визуализации геоданных [8] (табл. 7): в виде числовых значений; в виде таблиц (включая атрибуты объектов); медиа (фото-, видеоизображения, анимация); в виде графики – размерных символов (значков), качественного (для количественных данных) фона, точек, столбчатых и круговых локализованных диаграмм, изолиний.

Отображение в ГИС данных *в виде числовых значений* (*чисел, таблиц чисел*) реализует простейший способ визуализации данных, атрибутов и результатов их анализа.

Использование *фото-, видеоизображений и анимации* предполагает реализацию способа визуализации с помощью проигрывателей медиаданных.

Визуализация графики при *способе размерных символов* использует в качестве представления анализируемых характеристик объектов отображения специальных символов, размер которых передает количественную информацию, а форма и цвет – качественную.

В случае группировки данных применим *способ качественного фона* – присвоение определенного цвета каждой группе данных.

При *точечном способе* изобразительным средством является множество точек одинакового размера, каждая из которых имеет значение количественного показателя.

Столбчатые и круговые локализованные диаграммы позволяют отобразить соотношение нескольких характеристик. Диаграммы при этом имеют географическую привязку.

Способ изолиний, отображая различные показатели, формирует карты изотерм, изобар, изокоррелят и др. С помощью изолиний выделяются территории, характеризующиеся одинаковыми свойствами

(например, температуры). При этом различаются истинные изолинии (непрерывное изменение показателя) и псевдоизолинии (дискретное изменение показателя). Для представления применяются линии разных типов, толщины и цвета.

Проведенный анализ позволяет рассмотреть развитие ГИС только с одной стороны – как компьютеризацию средств картографии отечественного и импортного производства. С другой стороны, применение известных и хорошо апробированных алгоритмов функционирования ГИС, разработанных иностранными производителями, крайне ограничено, а именно: производители не поставляют или ограничивают функциональность средств аналитической обработки информации или данных при решении широкого круга задач.

Наличие противоречия выступает как следствие недостаточной проработанности вопросов анализа гео- и информации, необходимости разработки отечественных методов и способов анализа, трансформации и визуализации данных для синтеза управленческих решений.

Требуется повышение функциональности ГИС, придание ей новых свойств, а также расширение хранилища данных, приводящее к необходимости увеличения ресурса сил и средств системы. Большой объем разнородной телекоммуникационной информации дополнительно формирует необходимость разработки специализированных методов и способ анализа и обработки данных (например, формирование слоя специализированных геоданных) как составной подзадачи задачи синтеза управляющих решений.

Трансформация данных уже необходима не только для операций ротации геообъектов, но и для формирования описаний (дополнительных атрибутов), достаточных для принятия решений оператору.

Визуализация должна отвечать современным требованиям по возможности наглядного представления информации, включая картографическую и динамически изменяемую в зависимости от предъявляемых требований и решаемых задач.

В связи с этим перспектива развития ГИС предполагает их использование как средств поддержки принятия решения в системах реального и квазиреального времени. ГИС являются основой для построения современных систем принятия решений, что обусловлено необходимостью соответствующего информационного обеспечения для качественного решения задач управления (в любой сфере деятельности).

Кроме этого, функции для принятия управленческого решения – сбор, обработка, представление данных (информации) – аналогичны, как отмечалось выше, функциям ГИС для гео- и разнородных данных. При таком подходе старые методы функционирования и использования ГИС – электронный вариант бумажной карты – не работоспособны для ГИС нового поколения. ГИС должна не только отражать гео- и разнородную информацию в удобном электронном виде, но и помогать оператору ситуационного центра в принятии решения.

Подход без использования новых специализированных (интеллектуальных) алгоритмов анализа, трансформации, визуализации данных и поддержки принятия решения ведет к перегрузке экрана разнообразной информацией, которая дезориентирует, затрудняет восприятие и, следовательно, вместо помощи мешает в принятии решения. В рассмотренных ГИС реализованы простые методы обработки информации, которые не позволяют автоматизировать процесс поддержки принятия управленческих решений и не являются средством интеграции полноценного анализа гео- и разнородной информации в среду поддержки принятия управленческих решений.

Современные системы принятия решений используют в своем составе ГИС в качестве пространственно-информационной основы, формируя «умные» (интеллектуальные) ГИС. В работе Л.С. Бернштейна, И.Н. Розенберга, С.Л. Белякова [5] дается следующее определение интеллектуальной ГИС (ИГИС) – это ГИС, реализующая функции обработки пространственных данных, которые обычно связывают с выработкой рекомендаций для лица, принимающего решение в условиях неполноты или нечеткости, а также качественного характера исходной информации, путем логического вывода.

Березко А.Е., Соловьев А.А., Гвишиани А.Д., Жалковский В.А. [10] определяют ИГИС как ГИС, которая включает в свой состав интегрированные средства (системы) искусственного интеллекта, а также прикладные компоненты, реализующие наукоемкие пользовательские модели количественного обоснования вырабатываемых рекомендаций.

Ивакин Ю. и Сорокин Р. [11] конкретизируют прикладной характер определения ИГИС – это сложный программный продукт, включающий большое число программных компонент, реализующих как непосредственно саму ГИС, так и различные методы искусственного интеллекта для решения многих сложных задач, в том числе задач пространственного моделирования, поддержки принятия решения и интеллектуального анализа данных.

Функции, которые реализуют ИГИС, аналогичны функциям ГИС: анализ, обработка разнородных данных и их визуальное представление в удобном виде для восприятия. Дополнительные функции ИГИС: получение массивов разнородных данных в реальном (квазиреальном) времени и реализация бизнес-аналитики – работы с данными на разных уровнях иерархии различных систем. Современные ИГИС реализуют аналитику обработки данных в виде концепций метаданных (данных, описывающих организацию других данных) и гармонизации (доступа и преобразования), интеграции (объединения) и слияния (комбинирования для анализа данных и комбинирования для получения знаний) данных. В рамках объектно-ориентированного подхода [4] концепции реализуются через иерархию классов, отражающих понятия предметной области анализа, и связей между ними, получивших название онтологий. Компоненты объединены в системе на основе единой структуры представления и обработки данных и знаний.

К недостаткам ИГИС следует отнести отсутствие (кроме онтологии) механизмов (методов и способов) анализа и получения массивов гео- и разнородных данных, обработки данных по реализации аналитики и визуального представления как геоданных, так и результатов аналитической обработки информации. Также отсутствуют механизмы составления (трансформации) метаданных.

Следующий шаг ретроспективы развития ГИС – «умные» специализированные ГИС (СГИС) – ИГИС для качественного решения задач управления в специализированной сфере деятельности. Сложность, разнообразие и уникальность сфер деятельности обусловливают уникальность управленческих решений, и, следовательно, требуют применения ГИС – СГИС – как специализированных пространственно-информационных основ систем контроля обстановки и принятия решения.

Оценка эффективности использования геоинформационной системы в перспективе эволюционного развития

Оценка эффективности использования ГИС в рамках ее эволюционного развития целесообразна в ключе рассмотрения показателя качества визуализации и затрат на конструктивное исполнение технической части, соотнесенного с показателем предшествующего образца.

В качестве такого показателя эффективности использования ГИС предлагается интегральный показатель эффективности использования ГИС, позволяющий объединить оценку качества визуализации гео- и метаданных по критерию наглядности и конструктивного исполнения собственно технической части ГИС, соотнесенный к показателю обычной (эволюционно предшествующей) ГИС.

Математическая форма записи интегрального показателя имеет вид $\text{П} = \frac{k_{\text{ГИС}}\text{Ц}_{\text{ГИС}}}{\text{Ц}_{\text{ГИСн}}k_{\text{ГИСн}}}$, где $k_{\text{ГИСн}}$ – оценка качества визуализации гео- и метаданных новой (эволюционной) ГИС, реализующей новые методы и способы функционирования ГИС; $\text{Ц}_{\text{СГИСн}}$ – цена новой (эволюционной) ГИС; $k_{\text{ГИС}}$ – оценка качества визуализации гео- и метаданных (эволюционно предшествующей) ГИС; $\text{Ц}_{\text{ГИС}}$ – цена (эволюционно предшествующей) ГИС.

Интегральный показатель эффективности использования ГИС позволяет объединить оценку качества визуализации гео- и метаданных по критерию наглядности и конструктивного исполнения собственно технической части ГИС и рассмотреть положение ГИС в эволюционном ряде разработок ГИС, а также определить направления их последующего совершенствования и развития, которые будут рассмотрены в последующих статьях данного цикла.

- В ходе проведенного исследования целевая установка – анализ функционала ГИС – достигнута. Определены достоинства и недостатки ГИС, перспектива их развития. ГИС развиваются в направлении использования технологии клиент-сервер, специализированных расширений для распространенных SQL-серверов, решений на основе WEB-браузеров, открытых форматов и кодов программ, реализуя распределенные и интеллектуальные ГИС. Динамика развития современных ГИС – «умные» специализированные геоинформационные системы – ИГИС для качественного решения задач управления в специализированной сфере деятельности, требующие разработки методов и способов функционирования ГИС, а именно: анализа, трансформации и визуализации данных для синтеза управленческих решений в ситуационных центрах. Оценка эффективности использования ГИС в рамках ее эволюционного развития целесообразна рассмотрением показателя качества визуализации и затрат на конструктивное исполнение технической части, соотнесенного с показателем пред-

шествующего образца. Такая оценка позволяет изучить положение ГИС в эволюционном ряде разработок ГИС и определить направления последующего их совершенствования и развития.

Литература

1. OGC Standards. 2016. URL = http://www.opengeospatial.org/docs/is.
2. The Open Source Geospatial Foundation. 2016. URL = http://www.osgeo.org.
3. *Присяжнюк С.П.*, *Филатов В.Н.*, *Федоненков С.П.* Геоинформационные системы военного назначения. СПб.: Балт. Гос. техн. Ун-т. 2009.
4. Интеллектуальные географические информационные системы для мониторинга морской обстановки / Под общ. ред. чл-кор. РАН *Р.М. Юсупова* и докт. техн. наук *В.В. Поповича.* СПб.: Наука. 2013.
5. *Розенберг И.Н.*, *Беляков С.Л.* Программные интеллектуальные оболочки геоинформационных систем / Под ред. *Л.С. Бернштейна*. М.: Научный мир. 2010.
6. *Присяжнюк С.П.*, *Осипов Г.К.* Научно-методические основы создания территориальных информационно-аналитических систем для органов местного самоуправления // Информация и космос. 2007. № 2. С. 7–9.
7. *Присяжнюк С.П.*, *Филатов В.Н.* Автоматизированная поддержка принятия решения на геоинформационных системах // Информация и космос. 2004. № 2. С. 4–8.
8. *Ананьев Ю.С.* Геоинформационные системы. Томск: ТПУ. 2013. 70 с.
9. *Милихин М.М.*, *Гриценко Ю.Б.*, *Рычагов М.М.* Комбинированный метод визуализации картографических данных веб-ориентированной геоинформационной системы // Управление, вычислительная техника, и информатика. Доклады ТУСУРа. С. 112–116.
10. *Березко А.Е.*, *Соловьев А.А.*, *Гвишиани А.Д.*, *Жалковский В.А. и др.* Интеллектуальная географическая информационная система «Данные наук о Земле по территории России» // Инженерная экология. 2008. № 5. С. 32–40.
11. *Ivakin Y.*, *Sorokin R.* Application of artificial intelligence methods in geographic information systems // Proc. of International Workshop «Information Fusion and Geographic Information Systems» (IF&GIS2005). SPb. 25–27 September 2005. P. 105–114.

Поступила 12 декабря 2017 г.

Results of analyzing geoinformation systems perspectives

A.V. Voronin – Ph. D. (Eng.), Associate Professor, Leading Research Scientist,
FRC «Computer Science and Control» RAS (Moscow)
E-mail: aleksey.v.v@mail.ru

Geoinformation systems are developed in the direction of client-server technologies, specialized extensions for commonly used SQL-servers, WEB-browser decisions, open formats and instruction (program) codes, realizing distributed and intelligent geoinformation systems. Poorly developed domestic geoinformation systems (GIS) in matters relating with data analysis, transformation and visualization and also sanctions policy of the western countries against the Russian Federation create a particular situation in the modern sphere of domestic infocommunication development. As a result the development of methods and means of GIS functioning according to data analysis, transformation and visualization are required. Perspective of GIS development is eveation of intelligent GIS – IGIS for a qualitative problem of management solving in the specialized sphere.

References

1. OGC Standards. 2016. URL = http://www.opengeospatial.org/docs/is.
2. The Open Source Geospatial Foundation. 2016. URL = http://www.osgeo.org.
3. *Prisyazhnyuk S.P.*, *Filatov V.N.*, *Fedonenkov S.P.* Geoinformaczionny'e sistemy' voennogo naznacheniya. SPb.: Balt. Gos. texn. Un-t. 2009.
4. Intellektual'ny'e geograficheskie informaczionny'e sistemy' dlya monitoringa morskoj obstanovki / Pod obshh. red. chl-kor. RAN *R.M. Yusupova* i dokt. texn. nauk *V.V. Popovicha.* SPb.: Nauka. 2013.
5. *Rozenberg I.N.*, *Belyakov S.L.* Programmny'e intellektual'ny'e obolochki geoinformaczionny'x sistem / Pod red. *L.S. Bernshtejna*. M.: Nauchny'j mir. 2010.
6. *Prisyazhnyuk S.P.*, *Osipov G.K.* Nauchno-metodicheskie osnovy' sozdaniya territorial'ny'x informaczionno-analiticheskix sistem dlya organov mestnogo samoupravleniya // Informacziya i kosmos. 2007. № 2. S. 7–9.
7. *Prisyazhnyuk S.P.*, *Filatov V.N.* Avtomatizirovannaya podderzhka prinyatiya resheniya na geoinformaczionny'x sistemax // Informacziya i kosmos. 2004. № 2. S. 4–8.
8. *Anan'ev Yu.S.* Geoinformaczionny'e sistemy'. Tomsk: TPU. 2013. 70 s.
9. *Milixin M.M.*, *Griczenko Yu.B.*, *Ry'chagov M.M.* Kombinirovanny'j metod vizualizaczii kartograficheskix danny'x veb-orientirovannoj geoinformaczionnoj sistemy' // Upravlenie, vy'chislitel'naya texnika, i informatika. Doklady' TUSURa. S. 112–116.
10. *Berezko A.E.*, *Solov'ev A.A.*, *Gvishiani A.D.*, *Zhalkovskij V.A. i dr.* Intellektual'naya geograficheskaya informaczionnaya sistema «Danny'e nauk o Zemle po territorii Rossii» // Inzhenernaya e'kologiya. 2008. № 5. S. 32–40.
11. *Ivakin Y.*, *Sorokin R.* Application of artificial intelligence methods in geographic information systems // Proc. of International Workshop «Information Fusion and Geographic Information Systems» (IF&GIS2005). SPb. 25–27 September 2005. P. 105–114.

УДК 621

Выбор архитектуры системы хранения данных при создании информационного комплекса «Специализированная информационная среда «Биоресурсные Коллекции» на основе критерия обеспечения высокой доступности

Д.А. Мальцев – начальник отдела, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: Dmitry.Maltsev@frccsc.ru
Ю.Ю. Галимов – зам. начальника отдела, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: YGalimov@ipiran.ru
Д.В. Сигаев – вед. инженер, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: info28@bk.ru
С.В. Луньков – исполняющий обязанности науч. сотрудника, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: s_lunkov@mail.ru

Рассмотрены вопросы организации хранения больших объемов информации в облачных хранилищах, реализованных на открытом программном обеспечении.

Ключевые слова: *специализированная информационная среда «Биоресурсные Коллекции» (СБРК), облачное хранилище данных, база данных (БД), открытое программное обеспечение, научные сервисы, центр коллективного пользования (ЦКП), уникальные научные установки (УНУ).*

The questions of organization of storage of large volumes of information in cloud storages realized on open software are considered.

Keywords: *specialized information environment «Bioresource Collections» (RRBC), cloud storage, database (DB), open source software, scientific services, the Center for Collective Use (CCU), unique scientific installations (USI).*

Одним из важнейших современных мировых трендов технологического развития является расширение сферы применения информационно-телекоммуникационных технологий для извлечения знаний на основе аналитической обработки накопленных массивов данных, которые в настоящее время приобретают, по существу, статус одного из важнейших стратегических ресурсов.

Без анализа и обработки накопленных массивов данных в конкретных областях науки, промышленности, здравоохранения, обороноспособности, образования и других сфер деятельности невозможно принятие эффективных решений как научными коллективами и отдельными учеными-исследователями, так и органами государственной власти на различных уровнях (федеральном, ведомственном, региональном, муниципальном, местном и т.д.). Совокупность технологий, стоящих за подготавливаемой всем ходом технического прогресса цифровой революцией, сейчас условно называется Big Data. Большие данные – общий термин, используемый для описания огромного количества структурированных, неструктурированных и частично структурированных данных, которые требуется обработать для получения необходимого для эффективной деятельности аналитического продукта. Построенная на основе таких технологий система должна своевременно выявлять источники данных, доставлять и обрабатывать исходные данные, производить информационный продукт и доводить его до потребителя [1], что потребует разработки новых научных подходов, технологий и методов сбора, обработки и хранения накапливаемых данных [2–5].

Взаимоотношения научных, коммерческих и государственных организаций и коллективов принимают форму интеграции разрозненных сервисов в единый консолидированный сервис. В биоресурсных коллекциях (БРК), существующих на базе различных научных организаций страны, накапливаются и поддерживаются биологические материалы различного типа. Услуги по их обработке (научные сервисы) предоставляются, преимущественно, в рамках центров коллективного пользования научным оборудованием (ЦКП) и уникальных научных установок (УНУ).

Под ЦКП понимается структурное подразделение (совокупность структурных подразделений), которое создано научной организацией и (или) образовательной организацией, располагает научным и

(или) технологическим оборудованием и квалифицированным персоналом и обеспечивает в интересах третьих лиц выполнение работ и оказание услуг для проведения научных исследований, а также осуществления экспериментальных разработок (согласно Федеральному закону от 23.08.1996 № 127-ФЗ (ред. от 23.05.2016) «О науке и государственной научно-технической политике»), либо научно-исследовательская организация, обладающая современным научным и аналитическим оборудованием и высококвалифицированными кадрами и обеспечивающая проведение на имеющемся оборудовании научных исследований и оказание услуг (исследований, испытаний, измерений) в интересах организаций (согласно Постановлению Правительства РФ от 17 февраля 2016 г. № 109). Требования к ЦКП утверждены Постановлением Правительства РФ от 17 мая 2016 г. № 429.

Под УНУ понимается комплекс научного оборудования, не имеющий аналогов в РФ, функционирующий как единое целое и созданный научной организацией и (или) образовательной организацией в целях получения научных результатов, достижение которых невозможно при использовании другого оборудования (согласно Федеральному закону от 13.07.2015 № 270-ФЗ).

По состоянию на 2016 г. (согласно порталу «Современная исследовательская инфраструктура Российской Федерации», http://ckp-rf.ru), в 195 подведомственных ФАНО России организаций функционируют ЦКП и/или предоставляется доступ к УНУ.

Наиболее эффективным каналом передачи данных по объективным причинам является глобальная сеть Интернет, позволяющая обеспечить оперативный, малозатратный и всеобъемлющий охват территории, а также дать возможность эффективной совместной работы научным коллективам и организациям [9].

Все основные сервисы ЦКП и УНУ могут быть классифицированы как исследования, испытания и измерения. ЦКП и УНУ чаще всего построены на базе дорогостоящего оборудования (стоимостью в сотни миллионов рублей), поэтому одной из наиболее важных задач становится необходимость мониторинга степени загрузки данных объектов и повышение эффективности проводимых с их помощью исследований (с научной и финансовой точек зрения).

Информационный комплекс «Специализированная информационная среда «Биоресурсные Коллекции» (далее СБРК) создается как распределенная информационная система, предоставляющая научные сервисы для формирования сценариев (технологических цепочек) по получению новых знаний с использованием биоматериалов, накопленных в БРК, и их обработке с помощью научного и (или) технологического оборудования и квалифицированного персонала, сосредоточенных в научных ЦКП. Для этого система должна поддерживать данные как о самих БРК, так и о приборной базе, кадровом потенциале и компетенции сотрудников ЦКП. В дальнейшем такая система может быть использована в качестве торговой площадки.

Цель работы – рассмотреть вопросы организации хранения больших объемов информации в облачных хранилищах, реализованных на открытом программном обеспечении.

Выбор системы хранения данных

Облачная инфраструктура предъявляет высокие требования к системе хранения данных. Для обеспечения качественного сервиса система хранения данных должна обладать рядом свойств, таких как: высокая надежность хранения; минимальное время простоя при авариях; высокая скорость доступа и минимальные задержки; низкая удельная стоимость хранения; различные прикладные возможности – клонирование, снимки состояния и т.д.

Ни RAID-массивы, ни аппаратные системы хранения данных не способны решить все перечисленные задачи одновременно. Для решения поставленных задач целесообразно использовать программную технологию распределенного хранения данных. В рамках реализации проекта предлагается использовать распределенную систему хранения с открытым кодом Ceph.

Ceph – отказоустойчивое распределенное хранилище данных, работающее по протоколу TCP. Одно из базовых свойств Ceph – масштабируемость до петабайтных размеров. Ceph предоставляет на выбор три различных абстракции для работы с хранилищем: абстракцию объектного хранилища (RADOS Gateway), блочного устройства (RADOS Block Device) или POSIX-совместимой файловой системы (CephFS) [6–8].

Абстракция объектного хранилища (RADOS Gateway, или RGW) вкупе с FastCGI-сервером позволяет использовать Ceph для хранения пользовательских объектов и предоставляет API, совместимый с S3/Swift.

Абстракция блочного устройства (RADOS Block Device, или RBD) предоставляет пользователю возможность создавать и использовать виртуальные блочные устройства произвольного размера. Программный интерфейс RBD позволяет работать с этими устройствами в режиме чтения/записи и выполнять служебные операции – изменение размера, клонирование, создание и возврат к снимку состояния и т.д.

CephFS – POSIX-совместимая файловая система, использующая Ceph в качестве хранилища.

Хранилище объектов Ceph поддерживает три интерфейса:

S3-совместимый – предоставляет Amazon S3 RESTful API-совместимый интерфейс к кластерам хранения Ceph;

Swift-совместимый – предоставляет OpenStack Swift API-совместимый интерфейс к кластерам хранения Ceph (шлюз объектов Ceph может быть использован как замена для Swift в кластере OpenStack);

API-администратора – позволяет выполнять администрирование вашего кластера Ceph посредством HTTP RESTful API.

Основными сущностями инфраструктуры Ceph являются:

Metadata server (MDS) – вспомогательный демон для обеспечения синхронного состояния файлов в точках монтирования CephFS. Работает по схеме активная копия + резервы, причем активная копия в пределах кластера только одна.

Mon (Monitor) – элемент инфраструктуры Ceph, который обеспечивает адресацию данных внутри кластера и хранит информацию о топологии, состоянии и распределении данных внутри хранилища. Клиент, желающий обратиться к блочному устройству rbd или к файлу на примонтированной cephfs, получает от монитора имя и положение rbd header – специального объекта, описывающего положение прочих объектов, относящихся к запрошенной абстракции (блочное устройство или файл), – и далее общается со всеми OSD, участвующими в хранении файла.

Объект (Object) – блок данных фиксированного размера (по умолчанию 4 Мб). Вся информация, хранимая в Ceph, квантуется такими блоками. Чтобы избежать путаницы, подчеркнем – это не пользовательские объекты из Object Storage, а объекты, используемые для внутреннего представления данных в Ceph.

OSD (object storage daemon) – сущность, которая отвечает за хранение данных, основной строительный элемент кластера Ceph. На одном физическом сервере может размещаться несколько OSD, каждая из которых имеет под собой отдельное физическое хранилище данных.

Карта OSD (OSD Map) – карта, ассоциирующая каждой плейсмент-группе набор из одной Primary OSD и одной или нескольких Replica OSD. Распределение placement groups (PG) по нодам хранилища OSD описывается срезом карты osdmap, в которой указаны положения всех PG и их реплик. Каждое изменение расположения PG в кластере сопровождается выпуском новой карты OSD, которая распространяется среди всех участников.

Плейсмент-группа (Placement Group, PG) – логическая группа, объединяющая множество объектов, предназначенная для упрощения адресации и синхронизации объектов. Каждый объект состоит лишь в одной плейсмент-группе. Число объектов, участвующих в плейсмент-группе, не регламентировано и может меняться.

Primary OSD – OSD, выбранная в качестве Primary для данной плейсмент-группы. Клиентское I/O всегда обслуживается той OSD, которая является Primary для плейсмент-группы, в которой находится интересующий клиента блок данных (объект). Primary OSD в асинхронном режиме реплицирует все данные на Replica OSD.

RADOS Gateway (RGW) – вспомогательный демон, исполняющий роль прокси для поддерживаемых API объектных хранилищ. Поддерживает географически разнесенные инсталляции (для разных пулов, или, в представлении Swift, регионов) и режим active-backup в пределах одного пула.

Replica OSD (Secondary) – OSD, которая не является Primary для данной плейсмент-группы и используется для репликации. Клиент никогда не общается с ними напрямую.

Фактор репликации (RF) – избыточность хранения данных. Фактор репликации является целым числом и показывает, сколько копий одного и того же объекта хранит кластер.

Ceph OSD работает поверх физического диска, имеющего допустимый раздел Linux. Раздел Linux может быть Btrfs (файловая система B-деревьев), XFS или ext4. В отношении Ceph эти файловые системы отличаются друг от друга различными свойствами.

Btrfs. OSD с файловой системой Btrfs на нижнем уровне обеспечивает наилучшую производительность по сравнению с OSD на основе файловых систем XFS и ext4. Одним из основных преимуществ

использования Btrfs является ее поддержка копирования при записи и перезаписываемые моментальные снимки, которые очень выгодны в ситуации, когда дело доходит до подготовки и клонирования виртуальных машин. Она также поддерживает прозрачное сжатие и всеобъемлющие контрольные суммы, а также включает в себя управление многими устройствами в файловой системе. Btrfs поддерживает эффективные XATTR и встроенные данные для малых файлов, обеспечивает интегрированное управление томами, поддерживающее SSD, а также имеет особенности, требующиеся для онлайн *fsck*. Однако, несмотря на эти новые возможности, Btrfs в настоящее время не готова к промышленному использованию, но является хорошим кандидатом для тестового развертывания.

XFS. Это надежная, зрелая и очень стабильная файловая система, а, следовательно, рекомендуется для использования в промышленных кластерах Ceph. Поскольку Btrfs не готова к промышленному использованию, XFS является наиболее часто используемой файловой системой в системах хранения Ceph и рекомендуется для OSD. Тем не менее, при сравнении с Btrfs XFS располагается ниже. XFS имеет проблемы с производительностью при масштабировании метаданных. Кроме того, XFS является файловой системой с журналированием, то есть каждый раз, когда клиент отправляет данные на запись в кластер Ceph, они вначале записываются в пространство журналирования, а затем в файловую систему XFS. Это увеличивает издержки записи одних и тех же данных в два раза, и, таким образом, делает производительность XFS более медленной по сравнению с Btrfs, которая не использует журналы.

ext4. Четвертая расширяемая файловая система также является журналируемой файловой системой, которая является готовой к промышленному использованию файловой системой для Ceph OSD. Однако она не настолько популярна, как XFS. С точки зрения производительности ext4 не сопоставима с Btrfs

Потеря из вида одной из копий объекта приводит к переходу объекта и содержащей его плейсмент-группы в состояние degraded и выпуску новой карты OSD (osdmap). Новая карта содержит новое расположение потерянной копии объекта, и если через заданное время утраченная копия не вернется, недостающая копия будет восстановлена в другом месте, чтобы сохранить число копий, определяемое фактором репликации. Операции, выполнявшиеся в момент подобной ошибки, автоматически переключатся на одну из доступных копий. В худшем случае их задержка будет измеряться единицами секунд.

Важным свойством Ceph является то, что все операции по перебалансировке кластера происходят в фоновом режиме одновременно с пользовательским I/O. Если клиент обращается к объекту, который находится в recovering состоянии, Ceph вне очереди восстановит объект и его копии, а затем выполнит запрос клиента. Такой подход обеспечивает минимальное латенси I/O даже тогда, когда восстановление кластера идет полным ходом.

Одна из самых важных особенностей Ceph – возможность тонкой настройки репликации, задаваемой правилами CRUSH – мощного и гибкого механизма, базирующегося на случайном распределении PG по группе OSD с учетом правил (вес, состояние ноды, запрет на размещение в той же группе нод). По умолчанию OSD имеют вес, базирующийся на величине свободного места в соответствующей точке монтирования в момент ввода OSD в кластер, и подчиняются правилу распределения данных, запрещающему держать две копии одной PG на одной ноде. CRUSHMAP – описание распределения данных – может быть модифицирован под правила, запрещающие держать вторую копию в пределах одной стойки, тем самым обеспечивая отказоустойчивость на уровне вылета целой стойки.

- Преимущество Ceph перед прочими кластерными системами хранения данных состоит в отсутствии единых точек отказа и в практически нулевой стоимости обслуживания при восстановительных операциях. Избыточность и устойчивость к авариям заложена на уровне архитектурных решений. С Ceph восстановление и перестроение кластера происходят незаметно, практически не влияя на клиентский I/O. То есть деградировавший кластер для Ceph – это не экстраординарная ситуация, а всего лишь одно из рабочих состояний.

  Совокупные преимущества распределенной системы хранения Ceph позволяют организовать высоконадежное, отказоустойчивое и производительное решение для облачной инфраструктуры Системы как на блочном уровне, так и на объектном уровне хранения.

  Таким образом, приведенный в предыдущем разделе анализ показывает, что с точки зрения критерия высокой доступности выбор кластерной системы на основе Ceph является обоснованным, поэтому при реализации проекта СБРК предлагается использовать распределенную систему хранения с открытым кодом Ceph.

Литература

1. *Будзко В.И.* Системы высокой доступности и Большие Данные // Системы высокой доступности. 2013. Т. 9. № 4. С. 3–11.
2. *Shui Qing Ye.* Big Data Analysis for Bioinformatics and Biomedical Discoveries. Chapman & Hall/CRC Mathematical and Computational Biology. Taylor & Francis Group. LLC. 2016.
3. *Erciyes K.* Distributed and Sequential Algorithms for Bioinformatics. Computational Biology. Springer International Publishing. Switzerland. 2015.
4. *Stefanowski Jerzy, Japkowicz Nathalie* Big Data Analysis. New Algorithms for a New Society (Studies in Big Data). Springer International Publishing. Switzerland. 2016.
5. *Brabazon A., O'Neill M., McGarraghy S.* Natural Computing Algorithms. Springer International Publishing. Switzerland. 2016.
6. *Weil Sage A., Brandt Scott A., Miller Ethan L., Long Darrell D.E. and Maltzahn Carlos* Ceph: A Scalable, High-performance Distributed File System // Proc. of the 7th Symposium on Operating Systems Design and Implementation OSDI '06. 2006. Seattle, Washington: USENIX Association. P. 307–320.
7. *Ahmed W.* Mastering Proxmox. Packt Publishing. 2014. 310 p.
8. *Grant T. and Kooter B.* Comparing OODA & Other Models as Operational View C2 Architecture // Proc. of the 10th International Command and Control Research Technology Symposium. June 2005. McLean. VA. USA.
9. *Сучков А.П.* Аналитические аспекты мультиагентных распределенных систем управления // Системы и средства информатики. 2014. Т. 24. № 2. С. 166–177.

Поступила 15 декабря 2017 г.

Choice of the architecture of the data storage system when creating the information complex «Specialized information environment «Bioresource Collections» on the basis of the criterion of ensuring high availability

D.A. Maltsev – Head of Department, FRC «Computer Science and Control» RAS (Moscow)
E-mail: Dmitry.Maltsev@frccsc.ru
Yu.Yu. Galimov – Deputy Head of Department, FRC «Computer Science and Control» RAS (Moscow)
E-mail: YGalimov@ipiran.ru
D.V. Sigaev – Leading Engineer, FRC «Computer Science and Control» RAS (Moscow)
E-mail: info28@bk.ru
S.V. Lunkov – Acting Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: s_lunkov@mail.ru

Bioresource collections of FAOO Russia's scientific institutions are a component of the scientific infrastructure designed to provide Russian and foreign scientists with access to biological objects used in fundamental and applied scientific research. The questions of organization of storage of large volumes of information in cloud storages realized on open software are considered.

References

1. *Budzko V.I.* Sistemy' vy'sokoj dostupnosti i Bol'shie Danny'e // Sistemy' vy'sokoj dostupnosti. 2013. T. 9. № 4. S. 3–11.
2. *Shui Qing Ye.* Big Data Analysis for Bioinformatics and Biomedical Discoveries. Chapman & Hall/CRC Mathematical and Computational Biology. Taylor & Francis Group. LLC. 2016.
3. *Erciyes K.* Distributed and Sequential Algorithms for Bioinformatics. Computational Biology. Springer International Publishing. Switzerland. 2015.
4. *Stefanowski Jerzy, Japkowicz Nathalie* Big Data Analysis. New Algorithms for a New Society (Studies in Big Data). Springer International Publishing. Switzerland. 2016.
5. *Brabazon A., O'Neill M., McGarraghy S.* Natural Computing Algorithms. Springer International Publishing. Switzerland. 2016.
6. *Weil Sage A., Brandt Scott A., Miller Ethan L., Long Darrell D.E. and Maltzahn Carlos* Ceph: A Scalable, High-performance Distributed File System // Proc. of the 7th Symposium on Operating Systems Design and Implementation OSDI '06. 2006. Seattle, Washington: USENIX Association. P. 307–320.
7. *Ahmed W.* Mastering Proxmox. Packt Publishing. 2014. 310 p.
8. *Grant T. and Kooter V.* Comparing OODA & Other Models as Operational View C2 Architecture // Proc. of the 10th International Command and Control Research Technology Symposium. June 2005. McLean. VA. USA.
9. *Suchkov A.P.* Analiticheskie aspekty' mul'tiagentny'x raspredelenny'x sistem upravleniya // Sistemy' i sredstva informatiki. 2014. T. 24. № 2. S. 166–177.