Российский государственный гуманитарный университет
Russian State University for the Humanities

RSUH/RGGU BULLETIN
№ 3 (5)

Academic Journal

Series:
Records Management and Archival Studies.
Computer Science. Data Protection and Information Security

Moscow
2016

ВЕСТНИК РГГУ
№ 3 (5)

Научный журнал

Серия
«Документоведение и архивоведение. Информатика.
Защита информации и информационная безопасность»

Москва
2016

УДК 651.4(05)+930.25(05)+004(05)
ББК 65.050.2я5+79.3я5+32.81я5

Ответственный за выпуск: Е.П. Охапкина (РГГУ)

ISSN 2073-6371

СОДЕРЖАНИЕ

CONTENTS

Памяти
Александра Алексеевича Тарасова

(30.01.1958 – 07.05.2016)

Ушел из жизни Александр Алексеевич Тарасов – талантливый ученый, доктор технических наук, профессор, директор Института информационных наук и технологий безопасности РГГУ, член Научного совета при Совете безопасности Российской Федерации, один из столпов отрасли обеспечения в России информационной безопасности и защиты информации. Александр Алексеевич без преувеличения был уникальным человеком, чью ответственность и порядочность перед наукой и коллегами отмечали все те,

кто его знал и работал с ним. Человек тонкой душевной организации, он был открытым и чутким, готовым всегда прийти на помощь. Будучи по натуре своей человеком разносторонне и творчески одаренным, он никогда не удовлетворялся стандартными взглядами на научные проблемы и прикладные вопросы реализации научных исследований, которыми он занимался. Желая докопаться до самой сути обсуждаемой темы, Александр Алексеевич был всегда открыт дискуссиям, в процессе которых высказывал множество оригинальных идей и зачастую новаторских подходов к решению обсуждаемых задач. Умел вдохновлять своими идеями многочисленных учеников и коллег, много и плодотворно работал, не приемля безответственного и бездушного отношения к порученному делу. Сам по себе он был чрезвычайно целеустремленным человеком, настойчиво добиваясь поставленных задач, невзирая на огромную повседневную загрузку....

Отдавая дань светлой памяти об Александре Алексеевиче, хотелось бы осветить основные этапы его биографии, главные научные и профессиональные достижения.

Александр Алексеевич родился в селе Лух Лухского района Ивановской области, в семье военнослужащего, в 1958 г., в первый год после запуска первого искусственного спутника Земли, что и определило во многом всю его жизнь. С ранних лет его неведомым магнитом тянул космос. Этому способствовало и то, что ранние годы его жизни прошли в мало кому тогда известном Байконуре, где проходил службу его отец. Александр Алексеевич всегда с гордостью вспоминал случай, когда он гонял с мальчишками в футбол, и улетевший с поля мяч ловким ударом с правой ноги вернул юным футболистам не кто-нибудь, а сам... Юрий Гагарин! Вот такое космическое детство, освещенное нашими победами в космосе, общением с людьми, которые реально обеспечивали космические старты наших непревзойденных ракет, и формировало его как личность. Следует отметить, что на его профессиональный интерес к вычислительной технике огромное влияние оказала его мама Валентина Сергеевна, которая в те годы участвовала в создании первых отечественных ЭВМ «Урал», с которых началась история малых ЭВМ.

Начинал Александр Алексеевич своё служение Отечеству в славном Киевском высшем инженерном радиотехническом училище ПВО имени маршала авиации А.И. Покрышкина и всегда с гордостью отмечал, что он КВИРТУрианец, что звучало так, как будто он пришелец с другой планеты под кратким названием КВИРТУ...

В 1981 г. окончил с отличием Военную академию им. Ф.Э. Дзержинского по специальности «электронно-вычислительная техника». В 1989 г. защитил диссертацию на соискание ученой степени кандидата технических наук. В 1991 г. Александру Алексеевичу было присвоено звание старший научный сотрудник по специальности «военная кибернетика, информатика, системный анализ, исследование операций и моделирование систем и боевых действий». В 1993 г. он окончил механико-математический факультет МГУ им. М.В. Ломоносова по специальности «прикладная математика (инженерный поток)». Руководителем по его диплому был известный математик, доктор физико-математических наук, профессор, лауреат Государственной премии СССР, профессор кафедры теории вероятностей механико-математического факультета Александр Дмитриевич Соловьев, один из основателей отечественной математической теории надежности. И надо же было так сложиться, что много лет спустя, уже в ФАПСИ, судьба свела его с сыном его учителя, который в то время являлся заместителем руководителя одного из главков Агентства. Они сразу подружились, ведь их сроднило общее: отношение к великому математику А.Д. Соловьеву как к своему Учителю у одного и как к Учителю и Отцу – у другого.

В 2004 г. в Центральном научно-исследовательском институте радиоэлектронных систем Александр Алексеевич один из первых в деятельности диссертационного совета этого авторитетного учреждения блестяще защитил диссертацию на соискание степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность. 1 декабря 2011 г. ему было присвоено ученое звание профессора.

Всю свою жизнь, надев сознательно в 17 лет погоны курсанта КВИРТУ и пройдя ступени военной карьеры до полковника, Александр Алексеевич был настоящим патриотом своей страны, посвятив себя служению Отечеству:

- 1990–1998 – начальник лаборатории 4-го Центрального научно-исследовательского института Министерства обороны Российской Федерации;
- 1998–2000 – научный консультант 2-го отдела управления обеспечения правовой информатизации ФАПСИ;
- 2000–2003 – старший референт генерального директора ФАПСИ;
- 2003 – консультант генерального директора ФАПСИ;
- 2003–2011 – старший консультант Центра ФСБ России.

Одиннадцать лет, практически с самого момента основания нового самостоятельного направления в деятельности Совета Безопасности Российской Федерации, Александр Алексеевич трудился в подразделении, обеспечивающем разработку госполитики в области обеспечения информационной безопасности страны. Он внес огромную лепту в обеспечение межведомственной координации по решению ключевых проблем в этой области. И нет ни одного решения Научного совета и Межведомственной комиссии по проблемам информационной безопасности при Совете Безопасности Российской Федерации того времени, в которое не вложил бы он часть своей души и сердца.

За свою службу Александр Алексеевич был удостоен ряда наград Минобороны России, ФАПСИ, ФСБ России, Академии космонавтики им. К.Э. Циолковского. Среди них: почетная грамота Секретаря Совета Безопасности «За заслуги в обеспечении национальной безопасности»; почетный знак «Совет Безопасности Российской Федерации»; медаль Совета Безопасности Российской Федерации «За укрепление национальной безопасности»; медаль ФСТЭК России «За укрепление Государственной системы защиты информации» 1-й и 2-й степеней; знак отличия ФСТЭК России «За заслуги в защите информации».

За свою научную карьеру Александр Алексеевич стал автором более 150 научных трудов, основная тематика которых – организация и обеспечение устойчивого функционирования информационных систем, анализ функционирования распределенных информационно-телекоммуникационных систем, безопасность функционирования критически важных информационных систем, компьютерная безопасность и защита информации. Он также является автором 15 изобретений, основная тематика которых – отказоустойчивость вычислительных систем, распознавание изображений.

В последнее десятилетие активно занимался научно-педагогической деятельностью. С 2005 г. являлся профессором кафедры «Защита информации» Национального исследовательского ядерного университета «МИФИ», читая курс лекций по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем». С 2007 г. постоянный член ГАК НИЯУ «МИФИ» по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем». С 2011 г. директор Института информационных наук и технологий безопасности Российского государственного гуманитарного университета, заведующий кафедрой комп-

лексной защиты информации. Член докторских диссертационных советов при МГТУ им. Н.Э. Баумана и при Всероссийском научно-исследовательском институте проблем вычислительной техники и информатизации по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Также Александр Алексеевич занимался общественной деятельностью. Непосредственно участвовал в организации Национального форума информационной безопасности «ИНФОФОРУМ».Являлся членом редакционной коллегии журнала «Бизнес и безопасность в России» – официального печатного органа «ИНФОФОРУМ». Был членом редакционного совета журнала «Надёжность», экспертом Российского фонда фундаментальных исследований по рассмотрению проектов в области информационных технологий и информационной безопасности, а также членом научно-технического совета Минкомсвязи России.

Александр Алексеевич был прекрасным семьянином. Обожал свою супругу и дочь, с которыми проводил вместе свои отпуска, путешествуя по разным уголкам нашей прекрасной Родины. По жизни был скорее романтиком. Его любимым поэтом и бардом был Владимир Высоцкий. Александр Алексеевич собрал полную профессиональную фонотеку песен любимого певца и поэта, а некоторые его авторские песни, особенно посвященные Великой Отечественной войне, он не мог слушать иначе как с искренними мужскими слезами. Он и сам не был чужд поэзии, и в кругу его близких друзей славился своими короткими и точными эпиграммами.

С портрета взирает широкая, озорная улыбка Александра Алексеевича. Не верится, что она уже из прошлого. Спасибо тебе, достойный сын России, что ты славно служил ей всю свою, к сожалению, так рано и преждевременно оборвавшуюся жизнь. Жизнь как полет ракеты. Полет прервался внезапно и для всех неожиданно... Похоронен А.А.Тарасов на родовом кладбище, напротив церкви святых мучеников Андриана и Натальи. Золотые купола храма в солнечные дни горят на солнце и отраженные ими лучи устремляются в тишь старого московского кладбища, где нашел свой последний приют светлой души человек, настоящий русский офицер, яркий ученый, педагог и руководитель.

Купола в России кроют чистым золотом –
Чтобы чаще Господь замечал...

Александр Алексеевич Тарасов оставил светлую память о себе и своих делах в сердцах всех тех, с кем он работал, общался, дружил. А дело, которому он посвятил свою жизнь, обязательно продолжат его многочисленные ученики!

Семья, коллеги, друзья, редколлегия
журнала «Вестник РГГУ»

Теоретические и практические проблемы информатики

В.К. Жаров, Т.А. Гусева,
Ю.В. Таратухина

Педагогическая информатика как техническое, философское понятие и понятие современной педагогики

Статья посвящена развивающейся области знания, находящегося на стыке педагогики, информатики, технологий управления информационными потоками в современном образовательном процессе. В ней обосновывается предпочтение, отданное понятию «педагогическая информатика», нежели понятию «информационная педагогика». Приведены примеры значимости новой области знаний, которые изучаются с помощью педагогической информатики.

Ключевые слова: педагогическая информатика, культурно-релевантный интеллект педагога, образовательная среда, конструктивный трансфер знаний, кросс-культурная дидактика, информационно-педагогическая среда.

В настоящее время мы можем наблюдать плотное вхождение информационных технологий в нашу повседневную и профессиональную жизнь, в частности в педагогические практики.

На наш взгляд, информационная педагогика[1] не очень удачное понятие для педагогики. Во-первых, педагогика без информации о ребенке – это нонсенс, т. е. информация – доминанта процесса с самого начала общения Учителя и Ученика. Во-вторых, обмен информацией не только на уровне второй сигнальной системы, но и помимо нее существует как поток информации, который в зависимости от квалификации педагог считывает. В-третьих, деятельность ребенка в процессе развития (взросления) в рамках педагогической организации корректируется внешними обстоятельствами, дающими исторический срез в личностной среде ребенка. Можно привести еще несколько аргументов в пользу нашего утверждения, но они специфически выражены в конкретной учебной дисциплине.

В современной литературе синонимом к информационной педагогике определяется педагогическая информатика, которую можно рассмотреть как «область педагогической науки, изучающую использование в образовании ЭВМ, коммуникационных сетей, различных информационных технологий»[2].

Это понятие в данной трактовке также не приводит к согласию, прежде всего, из-за его технической направленности. В педагогике, а следовательно, в искусстве донесения знаний (читаем – информации), был всегда и остается теперь (а возможно, становится одним из главных компонентов) компонент *обмена* информацией между Учителем и Учеником. Компоненты же обработки, сохранения информации были сопутствующими. Эти три составляющие учебного процесса появились, как только процесс передачи знаний возник в культурах на Земле. С появлением машин по обработке и передаче информации – письменных приборов, счетных инструментов, печатных станков и различных организационно-технических атрибутов процесса обучения для следующих поколений, – образовательный процесс изменил скорость и качественные характеристики результатов обучения. В истории образования эти три названных компонента педагогического процесса меняли свою значимость и очередность и приоритеты. В педагогических теориях изучение каждой из компонент в определенный исторический период определяло развитие самой теории, но в целом их изучение и привело к появлению раздела в педагогике, который, очевидно, можно назвать *педагогической информатикой*. Причем не в смысле «использования ... ЭВМ, коммуникационных сетей, различных информационных технологий», это было и раньше с точностью до терминологии в образовательном процессе, но в том смысле, что она изучает способы передачи, обработки и хранения учебной информации, а также формирование и подготовку различных сред (микро- и макро-) индивида, социума, общества.

В таком случае данный раздел педагогики имеет свой объект и предмет. *Объектом* становятся структуры образовательного процесса, ориентированные на способы передачи необходимой в процессе обучения информации, *предметом* же – мышление как целостное явление процессов интериоризации и экстериоризации в процессе обучения, методы которого направлены на создание условий полного, точного сохранения обработанной в этом процессе информации. В такой трактовке рассматриваемое нами понятие «педагогическая информатика» обуславливает язык, универсальную знаковую систему и возможные коммуникационные связи между науками, «обслуживаемые» этим

разделом педагогики. Одно из прикладных его выражений мы обнаруживаем в новом направлении общей педагогики – кросс-культурной дидактике.

Отсюда ясно, что «педагогическая информатика» – более точное понятие. Предметом этого раздела является «воспитание мышления» в терминологии Дж. Дьюи, а объектом становится система организации образовательного процесса. Более того, методами исследования в этом случае являются не только методы психологии (читайте – математической статистики), но и более значимые – математического моделирования, прогнозирования с использованием модальных логик и построения компьютерных экспериментов.

Приведем два примера из приложений теории кросс-культурной дидактики. Пример первый находится у основания идей кросс-культурной педагогики.

На сегодняшний день поликультурная студенческая аудитория перестала быть редким явлением. Это касается как традиционного формата обучения, так и онлайн-образовательных практик. В результате проведенного нами опроса преподавателей, имевших подобный опыт работы, мы выявили ряд затруднений, специфичных именно для данных типов студенческих аудиторий и не имеющих место в монокультурных средах: различные модели коммуникации в системе «преподаватель – студент», культурно-специфичные особенности репрезентации учебной информации и учебного контента, когнитивная специфика и специфика принятия решений, различное понимание «креативности», неоднозначное понимание учебных задач, терминологии, предпочитаемый тип контрольно-измерительных материалов и т. д. В данном случае встает вопрос: как обеспечить конструктивное наращивание компетентностной модели в рамках национально-культурной и профессиональной полифонии? Иными словами, как организовать «дизайн курса», ориентированного на поликультурную аудиторию и обеспечить конструктивный трансфер знаний? В данном случае мы сталкиваемся с таким явлением, как образовательная кросс-культура. В интересующем нас контексте образовательная кросс-культура есть совокупность:

1. Культуры преподавателя (национальной и профессиональной).
2. Культуры студента (национальной и профессиональной).
3. Семиотического пространства (учебного заведения или онлайн-ресурса) и тезауруса учебной дисциплины.

На наш взгляд, на данном этапе совершенно необходимы разработки в области теории обучения в поликультурной среде – кросс-культурной дидактики.

По нашему мнению, кросс-культурная дидактика будет состоять из разделов, изучающих:
- Цели и ценности обучения в разных культурных группах.
- Общие особенности когнитивной деятельности в разных культурных группах.
- Стили обучения в разных культурах.
- Общие особенности методов обучения и контрольно-измерительных материалов в разных культурных группах.
- Особенности и проблемы педагогического дискурса (в частности, академического письма) в поликультурном пространстве, в том числе в онлайн-среде.
- Разработки в области кросс-культурной мультимедийной дидактики.
- Проблематику и специфику конструктивного трансфера знаний в кросс-культурной учебной-среде.

Отсюда можно вывести модель культурно-релевантного интеллекта педагога.

Таблица 1

Модель культурно-релевантного интеллекта педагога

Когнитивный – эмоциональный-операционный компоненты образовательной коммуникации	
Стиль обучения	Стиль преподавания
Понимание общей специфики когнитивной деятельности представителей разных культурных групп	
Организация учебного контента	
Организация методов обучения	
Специфика педагогического дискурса	
Особенности КИМов	
Рефлексия и конструктивная обратная связь	

Во многом специфика коммуникации в системе «преподаватель – студент» обусловлена социокультурными факторами. В рамках теории Г. Хофстеде были рассмотрены все составляющие культуры и определено их влияние на взаимодействие при процессе обучения. С точки зрения дихотомии критериев «низкая/высокая дистанция власти» культуры в образовательном пространстве делятся на те, которые сосредоточены в большей степени или на педагоге (*teacher-centred*), или на ученике *(learner-centred*).

В культурах с низкой дистанцией власти (США, Великобритания, Канада, Австралия, страны Центральной Европы и др.) центральной фигурой является учащийся – все «крутится вокруг него», тогда как учитель является скорее сопровождающей фигурой. Преподаватель не транслирует знания, а лишь помогает студенту самостоятельно находить необходимую информацию и делать собственные выводы. В странах с высокой дистанцией власти (Китай, Япония и др.), наоборот, центральная фигура – это преподаватель, играющий роль «гуру». Передаваемая им информация позиционируется как неоспоримая и, безусловно, высокоценимая. Из чего видно, что чем выше дистанция власти, тем выше необходимость признания статуса преподавателя, и тем меньше может быть дискуссий с ним. В странах с очень высокой дистанцией власти преподаватель должен руководить каждым шагом студента, в то время как при снижении дистанции инициатива переходит к студенту.

С точки зрения дихотомии критериев индивидуализма и коллективизма в странах с высоким индексом индивидуализма (США, Канада, Австралия, Великобритания и др.) *цель обучения* – научить индивида учиться и впоследствии самостоятельно получать необходимые знания, подготовив его, таким образом, к непрерывному обучению (англ. «education through life») в постоянно меняющемся мире, где информация быстро устаревает. В индивидуалистском культурном контексте обучающегося учат надеяться только на себя и собственные силы. Акцент на индивидуальных достижениях личности в культуре в общем, и на деятельности отдельного ученика в академическом контексте приводит к возникновению у учащихся трудностей в случае групповых и коллективных форм работы на занятии, поэтому большое внимание педагогами уделяется проектной деятельности и умению работать в команде. Большое внимание уделяется нестандартным и креативным подходам к решению заданий. Напротив, в странах с высоким индексом коллективизма (Китай, Япония, арабские страны и др.) упор делается на заучивание и запоминание большого объема информации. Нередко теория не подкрепляется практическими навыками. Таким образом, можно сказать, что в коллективистских культурах существует проблема практической применимости фундаментальных теоретических знаний.

С позиций параметра культуры «феминность/маскулинность» делается заключение, что «феминные» культуры, такие как Швеция, ориентированы прежде всего на психологический комфорт в учебной среде и социальную адаптацию. В свою очередь, в «маскулинных» культурах, например, США, процессу обучения сопутствует высокая конкуренция среди учащихся, в которой важны

внешние атрибуты академических успехов (портфолио, победы в олимпиадах, конкурсах и т. п.). Таким образом, в «маскулинном» обществе при обучении поощряется соперничество и результат, в «феминном» часто награждается само поведение студента.

С точки зрения параметра «избегание неопределенности», в культурах с низкой степенью избегания неопределенности процесс обучения часто ведется по нестандартизированным программам, предусматривающим высокий уровень вариативности и нечеткие критерии оценивания. В противоположность этому, в культурах с высокой степенью избегания неопределенности весь процесс обучения подчинен строгому расписанию и инструкциям согласно учебно-методическим регламентациям. В странах, стремящихся избежать неопределенности, преподаватель должен максимально четко обозначить задачу, способы ее решения, сроки и критерии оценки перед студентами. Студенты более склонны к получению высшего образования из-за чувства долга перед родителями и обществом, а не из-за того, что надо или хочется, как в культурах с ориентацией на долгосрочный временной горизонт.

Таблица 2

Этнометрические параметры Г. Хофстеде
в контексте образовательной коммуникации

Этнометрические параметры		Специфика коммуникации
	1	2
Дистанция власти	Низкая дистанция	– Студентоцентрированная модель. – Инициатива со стороны студента поощряется. – Коммуникация инициируется студентами. – Преподаватель поощряет студентов к выбору собственного пути обучения. – Студентам разрешается вступать в противоречия и критиковать преподавателя. – Эффективность обучения – двусторонний процесс. Важна постоянная обратная связь и интерактивность.
	Высокая дистанция	– Модель, центрированная на преподавателе. – Инициатива не поощряется и исходит от преподавателя.

Продолжение табл. 2

	1	2
		– Коммуникация инициируется преподавателем. – Студенты строят образовательную траекторию исходя из заранее оговоренных моделей. – Студентам не разрешается вступать в противоречия и критиковать преподавателя. – Эффективность обучения зависит от преподавателя и регламентируется им.
Индекс коллективизма/индивидуализма	Высокий индекс коллективизма	– Студенты говорят только тогда, когда спрашивает и поощряет преподаватель. – Индивидуальные выступления поощряются только в малых группах. – Гармония и эмоциональный комфорт в процессе обучения являются доминантой. – Ни преподаватель, ни студент не должен «терять лицо» в рамках учебной коммуникации. – Преподаватель может давать поблажки в некоторых случаях, делая скидку на индивидуальное отношение.
	Высокий индекс индивидуализма	– Любой вопрос может носить характер дискуссии. – Индивидуальные выступления и точки зрения обучающихся поощряются всегда. – Конфронтация, столкновение точек зрения и несогласия являются нормальной частью учебного процесса. – «Потеря лица» – признак профессиональной несостоятельности. – Единые требования ко всем.
Феминные/ маскулинные культуры	Феминные культуры	– Процесс обучения ориентирован на среднего студента. – Считается ценным такое качество, как умение адаптироваться в коллективе. – Поощряется неконфликтность студента, умение работать в команде, умеренность во всем. – Студенты выбирают предметы исходя из личного интереса.

Окончание табл. 2

	1	2
	Маскулинные культуры	– Процесс обучения ориентирован на лучшего студента. – Считаются ценными академические успехи студента. – Умение презентовать собственные достижения и уникальность. – Поощряется выделение из коллектива. – Студенты выбирают предметы, ориентируясь на их полезность для будущей карьеры.
Индекс избегания неопределенности	Низкий уровень	– Студенты чувствуют себя комфортно вне четких рамок расписаний и регламентов. – Преподаватель может сказать «я не знаю». – Хороший преподаватель использует простой язык. – Студенты предпочитают инновационный подход. – Преподаватели рассматривают несогласие по предметным вопросам как стимулирующий фактор.
	Высокий уровень	– Студенты чувствуют себя комфортно в условиях жесткого расписания и регламентов. – Преподаватель должен быть компетентен во всем. – Хороший преподаватель использует академический язык. – Студенты поощряются за аккуратность и соответствие заранее оговоренным требованиям. – Преподаватели рассматривают несогласие по предметным вопросам как личную нелояльность.

Согласно концепции Э. Дейла и его последователей, эффективность обучения определяется ролью студента в образовательном процессе. Наиболее эффективным способом усвоения информации является активное включение студента в образовательный процесс: участие в дискуссиях, выступления, имитация и выполнение реальной деятельности. А наименее эффективными – слушание лекций и чтение материалов. Позже, на основе «конуса опыта» Э. Дейла, была разработана пирамида обучения (рис. 1), из которой также видно, что наиболее эффективными способами обучения являются

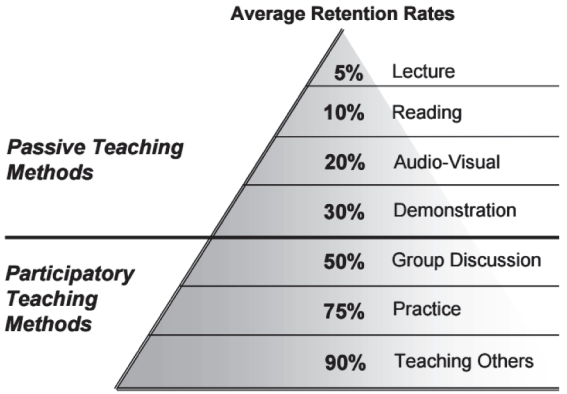


Рис. 1. Пирамида обучения (National Training Laboratories)

выполнение конкретной практики и непосредственное применение или обучение других. Однако мы утверждаем, что данная концепция эффективности методов обучения справедлива для сообщества западных стран, члены которого обладают импульсивными параметрами ККПЛ. В незападных культурах, преимущественно восточноазиатских, наблюдается обратная ситуация: методы обучения, определенные Э. Дейлом как наименее эффективные, являются наиболее продуктивными (так называемый «парадокс азиатского ученика»). Таким образом, по-нашему мнению, параметры эффективности обучения будут отличаться в зависимости от культуры и характеризующего ее ККПЛ. Дихотомия «активного» и «пассивного» обучения в данной работе будет определяться используемыми методами обучения, а не их эффективностью согласно концепции Э. Дейла, так как при разных типах обучения используются разные способы, которые соответственно являются наиболее продуктивными для каждого типа.

Таким образом, исходя из концепции «активного» и «пассивного» стиля обучения, мы определяем учащихся в восточноазиатских культурах как «обучаемых», а в западноевропейских – как «обучающихся». Обучаемые усваивают информацию посредством лекций, чтения учебной литературы и демонстрации полученных знаний, следовательно, основной целью пассивного обучения студентов является передача им фундаментальной информации по курсу. Обучающиеся, напротив, предпочитают получать информацию через дискуссии и практическое применение знаний, так как

Рис 2. Стратегия «пассивного» обучения

цель активного обучения заключается в развитии критического мышления и креативности у студентов для решения нестандартных задач и ситуаций. Также необходимо отметить, что стиль обучения во многом обуславливается преподавателем – его профессиональной и национальной культурой, так же как и тип поведения студента.

Следовательно, мы можем сделать вывод о том, что в условиях пассивного обучения для «обучаемых» характерно взаимодействие с образовательной средой следующего типа: образовательная среда воздействует на студента, формируя личность и профессиональные компетенции во время образовательного процесса (рис. 2); в условиях активного обучения для «обучающихся» – хотя образовательная среда по-прежнему оказывает влияние на студента, он также самостоятельно воздействует и принимает участие в ее формировании – может изменять и адаптировать ее (рис. 3).

Возникновение информационной среды инициировало возникновение образовательной кросс-культуры, что повлекло за собой определенного рода системные изменения, которые так или иначе найдут отражение в трансформации элементов организации информационно-образовательной среды. Критерии, по которым должна строиться поликультурная образовательная среда новой формации, видятся нам следующим образом: коммуникационный критерий (изменение традиционных форм коммуникации

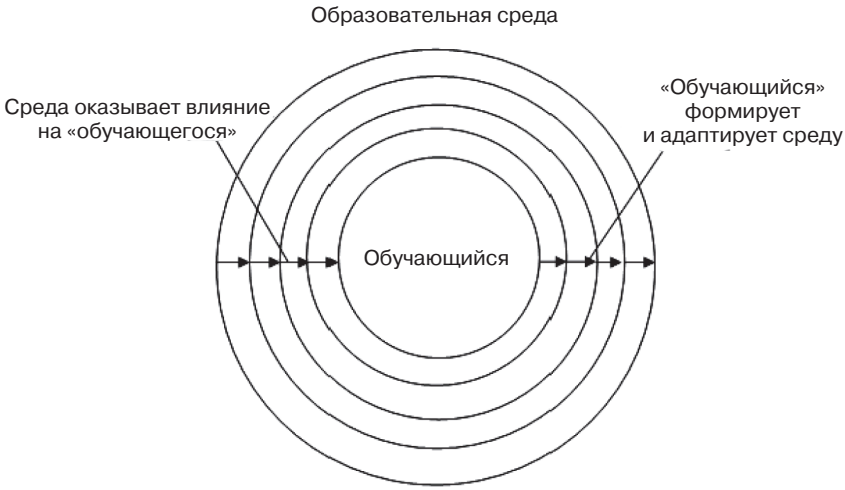


Рис 3. Стратегия «активного» обучения

в системе «преподаватель – студент»), методический (появление культурно-адаптивных методов работы с учебной информацией), контентный (дифференциация и возможная неоднородность учебного контента в образовательном процессе), информационный (разработка и использование образовательных ресурсов, учитывающих культурную специфику восприятия и работы с информацией).

Приведем еще одну цитату:

> С помощью информационных процессов люди присваивают общественно-исторический опыт предыдущих поколений. Зарождается информология – общая наука (метанаука) об информации, формирование которой стало объективной необходимостью и объединяет изучение всех проявлений и сторон информации, всех процессов, связанных с нею[3].

Эта цитата характерна, в ней отражается технологичность в отношении к педагогике. Иначе, человек – это результат: субъект, присваивающий деятельность предыдущих поколений (историческая деятельность) при возможном посильном участии текущего поколения. У автора цитаты ушло из рассмотрения, что «присвоение» – результат воспитательной, образовательной деятельности в постоянно изменяющейся среде, иногда с совершенно неконтролируемой скоростью передачи информации.

Мы (не только педагоги и ученики) находимся в ЭОС (электронно-образовательная среда). Поэтому передача информации в обезличенной или латентной форме для педагога – и помощь и опасность. Его готовность к работе в агрессивной информационной среде – реалии современных образовательных сред – свойство этого периода развития педагогической науки.

Вторая часть приведенной цитаты свидетельствует об упрощении понимания того, что же есть педагогическая информация. В специфической профессиональной деятельности педагога источником является текст (сообщение), транслируемый личностной средой и макросредой ученика, восприятие же текстов, т. е. чтение текстов, написанных с помощью различных письмен (разно-образье людей), и является содержанием профессиональности педагога. Здесь уместно привести соображение выдающегося старшего современника В.В. Налимова:

> Смыслы распаковываются всегда через тексты. Человек для нас – это текст, или, точнее, *многообразие текстов* (курсив наш. – *В. Ж. et al.*), грамматику и семантику которых мы хотим охватить единым, вероятностно задаваемым взглядом[4].

В философии Налимова существование смыслов во Вселенной так же естественно, как материальное, или энергетическое ее воплощение, а информация – «оболочка» смыслов, «семантический континуум которых неизменен и распаковывается каждый раз заново на языке современных представлений. Поэтому эволюция есть по существу изменение семантики текстов, через которые мы видим мир»[5]. И наконец, по Налимову, «*Смыслы* – это то, из чего создаются *тексты,* с помощью *языка*. *Тексты* – это то, что создано из *смыслов* с помощью *языка*. *Язык* – это средство, с помощью которого из *смыслов* рождаются *тексты*. Триада становится синонимом *сознания*» [6].

Таким образом, к схеме «текстура, текст и культура восприятия Ученика в педагогической деятельности, информационное общество» добавляется «скорость чтения» и «скорость ответной реакции», при этом рефлексия в этой деятельности становится профессиональной чертой, т. е. не действие по инструкции, а по обстоятельству, по тому, как научаешься читать сознание людей и ориентироваться в Реке времени[7].

Теперь приведем второй пример. Это пример деятельности педагога в реальной школьной практике. Хорошо известно, что в школьный период обучения ребенок при переходе из начальной школы в основную испытывает большие нервные перегрузки,

поскольку меняется среда комфортного его существования. Теперь ему встречаются различные преподаватели, со своими стилями, часто непривычными, ведущие новые учебные дисциплины. Причем и его личностную среду, и внешнюю среду (т. е. микро- и макросреды) *читают* люди с различными человеческими возможностями и совершенно различными реакциями, иногда совершенно непонятными ребенку. Итак, проще всего рассмотреть эту модельную ситуацию на примере преподавания математики с 5-го по 9-й классы обучения. В этот период в начале – стрессовые перегрузки воспитательной природы, а в конце периода – перегрузки психофизического свойства – взросление детского организма. Заметим, что математика как воспитывающая учебная дисциплина еще «удобна» тем, что в этот период изменяется и характер смыслов и информационная насыщенность потоков учебной информации на уроках, т. е. воспитывается стиль мышления. Здесь мы заметим, что изменение отношения к математике в государстве в худшую сторону ощутили на себе подданные США, которые спешно стали менять (усложнять содержание, менять методику преподавания математики) во времена Рейгана–Буша. Теперь же новациями в нашем традиционном образовании (российском традиционном математическом образовании) меняют стиль мышления, так, чтобы он не соответствовал нашему ментальному образу (с соборного на индивидуально-потребительский, иначе совершается переход от рассудительного стиля на стиль исполнения предписаний).

Обратимся к смыслам, вложенным в документы современного математического образования[8]. Это смыслоформирующие документы. Взглянем на них с помощью педагогической информатики.

Поскольку нас интересуют смыслы и расставленные приоритеты образовательной политики, можно будет представить, что же скрывается за декларированием целей образовательной политики и достижения необходимых знаний, умений, навыков. Итак, критерий «передача, обработка и хранение информации». Обратимся к пункту 11: «Предметные результаты освоения основной образовательной программы основного общего образования с учетом общих требований Стандарта и специфики изучаемых предметов, входящих в состав предметных областей, должны обеспечивать успешное обучение на следующем уровне общего образования»[9].

Сначала обратим внимание на структуру этого пункта: 11.1. – Филология; 11.2. – Общественные науки; 11.3. – Математика и информатика; 11.4. – Основы духовно-нравственной культуры народов России; 11.5. – Естественнонаучные предметы; 11.6. – Искусство; 11.7. – Технология; 11.8. – Физическая культура и основы безопасности жизнедеятельности.

Сравним состав текстов вводных к каждому подпункту пункта 11 (табл. 3).

Таблица 3

Блок дисциплин	Предметная область (попросту предмет научной дисциплины или некоторое приближение к ней)
1	2
«Изучение предметной области “Филология” – языка как знаковой системы, лежащей в основе человеческого общения, формирования гражданской, этнической и социальной идентичности, позволяющей понимать, быть понятым, выражать внутренний мир человека»	То, что в этом блоке родной язык и литература являются средством общения и представлением чувств индивида, известно в российской педагогике более чем сто лет и является традиционной значимой целью обучения.
«Изучение предметной области “Общественно-научные предметы” должно обеспечить [...]»	Легко заметить, что здесь не указана предметная область. Общественные дисциплины подпадают к условной градации в область так называемого гуманитарного знания, т. е. знания, не являющегося в строгом смысле научным знанием, иначе, гуманитарное знание зависит от интерпретации индивида. Это же замечание относится и к первому блоку.
«Изучение предметной области “Математика и информатика” должно обеспечить: [...]»	Здесь не указана предметная область. Математика является языком, на котором «говорит» природа и развивается техника. Также известно, что ей придавалось особое педагогическое значение еще со времен Петра Первого. Определение же предметной области можно было бы дать и по Ф. Энгельсу.
«Изучение предметной области “Основы духовно-нравственной культуры народов России” должно обеспечить: [...]»	Не указана предметная область. Возможно, духовно-нравственные отношения в обществе определяются в первую очередь культурой и их значением для государства. Поэтому нам кажется, что здесь все понятно.

Окончание табл. 3

1	2
«Изучение предметной области “Естественнонаучные предметы” должно обеспечить: [...]	В этом случае не указана предметная область. То, что учебный предмет «География» сделан не естественным предметом, вызывает наше удивление. Понятно, что предметная область наук, входящих в этот блок дисциплин, относится к частным языкам природы, универсальной (инвариантной) частью их является универсальный математический язык абсолютных смыслов.
«Изучение предметной области “Искусство” должно обеспечить: [...]»	Здесь, так же как и в предыдущих разделах, не указана предметная область. Возможно, эту предметную область следовало бы характеризовать как прикладную часть языка эмоций при формировании образов различной природы.
«Изучение предметной области “Технология” должно обеспечить: [...]»	То, что есть люди, которые познают мир с помощью «рук», т. е. практических действий, и есть люди с развитым абстрактным представлением о мире, в возрастной психологии известно более чем двести лет. Возникают некоторые сомнения в возможности развивать проектное мышление без развития естественнонаучного и математического мышления, более естественно при таком подходе развить исполнительское мастерство.
«Изучение предметной области “Физическая культура и основы безопасности жизнедеятельности” должно обеспечить: [...]	Известно, что человеку с развитым мышлением небезразлично свое тело и среда, в которой он пребывает.

Рамки этой статьи не дают возможности более детально разобрать терминологический состав обоснований всех подпунктов, но первые наши наблюдения довольно точно характеризуют подпункты пункта 11 (наблюдения – правая колонка таблицы 3).

Иначе, передача информации с вложенными смыслами явно, оказывается, носит декларативный характер. В документе существует пример строгой декларации, а именно: не определено понятие *информационно-образовательная среда*. Но нам интересен в исследовании аспект преподавания математики в период основной школы (5–9 классы), особенно в части переходов: от начальной к основной и, от основной к старшей школам. Рассмотрим далее[10] смыслы, которые базируются на документе[11]. Противоречащими друг другу являются в нашем исследовании ряд методических понятий, например: *оперирование понятиями* – знать определение понятия, уметь пояснять его смысл, уметь использовать понятие и его свойства при проведении рассуждений, доказательств, решении задач; *оперировать на базовом уровне* – распознавать (подчеркивание наше. – *Авт.*) конкретные примеры общих понятий по характерным признакам, выполнять действия в соответствии с определением и простейшими свойствами понятий, конкретизировать примерами общие понятия. В первом определении все ясно, во втором же мы имеем дело с представлением о математике, где нет примата уровня понимания, а главное – уровень узнавания. В последнем случае язык математики отступает на второй план, т. е. не нужно объяснять, не нужно обосновывать, но нужно распознать, нужно в лучшем случае вспомнить, а что говорил учитель или написано в книжке, или где-то мы что-то подобное обсуждали на уроке!» Т. е. происходит отказ от традиционной математической ценности – ответ на вопрос «почему?» заменяется ответом на вопрос «а что же там говорилось?» И еще один пример из следующего источника[12]. Что же значит: «*Свободно оперировать понятиями* – знать определение понятия, знать и уметь доказывать свойства (признаки, если они есть) понятия, характеризовать связи с другими понятиями, представляя одно понятие как часть целостного комплекса, использовать понятие и его свойства при проведении рассуждений, доказательств, решении задач»? После этой сентенции можно спросить: а что же, ***знать*** *определение понятия* можно не *зная* и не *умея доказывать свойства этого понятия*? Это явный пример гуманитарного подхода к математике, т. е. здесь знание образа, которое составляет определение, но не понимание сущности, главного, для чего нужно это понятие, и что будет, если его как-нибудь видоизменить, например, переставив порядок символов.

По прочтении этого документа, относящегося к управлению подачей информации из математической области знаний и методических аспектов математического образования, кажется, что писали его не специалисты-математики, а, возможно, чиновники-педагоги с математическим педагогическим образованием. Или это может

быть результат преобразований в области современного педагогического образования в России? К сожалению, современное положение в системе принятия решений таково, что ответственность за подобные «новации» не несет ни один чиновник. Возможно, это традиционное российское свойство: поставить задачу, а «внизу» сделают как надо! Но раньше «внизу» (учителю, преподавателю) было время «на подумать», а теперь же педагогу нужно заниматься бумажным оформлением своей деятельности. Таким образом, в части переработки, пусть поверхностной, мы приходим к наблюдению, что существует в рассматриваемом документе множество неоднородных понятий, т. е. понятий разного уровня абстракций, а некоторые из них вообще не определены.

Осталось рассмотреть эти документы на предмет сохранения информации. Сохранение этих документов произойдет естественным образом в ИПС (информационно-педагогической среде), поскольку продуктивность в бумагооформительстве педагогической деятельности бьет все «рекорды» в тоннах отчетов вместо творческой и спокойной работы с учениками и над собственным развитием.

В заключение нужно сказать, что если первый из приведенных примеров мы относим к непосредственному воплощению педагогической теории в образовательной деятельности, то второй пример – уже из области управления методикой такой деятельности. В том и в другом примере по существу реализуются возможности педагогической информатики как педагогической дисциплины, которая делает явной еще одну грань современной педагогики. Несомненно, современные образовательные технологии без педагога, умеющего работать в различных типах сред, понимающего и прогнозирующего развитие индивидуума в них, представляющего значение ментальных свойств личности в образовательном процессе, постоянно работающего над саморазвитием, окажутся пустыми декларациями, разрушающими государство.

Как правило, студенты, попадая в «чужую» культурную образовательную среду, постепенно адаптируются к ней под влиянием особенностей семиотического пространства данной среды. Преподаватели, знающие среду изнутри, во многом учитывают специфику учебного заведения. Однако при работе с поликультурной аудиторией могут возникать некоторые трудности: поликультурный состав аудитории не позволяет ориентироваться только на представителей одной культурной группы, так как учебный материал должен быть донесен до всех студентов в равной, но посильной степени восприятия. Данная проблема может быть решена за счет выбора разных методов обучения для представителей разных культур и развития культурного интеллекта педагогов, а также

за счет изменения дизайна (возможно, и ландшафта) педагогической среды. Выбор же индивидуальных траекторий обучения, приведение их в интерактивное состояние в каждый момент времени обучения индивида являются задачами области педагогической информатики, решение которых по форме связано с техническими методами представления знаний, но, по существу, они относятся к сугубо педагогическим проблемам образования.

Примечания

[1] *Хуторская Л.Н.* Информационная педагогика // Эйдос. 2002. 25 авг. [Электронный ресурс] URL: http://www.eidos.ru/journal/2002/0825.htm (дата обращения: 14.09.2016).

[2] [Электронный ресурс] URL: http://www.psyoffice.ru/slovar-s0.htm (дата обращения: 14.09.2016).

[3] *Хуторская Л.Н.* Указ. соч.

[4] *Грановский Ю.В., Дрогалина Ж.А., Маркова Е.В.* «Я друг свобод...»: В.В. Налимов: Вехи творчества: В 2 т. Т. 1. Томск; М.: Водолей Publishers, 2005. С. 18.

[5] Там же.

[6] Там же. С. 19.

[7] *Жаров В.К., Таратухина Ю.В.* Педагогический конструктивизм в кросс-культурной среде. М.: Янус-К, 2015.

[8] Федеральный государственный образовательный стандарт основного общего образования (утв. Приказом Министерства образования и науки Российской Федерации от 17 декабря 2010 г. № 1897, в ред. Приказа Минобрнауки России от 29.12.2014 № 1644); Примерная основная образовательная программа основного общего образования. Одобрена решением Федерального учебно-методического объединения по общему образованию (протокол от 8 апреля 2015 г. № 1/15, в ред. протокола № 3/15 от 28.10.2015) [Электронный ресурс] URL: http://fgosreestr.ru/wp-content/uploads/2015/06/primernaja-osnovnaja-obrazovatelnaja-programma-osnovogo-obshchego-obrazovanija.docx (дата обращения:15.09.2016).

[9] *Грановский Ю.В., Дрогалина Ж.А., Маркова Е.В.* Указ. соч. С. 7.

[10] Примерная основная образовательная программа основного общего образования...; Концепция развития математического образования в Российской Федерации (утв. Распоряжением Правительства Российской Федерации от 24 декабря 2013 г. № 2506-р). [Электронный ресурс] URL: http://rg.ru/2013/12/27/matematika-site-dok.html (дата обращения 14.09.2016).

[11] Федеральный государственный образовательный стандарт основного общего образования (утв. Приказом Министерства образования и науки Российской Федерации от 17 декабря 2010 г. № 1897).

[12] Примерная основная образовательная программа основного общего образования.

А.А. Бастрон, Е.В. Желудева

Медиаконвергенция в журналистике: от классики к универсальности

В статье исследуется тема использования информационных технологий в работе журналиста. Проанализированы задачи и возможности журналистики в условиях медиаконвергенции. Рассматривается проблема вузовской подготовки «универсального» журналиста в процессе интеграции информационных и коммуникативных технологий в единый информационный ресурс.

Ключевые слова: медиаконвергенция, средства массовой информации, информационные технологии, краудсорсинг, облачные технологии, процессы трансформации, контент.

Научно-техническая революция, интенсивное развитие электронно-вычислительной техники, стремительное распространение новых средств связи нашли свое отражение во всех средствах массовой информации. Возможность использовать новые информационные и коммуникационные технологии способствовала созданию разветвленной информационной индустрии и новой медиакультуры, а Интернет сыграл свою основополагающую роль в формировании облика современных СМИ.

Именно Всемирная компьютерная сеть стала новым средством передачи текстовой, звуковой и визуальной информации в режиме реального времени, обусловила интерактивный и мультимедийный характер коммуникаций, несвойственный «традиционным» массмедиа. Она объединила в себе все основные формы деятельности, свойственной средствам массовой информации (сбор, обработку, перемещение, хранение информации)[1].

Многочисленные сетевые издания предоставили пользователям широкие интерактивные возможности. Интерактивность как главное их отличие от печатных СМИ сделала осуществимым главное желание пользователя: принимать и отправлять сообщения, быть одновременно и потребителем информации, и активным участником коммуникационного процесса.

Профессия журналиста обогатилась многочисленными аспектами, связанными с технологиями информационных систем: оперативностью получения информации, многоканальностью коммуникаций, универсальностью информации, обязанной быть принятой на всех существующих цифровых платформах и языках[2].

Таким образом, возникла необходимость рассмотреть задачи и возможности журналистики в условиях медиаконвергенции: от классики к универсальности.

Следует отметить, что в настоящее время изменившиеся условия массового коммуницирования все больше и больше нуждаются в «универсальных» журналистах. И хотя журналистика по-прежнему остается востребованной, меняются формы, способы сбора и передачи информации, что актуализирует потребность в теоретическом, научном осмыслении творческой деятельности журналистов в условиях медиаконвергенции.

В отечественной научной литературе процессам конвергенции в СМИ, а также проблемам по общим вопросам организации творческой деятельности журналиста «доцифровой эпохи» большое внимание уделяли такие известные исследователи, как С. Корконосенко, Е. Прохоров, Я. Засурский, И. Дзялошинский, Л. Свитич, Г. Лазутина, В. Олешко, М. Ким, В. Мансурова и многие другие ученые.

К вопросам теоретического обоснования процессов трансформации, происходящих в СМИ, обращались в своих трудах М. Кастельс, Э. Тоффлер, М. Маклюэн, З. Бауман, П. Вирильо, А. Бард и Я. Зодерквист и др.

Вопросы влияния конвергенции на деятельность СМИ и журналистов нашли свое отражение в работах зарубежных исследователей М. Дейзе, П. Брэдшоу и других.

Следует отметить также научные изыскания Е. Вартановой, М. Лукиной, С. Балмаевой, А. Калмыкова, И. Кирии, А. Качкаевой, Ю. Пургина, В. Овчинникова, исследовавших процессы конвергенции в СМИ, проанализировавших формы и методы творческой деятельности профессионального журналиста в условиях медиаконвергенции.

Влияние информации на прогресс человечества резко изменилось по сравнению с предшествующим периодом. Нелинейность и скачкообразный характер стали главными особенностями данного процесса трансформации[3].

Очевидно, что современная журналистика в качестве самоорганизующейся и многоаспектной системы функционирует по законам нелинейной динамики и синергетики, и профессия жур-

налиста, представляющая собой яркую динамическую структуру, в данном случае подвержена значительным изменениям.

Цифровая эпоха поставила перед ней новые задачи: журналист выходит в своей работе на смешанный формат. Он тесно взаимодействует с читателем, техническим специалистом, использует в работе инновационные технологии: краудсорсинг, облачные технологии, базы данных. Кратко обратимся к основным понятиям, связанным с этим явлением.

Так, конвергентная журналистика (*англ.* convergence journalism) – это процесс слияния, интеграции информационных и коммуникативных технологий в единый информационный ресурс. Слово «конвергенция» происходит от латинского «convergo» – «сближаю» и в английском языке означает «схождение в одной точке». Теоретик журналистики М.М. Павликова, ссылаясь на канадского исследователя СМИ и коммуникаций Д. Макуэйла, утверждает, что это распространение одного и того же содержательного продукта по разным каналам и при помощи разных средств.

В широком смысле конвергенция понимается не только как взаимное влияние явлений, но и как взаимопроникновение технологий, стирание границ между ними, слияние[4].

Российская журналистка и радиоведущая А.Г. Качкаева классифицирует конвергенцию следующим образом. По ее мнению, это бизнес-стратегия медиахолдинга; тактика; «переупаковка»; объединение сбора и производства информации; новый вид подачи данных. То есть буквально «передача единого контента разными средствами (с помощью текста, звука или видео) и по разным каналам коммуникации (пресса, телевидение, радио, интернет)»[5].

Впервые данный подход к деятельности СМИ и определение понятия «система средств массовой информации» были введены профессором В.С. Хелемендиком в 1977 г. Он обозначил основные принципы координации средств массовой коммуникации: специфичность, систематическое корректирование содержания, функциональную взаимозависимость и необходимость признания общности функций печати, радио и телевидения и их взаимодействия. Это позволило ученому еще в 1970-е годы выдвинуть гипотезу о том, что «со временем организационная структура журналистики изменится и ныне самостоятельные газета, радио, телевидение сольются в своеобразные объединения с общим информационным центром, планированием и измерением эффективности их воздействия на массы»[6].

Идея нового переосмысления конвергенции принадлежит также американскому социологу и публицисту Дэниелу Беллу.

Так, с 1970-х годов понятие «конвергенция» все чаще употреблялось для обозначения интеграции информационных и коммуникационных технологических устройств, например, компьютеров, телефонов, телевизоров. Дальнейшее развитие термин получил в ходе обсуждений о дерегулировании телекоммуникационного рынка в США и вещательного рынка в Западной Европе в 1980-х годах. И лишь в 1990-е годы быстрое внедрение Интернета в привычную жизнь миллионов людей нашло широкое практическое применение[7].

Понятие «конвергенция» (медиаконвергенция) можно отнести еще и к процессу «сотрудничества» и взаимопроникновения новейших технологий и традиционных массмедиа, результатом чего становится появление новых разновидностей СМИ.

Невозможно говорить о медиаконвергенции, не касаясь новейших технологий – в первую очередь дигитализации (оцифровки) массовых коммуникаций. Как известно, совсем недавно все средства связи действовали разрозненно, широко использовались различные «технологические платформы» и коммуникационные сети. Существовало четкое распределение коммуникационных ролей: печатная периодика, вещание, телефонная связь, компьютерные услуги в системном on-line. Благодаря цифровому сжатию информации дигитализация позволила «уплотнить» информационные потоки, что, в свою очередь, дало возможность осуществлять многоканальную массовую коммуникацию с обратной связью[8].

С помощью дигитализации начал осуществляться процесс стирания границ между различными типами массовых коммуникаций: теперь, используя цифровую технологию, можно применять интегрированные устройства, работающие одновременно как телефон, телевизор и персональный компьютер. Так, например, в настоящее время мы можем наблюдать проникновение мобильной телефонии, развивающейся на цифровой платформе, в медийную сферу: читать газеты, смотреть телевидение, слушать радио можно с помощью сотового телефона. Гибкость цифровых технологий позволяет телекоммуникационным, вещательным и информационным компаниям выходить за пределы своих традиционных областей[9].

Неоднозначность определений понятия «медиаконвергенция» уже само по себе яркое свидетельство сложности, «многослойности» этого феномена. Явление медиаконвергенции обладает технологическим измерением, так как характеризуется слиянием разнотипных технологий производства и распространения информации, позволяющих различным СМИ предоставлять аудитории медиатексты, сочетающие текстовые и аудиовизуальные элементы содержания.

Под влиянием конвергенции медиатексты, продуцированные разными СМИ, приобретают свойства мультимедийности и интерактивности. Но существует и системное измерение медиаконвергенции (под ее влиянием радикально трансформируется сложившаяся система массмедиа и распределение коммуникационных ролей внутри нее), а также и профессиональное измерение, поскольку под влиянием этого процесса происходят изменения в организации и содержании труда журналистов и других коммуникаторов, в характере предъявляемых к ним профессиональных требований[10].

Медиаконвергенция соединяет, переплетает «традиционные» СМИ; она внедряет их в Сеть, перемежая письменную речь с устной, комбинируя текст, звук и изображение; она рождает новые качества журналистики, которая становится мультимедийной, интерактивной и гипертекстовой.

За последние 20 лет мультимедиа стали темой многочисленных исследований. И это объяснимо, ведь прогресс в развитии компьютерной техники, компьютерных носителей и компьютерных сетей как способа трансляции позволил объединить внутри одного носителя – компакт-диска – разные и ранее необъединимые средства коммуникации – визуальную, текстовую и звуковую[11].

На сегодняшний день работа с видеомонтажом, с цветом, компьютерная обработка фотографий, анимация, инфографика, работа со звуком достигли необычайных высот: они свободно интегрируются в медиа. А уровень технологий создания продукта СМИ позволяет реализовать практически любую творческую идею.

Таким образом, в настоящее время одной из наиболее успешных концепций развития медиаиндустрии и отношений между СМИ и аудиторией стали мультимедиа. По определению специалистов, это интеграция двух или более коммуникационных средств и каналов с компьютером[12].

Теперь мультимедиа – это единая информационная система, в основе которой оперируют несколько типов СМИ. Их информационные продукты частично или полностью проникают друг в друга и могут объединять текст, звук, графику, фото, видео в одном цифровом представлении[13].

Говоря о медиаплатформе, надо отметить, что это целостная система взаимозависимых компонентов, позволяющая реализовать целевые модели жизни общественно значимой информации, производимой для регулярного потребления профессиональными конвергентными редакциями, а также участниками социальных сетей. Для потребителя медиаплатформа предстает в качестве сервиса, предоставляющего услуги по просмотру,

прочтению, прослушиванию, комментированию и дополнению печатного, а также аудиовизуального контента. Важнейшие компоненты медиаплатформы на сегодняшний день – интернет-ресурс, печатный носитель, радио- и телеканал.

Процесс конвергенции в медиабизнесе позволяет одновременно распространять контент в виде мультимедийных форм через разные медиаплатформы, что дает возможность создавать кросс-медийные и межотраслевые холдинги[14].

В то же время не следует забывать, что конвергенция выступает лишь как определенный этап в процессе изменения формы средств массовой информации в целом. В результате анализа развития СМИ можно заметить, что с самого начала различные типы СМИ сосуществовали в условиях совместного развития и интеграции. Конвергенция компьютерных и телевизионных технологий – это общая тенденция технологического развития[15].

Институционально медиаконвергенция не является «новым» процессом, она лишь тождественна кооперированию на предыдущих этапах вхождения в систему СМИ новых компонентов. Современные процессы медиаконвергенции представляют собой результат взаимодействия различных факторов, наиболее важными из которых стали научно-технический прогресс, изменение информационного потребления аудитории и усиливающаяся рыночная конкуренция[16].

Контент (*англ.* content – содержание) – любое информационно значимое (содержательное) наполнение информационного ресурса (например, веб-сайта) – тексты, графика, мультимедиа – вся информация, которую пользователь может загрузить на диск компьютера с соблюдением законности, как правило, только для личного пользования.

В IT-сфере чаще всего этот термин употребляют, когда речь идет о текстовом наполнении веб-сайта. Весь web-контент (*англ.* web content) охраняется законом об авторском праве, поскольку представляет собой продукт интеллектуального труда, является собственностью конкретных авторов и владельцев. Один из важных критериев контента – его доступность, актуальность, значимость, достоверность в отношении предоставления данных, а также соответствие контента поставленным целям по его поиску. Количество и качество контента характеризуются степенью пользовательского интереса к web-сайту, на котором он размещен.

Важной характеристикой контента является его уникальность: он не должен иметь аналогов на ресурсах схожей тематики. Чаще всего этот термин применим к текстовому наполнению сайтов

(текстовый контент). Уникальные статьи, написанные для конкретного ресурса, размещаются на нем и являются первоисточником, а любая перепечатка допустима только с разрешения законного владельца и на его условиях.

Краудсорсинг (*англ.* crowdsourcing: crowd – «толпа» и sourcing – «использование ресурсов») – привлечение к решению тех или иных проблем инновационной производственной деятельности широкого круга лиц для использования их творческих способностей, знаний и опыта по типу субподрядной работы на добровольных началах с применением инфокоммуникационных технологий.

Этот термин был впервые введен писателем Джеффом Хау и редактором журнала «Wired» Марком Робинсоном в июне 2006 г. Всю необходимую работу делают неоплачиваемые или малооплачиваемые специалисты-любители, тратящие свое свободное время на создание контента, решение проблем или даже на проведение исследований и разработку. Для объяснения концепции привлечения трудовых ресурсов, координируемых через Интернет, приводится сравнение с добровольными вычислениями, в которых через Интернет привлекаются на добровольной основе вычислительные ресурсы широкого круга пользователей[17] (при этом иногда и сами проекты добровольных вычислений относят к одной из форм краудсорсинга[18]). Отличительный признак краудсорсинга – разбивка работы на мелкие части (модули)[19].

Таким образом, понятие «краудсорсинг» можно представить как безвозмездную деятельность круга лиц для достижения цели, поставленной владельцем коммуникационного процесса.

Понятие «дигитализация прессы» означает не просто «газету в цифровой форме». Ее главные задачи: создание платформ для сбора, упаковки и распространения информации в цифровой среде (IT-платформа), перестройка организационной структуры редакции и укрепление жизнеспособности производства цифровых медиапродуктов, повышающих конкурентоспособность и стирающих границы между газетой и другими средствами массовой информации[20].

Конвергентная редакция – это предприятие, созданное для производства общественно значимых журналистских текстов в режиме многоканальности, интерактивности, непрерывности коммуникационных потоков.

Развитие медиаотрасли ведет к необходимости перехода журналистов в транспрофессионалы. Их базовые транспрофессиональные компетенции включают в себя и специализацию в определенной области, и способность к межпрофессиональной коммуникации и трансдисциплинарному синтезу знаний,

и ориентацию на сочетание фундаментальных исследований с практическим решением проблем, и непрерывное саморазвитие и самосовершенствование[21].

Социальная ориентированность, широкий кругозор, предрасположенность к журналистской деятельности, опора на навыки и умения – вот основные константы базового ядра профессии журналиста. Но при этом в функциональной модели журналистской деятельности появились и динамические переменные: владение минимумом технических навыков для сбора и фиксации информации, способность выполнять разные роли и разные виды работ одновременно и в условиях многозадачности, обладание отточенными навыками написания коротких заметок и броских заголовков, продвижение контента и т. д.

Кроме того, журналист обязан быть мобильным, оперативным, активным, открытым к новым каналам распространения информации; способным адаптироваться к языку электронных СМИ. Для журналиста расширился диапазон реализации его творческих возможностей, включающих более креативный подход к подаче информации на разных платформах, а также избавление от части рутинных операций.

В настоящее время журналисты должны обладать большей гибкостью мышления, сохранять баланс между работой на результат и творческой составляющей. В деятельности по созданию журналистских текстов на первый план выступают эвристические зоны для активизации творческого процесса и создания эксклюзивного контента.

Новый диапазон функций журналиста значительно расширился: требуются новые формы подачи текста, творческий подход к его созданию, целенаправленное повышение его качества. Решается сложная задача по переходу от платформенного подхода подачи информации к помещению ее в подходящий формат и ее связи с другими форматами[22].

И конвергенция в данном случае выступает в качестве основной технологии для адаптации СМИ к новым технологическим условиям. Существование конвергентных редакций, в основе которых лежит интеграция всех возможных на сегодняшний день форматов медиапродукта, не является чем-то фантастическим, это реальность, которую обязаны учитывать все СМИ. Именно в конвергенции есть перспективы для развития современной журналистики[23].

Конечно, одновременно существуют и традиционные редакции, где журналисты работают в прежнем формате. И хотя перспектива внедрения мультимедийности и конвергенции в указанную отрасль очевидна, переходные процессы в ней происходят недостаточно

динамично. Журналисты же, лишенные возможности использовать современные информационные технологии, по существу находятся в информационной изоляции, не позволяющей им полноценно ориентироваться в окружающей действительности.

Можно уверенно сказать, что журналистика как профессия, субъекты которой выносят приговор общественным процессам, сегодня не имеет альтернативы. Социум по-прежнему будет нуждаться в общественно значимой информации, которая будет перепроверена, проанализирована и доставлена по всему спектру доступных каналов дистрибуции потребителю. И на данном этапе развития информационных технологий все эти функции в едином комплексе способны реализовать профессиональные журналисты, поскольку именно эта профессия остается главной точкой притяжения в медиасистеме[24].

Развитие информационных и мультимедийных технологий, изменение структуры потребления информации, когда аудитория оперативно получает информацию в удобное ей время и по удобному ей каналу, потребовало от журналистов дополнительных навыков, переосмысления подходов и принципов работы. Сами журналисты признают трансформацию своей профессии, расширение ее границ. Это вызвано объективными факторами: кардинальным ускорением передачи информации, беспрецедентным в истории увеличением ее объемов, появлением новых носителей, ее доступностью для максимально широкой аудитории. Ключевыми здесь выступают фактор времени и скорость информационных взаимодействий, а критерием успеха – оперативность индивидуального решения. Для подобной системы характерно постоянное формирование в ней новых элементов, систем и взаимосвязей между ними.

Новые каналы получения и передачи информации трансформируют текст СМИ, позволяя обойти традиционные форматные ограничения, поскольку гипертекст, свойственный конвергентным СМИ, состоит из неограниченного количества элементов и вариантов их сочетания. Основным в этих условиях становится язык визуальной коммуникации. Ведь журналистское произведение состоит уже не только из текста, а сопровождается графикой, аудио, видео, а на мобильных устройствах может даже реагировать на тактильные прикосновения пользователя[25].

Смешанный формат становится уделом журналистской деятельности, традиционная журналистика перестраивается, тесно взаимодействуя с читателем и с техническими специалистами. И это предопределяет необходимость использования инновационных технологий работы журналиста с окружающей медиасредой: краудсорсинга, облачных технологий, баз данных.

Средства массовой информации, в той или иной степени испытавшие на себе многообразное влияние конвергенции, могут обозначаться как конвергированные (т. е. затронутые процессом конвергенции, приобретшие некие общие либо сходные характеристики под воздействием этого процесса).

И это не обязательно полностью интернет-базирующиеся СМИ, поскольку наряду с сетевым подразделением многие конвергированные средства массовой информации сохраняют «традиционные» структуры и информационные продукты («бумажный» тираж, эфирные теле- и радиотрансляции).

Все более востребованными в журналистике становятся универсальные журналисты, поскольку процесс конвергенции базируется на единовременном производстве контента и последующем его тиражировании на разных информационных платформах. В этих условиях журналисту обязательно надо владеть базовыми технологиями, применяемыми в мультимедийной редакции: обладать навыками верстки, цифровой фотографии, видео- и звукового монтажа, работы с компьютерными базами данных, уметь посредством современных сетей добывать и проверять необходимую информацию.

Технологическая революция предъявляет высокие требования к профессии журналиста: требуются профессионалы, способные выполнять одновременно функции и дизайнера, и редактора, и менеджера, и копирайтера, и психолога, и экономиста, и проектировщика, и верстальщика. Кроме того, транспрофессиональный подход к данной проблеме определяет также и беспрецедентное развитие профессии журналиста в будущем, обеспечиваемое динамикой развития отрасли.

И такие дисциплины, как «Современные информационные технологии» и «Интернет-ресурсы», представленные в общеобразовательной программе подготовки будущих журналистов, призваны дать студентам необходимые знания по данной тематике[26] .

Знания и умения, приобретенные студентами в результате изучения этих курсов, будут использованы ими для поиска, обработки, структурирования, хранения и применения информации в процессе изучения практически всех дисциплин данного направления.

В процессе обучения у студентов должны сформироваться следующие компетенции:

1) способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;

2) способность ориентироваться в современной системе источников информации в целом и по отдельным отраслям знаний и сферам общественной практики, знание и умение владеть основными методами, способами и средствами получения, хранения и обработки информации, умение использовать различные программные средства, базы данных, работать в Интернете и использовать его ресурсы, пользоваться поисковыми системами, работать с информацией в глобальных компьютерных сетях;
3) знание возможностей электронных баз данных, методов работы с ними, способов участия в их создании;
4) знание методов редактирования текстов СМИ, основанных на использовании новых технологий.

Таким образом, в результате освоения дисциплины обучающийся должен:
– *знать:* фундаментальные разделы информатики; основные новые информационные технологии; основные опасности и угрозы, возникающие в процессе информационного развития общества;
– *уметь:* работать с традиционными носителями информации; создавать базы данных и использовать ресурсы Интернета; применять навыки и умения из области информатики для решения профессиональных задач; соблюдать основные требования информационной безопасности;
– *владеть:* навыками использования программных средств; навыками работы в компьютерных сетях; основными методами получения, обработки, хранения и передачи информации.

И все же, несмотря на возросшую доступность цифровых технологий, и у профессионалов, и у будущих журналистов ни в коем случае не должна создаваться иллюзия того, что наличие интернета и облачных технологий дает повод «расслабиться» и позволить себе не повышать свой интеллектуальный уровень. Ведь лишь используя собственные интеллектуальные ресурсы, в условиях дефицита времени и диктата технологий журналист может быстро связывать факты, оперировать большими массивами информации и находить кратчайший путь для оптимизации своей деятельности. Только благодаря глубокому и обширному интеллектуальному запасу могут рождаться по-настоящему креативные формы творческой деятельности журналиста.

Журналистика – это профессия энергичных, ищущих, остро и глубоко мыслящих людей. А журналист – это человек энциклопедических знаний, обладающий широчайшим кругозором, постоянно стремящийся узнать что-то новое, интересное и донести эти сведения до социума.

Изменяются не только медиасистемы, но и философия, профессиональные принципы, подход к пониманию природы и задач профессии, которой можно научить, только сохраняя ее этические и нравственные принципы.

Несмотря на технологизацию журналистики, творчество не перестало быть сутью этой профессиональной деятельности. Кроме того, исследования актуальных проблем существования современной журналистики в системе массовых коммуникаций указывают на то, что журналистика как система трансформируется за счет динамических изменений «ядра» своей деятельностной основы: принципов функций и методов деятельности, которые по-прежнему социально обусловлены и идейно-нравственно детерминированы[27].

И поэтому следует вновь подчеркнуть, что профессия журналиста по-прежнему остается в зоне творчества, и проблеме теоретического обоснования ее трансформаций, в том числе и в условиях медиаконвергенции, еще предстоит найти свое решение, пройдя путь от классики к универсальности.

Примечания

[1] *Баранова Е.А.* Конвергенции СМИ глазами российских журналистов-практиков // Вестник Московского университета. Серия 10: Журналистика. 2010. № 4. С. 91–100.

[2] *Баранова Е.А.* Процесс конвергенции СМИ и журналистское образование // Медиаскоп. 2010. № 1. [Электронный ресурс] URL: http://www.mediascope.ru/node/528 (дата обращения: 4.03.2016).

[3] *Шестеркина Л.П.* Подготовка журналиста универсального типа в условиях конвергенции СМИ // Вестник электронных и печатных СМИ. № 13. [Электронный ресурс] URL: http://vestnik.ipk.ru/index.php?id=2099 (дата обращения: 3.03.2016).

[4] *Павликова М.М.* Сетевые технологии и журналистика: Эволюция финских СМИ. М.: РИП- холдинг, 2001. С. 12.

[5] *Качкаева А.Г.* Журналистика и конвергенция. Почему и как традиционные СМИ превращаются в мультимедийные. М., 2010.

[6] *Хелемендик В.С.* Союз пера, микрофона и телекамеры. М.: Мысль, 1977. С. 96.

[7] *Вартанова Е.Л.* К чему ведет конвергенция в СМИ. М.: Аспект-Пресс, 1999. С. 86.

[8] Журналистика и медиаобразование в XXI веке: Сб. науч. тр. Междунар. научно-практ. конф. / Под ред. А.П. Короченского. [Электронный ресурс] URL: http://window.edu.ru/catalog/pdf2txt/008/62008/31914?p_page=15 (дата обращения: 3.03.2016).

[9] Там же.

[10] Интернет и интерактивные электронные медиа: Исследования: Сб. Лаборатории медиакультуры, коммуникации, конвергенции и цифровых технологий / Под ред. И.И. Засурского. М.: МГУ, 2007.
[11] *Качкаева А.Г.* Указ. соч. С. 15.
[12] СМИ в меняющейся России: Коллективная монография / Под ред. Е.Л. Вартановой. М.: Аспект Пресс, 2010.
[13] *Вартанова Е.Л.* От человека социального к человеку медийному // От книги до Интернета: Десять лет спустя. М.: МедиаМир, 2009.
[14] *Уразова С.Л.* Конвергентно-интеграционные аспекты эволюции СМИ // Вестник ВГИК. 2010. № 5.
[15] Журналистика и конвергенция: Почему и как традиционные СМИ превращаются в мультимедийные / Под ред. А. Г. Качкаевой. М.: Фокус-медиа, 2010.
[16] Интернет-СМИ: Теория и практика / Под ред. М.М. Лукиной. М.: Аспект Пресс, 2011.
[17] *Хау Дж.* Краудсорсинг: Коллективный разум как инструмент развития бизнеса. М.: Альпина Паблишер, 2012.
[18] *Егерев С.В., Захарова С.А.* Краудсорсинг в науке // Наука. Инновации. Образование: Альманах / Российск. науч.-исслед. ин-т экономики, политики и права в науч.-техн. сфере (РИЭПП). М.: Языки славянской культуры, 2013. № 14. С. 175–186.
[19] *Хау Дж.* Указ. соч.
[20] *Егерев С.В., Захарова С.А.* Указ. соч.
[21] *Шестеркина Л.П.* Указ. соч.
[22] *Рэндалл Д.* Универсальный журналист. СПб.: Национальный ин-т прессы, 2000.
[23] *Дворко Н.И.* Мультимедиа: Творчество, техника, технология. СПб.: СПбГУП, 2005.
[24] *Шестеркина Л.П.* Указ. соч.
[25] *Копылов О.В.* Особенности творческой деятельности журналиста в условиях медиаконвергенции: Автореф. дис. ... канд. филол. наук. Екатеринбург, 2013.
[26] *Желудева Е.В.* Культура учебного труда в журналистском образовании: учебное пособие. М.: МГГЭУ, 2015. С. 13–14.
[27] *Копылов О.В.* Указ. соч.

Н.Ю. Бобкова, А.А. Роганов,
С.М. Строганова, Н.Н. Теодорович

Дистанционные технологии в преподавании технических дисциплин: тенденции, перспективы, трудности

Статья посвящена вопросам использования информационно-коммуникационных технологий и технологий дистанционного обучения в работе преподавателя высшей школы. Рассмотрены тенденции развития применения дистанционных технологий в современных условиях. Обобщен опыт создания и применения дистанционного обучения техническим дисциплинам. Выявлен и проанализирован ряд трудностей, характерных для реализации дистанционного обучения техническим дисциплинам на примере дисциплины «Электротехника», а также предложен вариант решения проблемы посредством применения кейс-технологий.

Ключевые слова: дистанционное обучение, информационно-коммуникационные технологии в образовании, образовательная среда, кейс-технология, дистанционное обучения техническим дисциплинам.

С возрастанием роли ИКТ в образовательном процессе актуализируются изменения в форме участия педагога в сопровождении учебной деятельности. В современных условиях традиционная парадигма образования, при которой на всех ступенях обучения педагог выступал не только носителем знаний, но и влиял на формирование профессионального мастерства и развитие личности обучающегося, дополняется необходимостью разработки, проектирования и наполнения информационно-образовательной среды и предметно-образовательного пространства с учетом специфики направления подготовки. В концепции социально-экономического развития Российской Федерации до 2020 г. приоритетным направлением применения информационно-коммуникационных технологий является развитие новых форм и методов обучения, в том числе дистанционных[1].

Перечисленные выше предпосылки, несомненно, оказывают воздействие на формирование системы высшего образования и дают толчок для разработки и создания большого количества курсов дистанционного обучения по различным дисциплинам.

В системе высшего образования применение дистанционных технологий дает возможность для развития глобализационных процессов, которые обусловлены возможностью выбора обучения у лучших преподавателей и в лучших учебных заведениях. Также хорошо известны плюсы применения дистанционных технологий в образовательном процессе: от экономии времени на перемещение к месту работы и обучения, расходов на транспорт, эксплуатацию помещений, повышение самоорганизации студента, доступности обучения для студентов с ограниченными возможностями здоровья до возможности изучать предмет в свободном режиме и темпе[2].

Кроме очевидных достоинств дистанционного образования, существует ряд трудностей и проблем, которые можно условно разделить на две категории:

– трудности, связанные с организацией дистанционного обучения специализированным предметам при отсутствии непосредственного контакта преподавателя и студента;
– готовности преподавателя к созданию качественного контента.

Рассмотрим подробнее обе категории.

Основная роль в проектировании информационной образовательной среды отводится преподавателю. При этом он не только наполняет ее учебной информацией, но и структурирует ее в соответствии с планом рабочей дисциплины и с учетом компетентностного подхода при формировании знаний, умений и навыков.

Специфика технического образования заключается в том, что применение информационных технологий и дистанционного обучения при динамичности смены наукоемких технологий не всегда в состоянии полностью заменить процесс обучения с преподавателем. Отсутствие непосредственного контакта преподавателя с аудиторией также усложняет и ограничивает применение некоторых образовательных инструментов, затрудняет процесс оценивания степени обученности студента и приобретенных навыков работы.

Любой процесс обучения, в том числе и дистанционного, состоит из следующих составляющих:

– изучение теоретического материала, размещенного в электронном виде в системе дистанционного обучения, или посещение лекций, проводимых преподавателем онлайн в формате вебинара или видеолекций;

– закрепление знаний, полученных в ходе изучения теории, путем выполнения практических заданий, участия в семинарских занятиях, проводимых в формате форума или чата;
– выполнение заданий контрольного блока.

Законодательно определены общие требования к техническим и структурным характеристикам применяемых вузами систем дистанционного обучения: это модульно-ориентированные платформы с автоматизацией освоения дисциплины.

Схематически минимально необходимый комплект инструментов СДО приведен на рисунке 1.

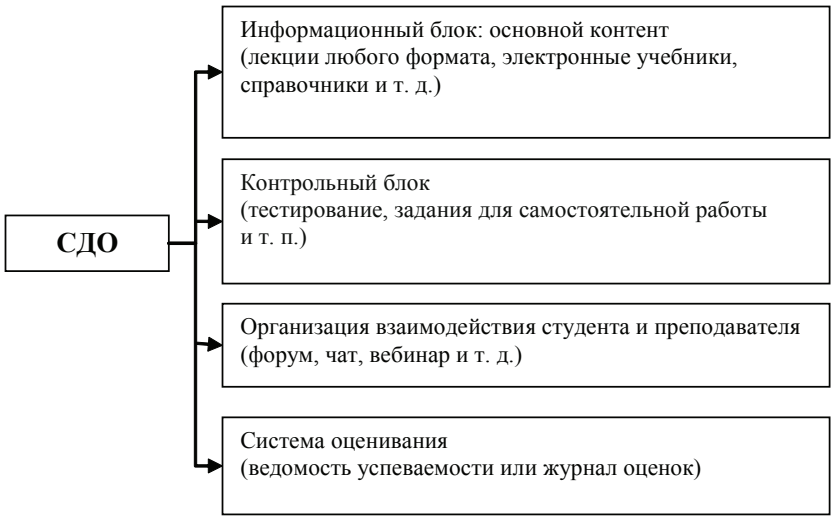


Рис.1. Модули СДО

Основной сложностью при реализации дистанционного обучения специализированным дисциплинам является отсутствие традиционных аудиторных лабораторных и практических занятий, требующих использования лабораторных установок, дорогостоящего программного обеспечения. Удаленное подключение студента к серверу с учебным программным обеспечением позволяет решить данную проблему в случае обучения дисциплинам, рабочий инструментарий которых может быть представлен программно[3]. В случае, когда необходимо использование программно-аппаратного комплекса, например, при обучении электротехнике, удаленное подключение невозможно. Вариантом решения данной проблемы может быть применение компьютерных симуляций.

Рис. 2. Алгоритм формирования кейсов дисциплины «Электротехника»

Так, при обучении студентов по дисциплине «Электротехника» с применением ИКТ и дистанционных технологий была выбрана смешанная модель обучения с использованием кейс-технологий[4]. Применяемая в процессе обучения платформа eLearningServer 4G отвечает всем требованиям законодательства для реализации дистанционного обучения. Применение дистанционных технологий в данном случае можно рассматривать как дополнение к общему образовательному маршруту. Использование кейс-технологий преподавания электротехники позволяют гибко сочетать традиционные формы обучения с дистанционным обучением. Алгоритм применения кейс-технологий при обучении дисциплине «Электротехника» приведен на рисунке 2.

Структурирование учебного материала проводится в соответствии с рабочей программой и учебным планом дисциплины. Учебно-методические материалы компонуются в отдельные блоки – кейсы. Каждый кейс, в свою очередь, состоит из лекционного,

практического и проверочного блока. Выбор формы проведения занятий (смешанная форма/дистанционная) определяется исходя из технических условий реализации обучения.

Основной упор делается на проведение ряда аудиторных занятий: установочные лекции, семинары, консультации. Далее формируется пакет для самостоятельного изучения материала, при котором контакт преподавателя с аудиторией осуществляется в режиме онлайн, а основной лекционный и лекционно-практический материал выкладывается в системе дистанционного обучения.

Примерное распределение видов занятий кейса по дисциплине «Электротехника» при смешанном обучении приведено в таблице и может при необходимости изменяться преподавателем при анализе успеваемости студентов в учебной группе[5].

Таблица

Пример построения кейса
«Электрические цепи постоянного тока», 29 часов

№ п/п	Наименование вида занятий	Форма проведения	Количество часов
1	Установочная лекция	Аудиторное занятие	2
2	Лекция по темам 1, 2, 3	Дистанционно	2 × 3
3	Ответ на задание по теме	Дистанционно	4
4	Решение ситуационных задач	Дистанционно	2
5	Семинар в форме форума	Дистанционно	2
6	Консультация	Аудиторное занятие	2
7	Кейс-стади	Дистанционно	2
8	Опрос (контрольное занятие)	Дистанционно	1
9	Тестирование	Дистанционно	2

В данном перечне по сравнению с традиционным обучением появляются виды занятий, характерные для дистанционной формы обучения.

Решение производственных ситуационных задач. Главное отличие такого занятия от решения обычной задачи заключается

в изменении привычной последовательности действий. Если алгоритм решения обычной задачи состоит из:
– четкой постановки задачи с указанием исходных данных;
– выбора варианта решения;
– непосредственно самого решения;
– выдачи ответа,
то решение ситуационной задачи начинается с поиска исходных данных для определения проблемы, и уж только после этого происходит выбор пути решения и выработка самого решения. Таким образом, студент должен сам определить источник проблемы.

Например, при расчете сложных цепей постоянного тока обучаемый должен самостоятельно определить количество ветвей, узлов и контуров, составить уравнения по первому и второму закону Кирхгофа, произвести вычисления и убедиться, что ход решения верен.

Кейс-стади – искусственно разработанная, вымышленная ситуация профессиональной деятельности обучающегося в соответствии с темой кейса. Направлена на самостоятельный поиск источников для ответа на поставленный вопрос и зачастую используется при работе в группе. Возможным путем поиска правильного решения может быть его перенаправление к информационно-библиотечным ресурсам, мотивация студента к более глубокому изучению вопроса, «погружению» в проблему. Последующий совместный анализ поиска решения и самого решения позволяют преподавателю не только определить, насколько студент усвоил теоретический материал, но и оценить степень его готовности применять на практике приобретенные практические навыки.

Например, если при расчете сложной цепи постоянного тока обучаемый не может оценить правильность хода решения, значит, теоретический материал не усвоен.

Процесс обучения может проводиться посредством формирования небольших групп студентов для более эффективного взаимодействия студентов, обмена опытом и определения «проблемных зон» в обучении. Ответы на вопросы разбирались преподавателем на консультации, проводимой аудиторно.

Вторым актуальным вопросом применения информационно-коммуникационных и дистанционных технологий является готовность преподавателя вуза к разработке качественного контента. Одним из эффективных способов решения этой проблемы может стать повышение квалификации профессорско-преподавательского состава в области применения информационно-коммуникационных технологий[6]. На сегодняшний день разработана масса дополнительных программ повышения квалификации данного

направления подготовки. При выборе определенной программы следует учитывать следующее:

– степень готовности преподавателя организовывать процесс обучения в виртуальном пространстве (навыки работы в применяемой в образовательной организации СДО: авторизация в системе; размещение готового материла; принципы формирования и корректировки журнала успеваемости; реализация простейших контрольных мероприятий; организация взаимодействия преподавателя и студента: проведение онлайн-семинаров в формате форума, проверка знаний в формате чата, проведение опросов);
– уровень знаний специализированного программного обеспечения для создания контента (создание учебных flash-роликов, разработка анимации, использование различных графических редакторов, применение 3D-моделирования и т. п.).

Для кейса дисциплины «Электрические цепи постоянного тока», помимо простейших процедур размещения в СДО лекционного и тестового материала, было организовано семинарское занятие в формате форума с использованием закрытых ответов на вопрос преподавателя и открытого обсуждения изучаемой темы с дальнейшим оцениванием активности студентов и правильности ответов и занесением результата в ведомость успеваемости.

Таким образом, проектирование и создание курса дистанционного обучения технической дисциплине «Электротехника» выявили ряд определенных трудностей как в организации процесса обучения, так и в создании контента. Создание курсов дистанционного обучения гуманитарным дисциплинам изначально располагает большим набором педагогического инструментария, и соответственно требует меньшей подготовленности преподавателя в области знаний и применения ИКТ. При реализации технических дисциплин лучший результат показала смешанная модель обучения. Несмотря на наличие аудиторных занятий в графике обучения, которые, как правило, были посвящены разбору ошибок и сложных производственных ситуаций и использование программно-аппаратного лабораторного оборудования, очевидна необходимость применять на практике более сложное программное обеспечение и новые информационные технологии[7]. В свою очередь, разбиение дисциплины на кейсы позволило равномерно распределить нагрузку преподавателя по формированию контента. Затраты на обучение преподавателей работе в СДО и создание качественного контента компенсируются минимизацией необходимых материальных ресурсов.

Примечания

[1] Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 г. [Электронный ресурс] URL: http://base.consultant.ru (дата обращения: 14.05.2016).

[2] *Мисаилов А.Ю., Роганов А.А., Теодорович Н.Н., Мохов А.И.* Педагогические инновации в современном высшем профессиональном образовании // Науковедение. 2014. № 6 (25) (Интернет-журнал). [Электронный ресурс] URL: http://naukovedenie.ru/PDF/67PVN614.pdf (дата обращения: 14.05.2016).

[3] *Мустафин Ю.А., Шадрин Д.Б.* Дистанционное образование в технических вузах. Решение проблемы преподавания специализированных дисциплин // Современная техника и технологии. 2015. № 2. [Электронный ресурс] URL: http://technology.snauka.ru/2015/02/5751 (дата обращения: 15.05.2016).

[4] *Денисов С.В., Теодорович Н.Н.* Перспективные методики преподавания электротехнических дисциплин // Инновационные технологии в современном образовании: Сб. тр. по материалам III Междунар. науч.-практ. Интернет-конф. 18 дек. 2015 г. М.: Научный консультант, 2016. С. 173–177.

[5] Там же.

[6] *Мисаилов А.Ю., Роганов А.А., Теодорович Н.Н., Мохов А.И.* Указ. соч.

[7] *Роганов А.А., Теодорович Н.Н.* Тенденции развития облачных технологий // Современные информационные технологии / Под науч. ред. В.М. Артюшенко. М.: Научный консультант, 2015. С. 125–132.

А.Е. Сатунина, Л.А. Сысоева

Использование моделей оценки процессов при формировании панелей индикаторов информационно-аналитической системы организации

В статье рассматриваются подходы к использованию методологии оценки процессов, представленной в серии стандартов ГОСТ Р ИСО/МЭК 15504, при разработке контрольных панелей информационно-аналитической системы организации. В результате проведенного анализа была представлена технология формирования обеспечивающих компонентов процесса оценки схемы измерения, базовой модели процесса, модели оценки процесса с целью получения набора индикаторов процессов для визуализации их на информационных (контрольных) панелях аналитической системы. Технология формирования модели оценки процесса представляет собой системный подход к разработке шкал, индикаторов и показателей процессов.

Ключевые слова: информационно-аналитическая система; процессный подход в управлении; оценка процесса; модель оценки процесса; профиль процесса.

В настоящее время одним из направлений повышения эффективности управления организацией является использование информационно-аналитических систем. Все больше организаций для получения качественной информации, необходимой для принятия решений на различных уровнях управления, ставят задачу внедрения в существующую IT-инфраструктуру системы аналитической обработки данных. По прогнозам Gartner, рынок BI и аналитических платформ будет расти со среднегодовым темпом роста 8,7% до 2018 г.[1]

Функциональные и корпоративные информационные системы, применяемые в организациях, порождают огромные объемы оперативной информации, которые требуют предварительной аналитической обработки, прежде чем они могут быть использованы менеджерами различного уровня. Именно анализ первичной

информации делает ее действительно ценной, способной улучшить обоснованность управленческих решений.

Актуальной становится задача построения корпоративной системы управления с помощью информационно-аналитических систем, что позволяет учитывать специфику не только отдельных областей управления, но и связи между всеми сферами деятельности организации.

Растет интерес и к такому классу аналитических систем, как системы, управляемые событиями, осуществляющие возможность непрерывного мониторинга и запуска предопределенных бизнес-процессов при выделении критических состояний или обнаружении заданных событий.

Другой аспект, влияющий на активизацию использования систем аналитической обработки информации, связан с широким внедрением процессного управления (BPM), где большую роль играет аналитическая информация по показателям результативности бизнес-процессов.

Современные технологии аналитических систем позволяют внедрять и применять аналитические приложения на всех уровнях организационной структуры и управления. На стратегическом уровне – осуществлять мониторинг показателей эффективности деятельности организации, на тактическом уровне – выполнять оперативную оценку и расчет ключевых показателей с возможностью моделирования различных сценариев развития событий, на операционном уровне – встраивать аналитические средства в функциональные ИС, обеспечивающие повседневную деятельность организации, и в оперативные бизнес-процессы.

Информационно-аналитические системы предоставляют в зависимости от поставленных задач и квалификации пользователей различные средства для визуализации данных – отчеты, OLAP-кубы, информационные (контрольные) панели, карты показателей[2].

Менеджеры, осуществляющие разработку стратегических, тактических решений, применяют инструментарий OLAP-кубов, который позволяет проводить многофакторный анализ с требуемой степенью детализации.

Менеджеры, которые принимают управленческие решения и выполняют анализ эффективности по отдельным направлениям деятельности организации, наиболее заинтересованы в применении карт показателей и контрольных панелей, на которых в виде шкал и индикаторов отображается состояние организации в целом, с возможностью переключения по направлениям ее деятельности.

Менеджеры структурных подразделений применяют контрольные панели для решения своих текущих задач, мониторинга за ходом выполнения отдельных видов работ и операций, контроля деятельности отдельных работников и подразделения в целом. Информационные панели позволяют получать сведения о реализации взаимосвязанных задач или процессов в смежных структурных подразделениях, что повышает координированность и согласованность взаимодействия структурных подразделений.

Поэтому цель данной статьи – попытаться определить методологии и подходы к формированию информационных (контрольных) панелей в системах аналитической обработки информации с учетом процессного подхода в управлении организацией.

Методологические аспекты оценки процессов

Внедрение систем аналитической обработки информации в IT-инфраструктуру организации обусловлено рядом предпосылок[3]:

- использование единого источника для оперативной отчетности (построение корпоративного хранилища данных на основе общих справочников и показателей);
- применение единой методологии формирования ключевых показателей (единая интерпретация и методика расчета показателей);
- автоматизация сбора и консолидации данных для анализа;
- принятие решений с учетом информации о ключевых показателях и процессах на различных уровнях управления (создание корпоративной системы отчетности).

Ряд предпосылок, связанных с формированием и расчетом ключевых показателей, предполагают активное применение на всех уровнях менеджмента организации процессного подхода. В связи с этим возрастает роль аналитической обработки показателей процессов для принятия наиболее обоснованных управленческих решений.

В методологии ITIL отмечается, что эффективность управления обеспечивается путем регулярного проведения мониторинга и оценки показателей процессов, постоянного улучшения их на основе аналитической обработки полученной информации[4].

Процесс оценки – это определение того, в какой степени стандартные процессы организации вносят вклад в достижение ее бизнес-целей и помогают организации сфокусироваться на необходимости непрерывного улучшения процессов[5].

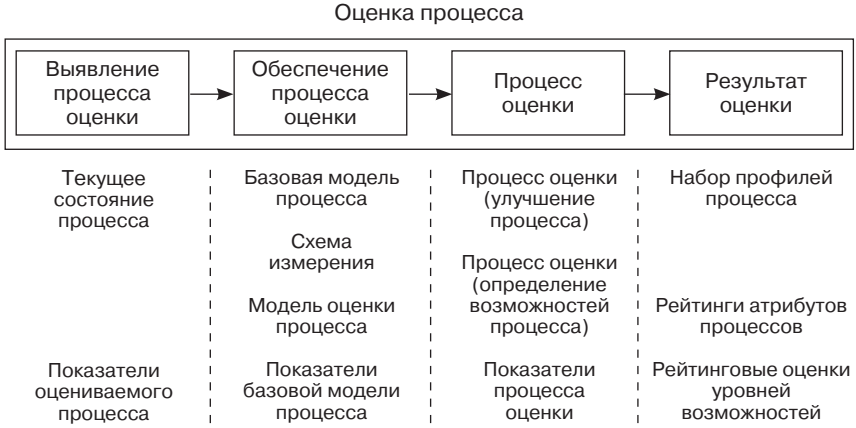


Рис. 1. Схема проведения оценки процессов в соответствии с методологией стандартов ГОСТ Р ИСО/МЭК 15504

В стандартах серии ГОСТ Р ИСО/МЭК 15504 определены подходы к оценке процессов, проводимых с целью улучшения процессов и определения возможностей процесса.

Общая схема проведения оценки процессов в соответствии с методологией стандартов ГОСТ Р ИСО/МЭК 15504[6] включает ряд шагов (рис. 1):

– выявление процесса (процессов), подлежащего (подлежащих) оценке;
– подготовка обеспечивающих составляющих оценки процесса: разработка одной или нескольких базовых моделей процесса, схемы измерения и модели оценки процесса;
– проведение процесса оценки с целью улучшения процесса или определения возможностей процесса;
– формирование отчетных документов по результатам оценки процесса.

Таким образом, под оценкой процесса понимается упорядоченная оценка процесса организации относительно модели оценки процесса[7].

Основными элементами процесса оценки являются (рис. 2):

– процесс оценки (планирование, сбор данных, валидация данных, определение рейтингов атрибутов процессов, формирование отчетов);

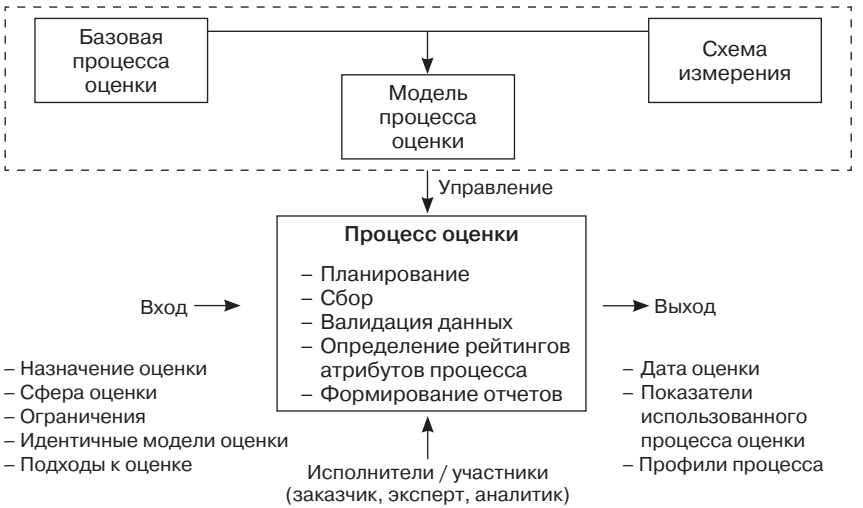


Рис. 2. Схема основных элементов процесса оценки (ГОСТ Р ИСО/МЭК 15504–2–2009)

– входные данные/объекты (назначение, сфера действия, ограничения, идентичность используемой модели оценки, подход к оценке и др.);
– выходные данные/результат (дата оценки, профили процессов, использованный процесс оценки и его показатели и др.);
– исполнители (роль и ответственность участников процесса: заказчик, эксперт, оценщик(и), аналитик);
– обеспечивающие компоненты процесса оценки (базовая модель процесса, схема измерения, модель оценки процесса).

Схему процесса оценки можно представить в виде функциональной модели процесса[8] на основе методологии SADT (рис. 2).

Использование базовой модели процесса и модели оценки процесса позволяет получить характеристику текущего состояния процесса, провести анализ текущих показателей и выявить роль и риски, присущие процессу, а затем определить приоритеты в направлениях по улучшению процесса.

Кроме того, имея профили базовых моделей процессов, можно провести анализ текущих возможностей выделенных процессов относительно целевых профилей возможностей процессов для выявления потенциальных рисков в текущем состоянии организации, в тех сферах деятельности, где участвуют контролируемые процессы.

Методика формирования обеспечивающих компонентов процесса оценки

Рассмотрим более подробно методику формирования обеспечивающих компонентов процесса оценки.

Этап 1. Инициация оценки процесса.

Обоснование необходимости проведения оценки процесса

1.1. Цель проведения оценки процесса:
- улучшение процесса;
- определение возможностей процесса.

1.2. Определение области оценки:
- перечень процессов, которые должны быть исследованы в организации;
- наивысший уровень возможностей, который должен быть исследован для каждого процесса;
- владельцы процессов (подразделения);
- контекст процесса (масштаб подразделения, прикладная область продуктов или услуг, ключевые характеристики продуктов или услуг).

1.3. Подходы к оценке (используемые методологии, стандарты).

1.4. Ограничения оценивания (максимальная продолжительность оценки, количество и тип объективных свидетельств, используемых при оценке, контроль конфиденциальной информации и др.).

1.5. Идентичность модели оценки процесса (идентичность базовой(ых) модели(ей) процесса(ов)).

Этап 2. Формирование схемы измерения

Последовательность и содержание работ по формированию схемы измерения представлены в таблице 1.

Таблица 1

Формирование схемы измерения

№	Содержание	Пример реализации
1	Формирование шкалы категорий процесса. Шкала категорий процесса отражает возрастание возможностей выполнения процесса от осуществления, которое неспособно достичь требуемых результатов процесса, до реализации, когда достигаются текущие и планируемые бизнес-цели	Шкала категорий процесса (балльная): П0 – неполный (0, уровень 0) П1 – осуществленный (1, уровень 1) П2 – управляемый (2, уровень 2) П3 – установленный (3, уровень 3) П4 – предсказуемый (4, уровень 4) П5 – оптимизирующий (5, уровень 5)

Продолжение табл. 1

<table>
<tr><td>2</td><td>Формирование атрибутов процессов и их показателей</td><td></td></tr>
<tr><td>2.1</td><td>Выявление атрибутов для каждой категории процесса</td><td>Атрибуты процессов:
П1: АП 1.1, АП 1.2
П2: АП 2.1, АП 2.2, АП 2.3
...</td></tr>
<tr><td>2.2</td><td>Определение допустимых значений атрибутов или признаков достижения этого атрибута</td><td>Атрибуты процессов и их признаки:
П1: АП 1.1, АП 1.2
АПП 1.1, АПП 1.2
П2: АП 2.1, АП 2.2, АП 2.3
АПП 2.1, АПП 2.2, АПП 2.3
...</td></tr>
<tr><td>2.3</td><td>Формирование шкалы рейтингов атрибутов.
Степень (уровень) достижения атрибута процесса определяется по шкале рейтингов атрибутов</td><td>Шкала рейтингов атрибутов (упорядоченная и процентная)
Н – не достигнут – 0–15%
Ч – частично достигнут – 15–50%
В – в основном достигнут –50–85%
П – полностью достигнут – 85–100%</td></tr>
<tr><td>3</td><td>Сопоставление уровней оценки процесса комбинаций достижений признаков атрибутов процесса.
Каждый атрибут процесса получает рейтинговую оценку</td><td>Комбинации достижений признаков атрибутов процесса
Атрибут процесса: АП 1.1
Признаки атрибута:
АПП 1.1.1, АПП 1.1.2
АП 1.1= Ч, если
<table><tr><td></td><td>Н</td><td>Ч</td><td>В</td><td>П</td></tr><tr><td>АПП 1.1.1</td><td>+</td><td>+</td><td>–</td><td>–</td></tr><tr><td>АПП 1.1.2</td><td>+</td><td>+</td><td>+</td><td>+</td></tr></table></td></tr>
<tr><td>4</td><td>Формирование рейтинговых оценок атрибутов процессов.
Набор рейтингов атрибутов процесса образует профиль этого процесса</td><td>Профиль процесса
Процесс: Пр1
Категория: П1
Атрибуты процесса: АП 1.1, АП 1.2
<table><tr><td>П1</td><td>Н</td><td>Ч</td><td>В</td><td>П</td></tr><tr><td>АП 1.1</td><td>+</td><td>+</td><td>+</td><td>+</td></tr><tr><td>АП 1.2</td><td>+</td><td>+</td><td>+</td><td>–</td></tr></table></td></tr>
</table>

Окончание табл. 1

<table>
<tr>
<td>5</td>
<td>Формирование модели рейтинговой оценки процесса. Достигнутый процессом уровень формируется из рейтингов атрибутов этого процесса в соответствии с моделью рейтинговой оценки процесса</td>
<td>
<table>
<tr><th>Уровень/ категория</th><th>Атрибут процесса</th><th>Рейтинговая оценка</th></tr>
<tr><td>Уровень 1/ П1</td><td>АП 1.1

АП 1.2</td><td>П

В</td></tr>
<tr><td>Уровень 2/ П2</td><td>АП 1.1
АП 1.2
АП 2.1
АП 2.2
АП 2.3</td><td>П
П
П
В или П
В</td></tr>
</table>
</td>
</tr>
</table>

На данном этапе разрабатывается общая схема и методика создания модели рейтинговой оценки процесса и формирования профилей процессов.

Этап 3. Формирование базовой модели процесса

Модели для оценки процесса включают:

– базовую(ые) модель(и) процесса;
– модель оценки процесса.

Базовая модель процесса представляет собой определение процесса в жизненном цикле, описанная в терминах назначения и выходов процесса, вместе с архитектурой, отражающей взаимосвязи между процессами[9].

Базовая модель процесса разрабатывается с учетом стандартов и нормативных документов, соответствующих контексту процесса, и содержит:

– определение области применения модели;
– описание процесса;
– описание взаимосвязей между процессами в базовой модели;
– описание взаимосвязей между базовой моделью процесса и контекстом ее использования.

Базовая модель процесса применяется в ходе оценки процесса для сопоставления текущих показателей процесса с показателями базовой модели на основе принятой схемы измерения.

Описание процесса в базовой модели включает определение профиля и рейтинговой оценки процесса, которые разрабатываются с учетом методики, принятой в схеме измерения (табл. 2).

Таблица 2

Формирование профиля
и рейтинговой оценки процесса базовой модели

<table>
<tr><th>№</th><th>Содержание</th><th>Пример реализации</th></tr>
<tr><td>1</td><td>Определение категорий процессов, которые будут описаны в базовой модели</td><td>Перечень анализируемых категорий процессов:
П1, П2</td></tr>
<tr><td>2</td><td>Формирование атрибутов процессов и их показателей</td><td>Атрибуты процессов, их признаки и допустимые значения:
П1: АП 1.1 (АПП 1.1.1, АПП 1.1.2);
АП 1.2 (АПП 1.2.1, АПП 1.2.2)
...</td></tr>
<tr><td>3</td><td>Разработка профилей процессов базовой модели</td><td>Профиль процесса базовой модели
Процесс: БПр1
Категория: П1
Атрибуты процесса: АП 1.1, АП 1.2
<table><tr><th>П1</th><th>Н</th><th>Ч</th><th>В</th><th>П</th></tr><tr><td>АП 1.1</td><td>+</td><td>+</td><td>+</td><td>+</td></tr><tr><td>АП 1.2</td><td>+</td><td>+</td><td>+</td><td>–</td></tr></table></td></tr>
<tr><td>4</td><td>Модель рейтинговой оценки процессов базовой модели</td><td>Рейтинговая оценка процесса
Процесс: БПр1
<table><tr><th>Уровень/ категория</th><th>Атрибут процесса</th><th>Рейтинговая оценка</th></tr><tr><td>Уровень 1/ П1</td><td>АП 1.1
АП 1.2</td><td>П
В или П</td></tr><tr><td>Уровень 2/ П2</td><td>АП 1.1
АП 1.2
АП 2.1
АП 2.2
АП 2.3</td><td>П
П
П
В или П
В</td></tr></table></td></tr>
</table>

Этап 4. Формирование модели оценки процесса

Модель оценки процесса определяет подход к оценке на основе двухмерного представления характеристик процесса[10]. По оси X

(размерность процесса) отображается совокупность категорий процесса (П1, П2, П3, П4, П5), определенных в базовой модели, а по оси Y (размерность характеристик, возможностей) – атрибуты (уровни возможностей) процесса, определенные в схеме измерений (рис. 3).

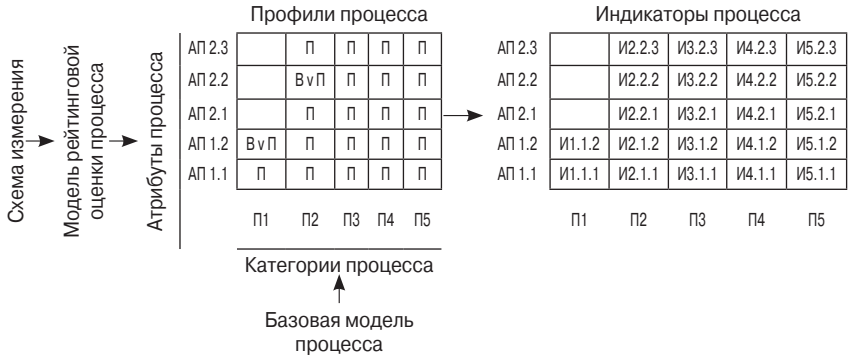


Рис. 3. Модель оценки процесса

Модель оценки процесса включает определение наборов индикаторов, которые явным образом направлены на назначение и выходы процесса и являются источниками объективных свидетельств.

Выделяют несколько видов индикаторов[11]:

– индикатор атрибута оценки процесса (поддерживает суждение о степени достижения конкретного атрибута заданного значения);
– индикатор выполнения атрибута (поддерживает суждение о выполнении конкретного процесса – индикатор атрибута для атрибута конкретного процесса);
– индикатор возможности процесса (поддерживает суждение о возможности конкретного процесса оценки).

Наборы индикаторов позволяют сформировать перечень объективных источников данных о состоянии контролируемого процесса и дать ему оценку, соответствующую требованиям стандартов.

Контрольные панели как инструмент визуализации профилей процессов

Одним из инструментов, применяемых для мониторинга и анализа информации о реализуемых процессах в организации, являются информационные (контрольные) панели.

Информационные (контрольные) панели – «это многослойное приложение на базе инфраструктуры бизнес-анализа и интеграции данных, которое позволяет организации осуществлять измерение, мониторинг и управление бизнесом более эффективно»[12].

Информационные (контрольные) панели позволяют представить данные о процессах в наглядном, интуитивно понятном виде, при помощи различных шкал, показателей, индикаторов, обеспечивающих возможность контролировать текущие значения выбранных показателей, сравнивать их с целевыми или критическими (минимально/максимально допустимыми) значениями и выявлять потенциальные риски и угрозы для реализуемых процессов[13].

Вышеописанная модель оценки процесса представляет системный подход к формированию шкал, индикаторов и показателей процессов с учетом рекомендаций стандартов серии ГОСТ Р ИСО/МЭК 15504, который может быть использован при разработке контрольных панелей информационно-аналитической системы организации.

На контрольную панель могут быть выведены следующие наборы сведений:

- показатели текущего процесса;
- текущая рейтинговая оценка процесса;
- текущий профиль процесса – рейтинговые оценки по каждому атрибуту процесса (с возможностью просмотра текущей рейтинговой оценки по признакам атрибутов процесса);
- показатели отклонения текущей рейтинговой оценки процесса от рейтинговой оценки базовой модели процесса.

Таким образом, контрольная панель позволит отображать операционную информацию в реальном времени и представлять ее с учетом аналитической обработки.

Рост интереса к бизнес-аналитике, в особенности к процессно-ориентированной, необходимость интеграции существующих и разрабатываемых информационных систем с BI-системами и аналитическими платформами, требует продуманного, научно обоснованного подхода к формированию показателей и метрик процессов.

Компания Gartner отмечает, что рынок BI и аналитических платформ останется одним из наиболее быстрорастущих рынков программного обеспечения в течение нескольких ближайших лет,

и выделяет ряд тенденций, характерных для систем данного класса на 2015 год[14], в число которых входит и стандартизация измерений – разработка и применение единых методологий формирования, расчета и интерпретации ключевых показателей эффективности и показателей процессов.

Рассмотренная в статье технология формирования модели оценки процесса представляет системный подход к разработке шкал, индикаторов и показателей процессов, основанный на положениях стандартов серии ГОСТ Р ИСО/МЭК 15504, и отвечает требованиям стандартизации методологий применения ключевых показателей эффективности в деятельности организаций. Проведение оценки процессов с учетом требований международных и российских стандартов позволяет сформировать обоснованные, согласованные показатели, рейтинги и профили процессов.

Примечания

[1] Magic Quadrant for Business Intelligence and Analytics Platforms / Gartner; R.L. Sallam, J. Tapadinhas, J. Parenteau, D. Yuen, B. Hostmann. 2014. February 20. [Электроный ресурс] URL: http://www.webmining.cl/wp-content/uploads/2015/02/mqbi2015.pdf (дата обращения: 09.02.2016).

[2] Системы для бизнес-анализа (BI) в России 2009: Аналитический обзор: BI в России 2009. [Электронный ресурс] URL: http://www.tadviser.ru/articles/64548 (дата обращения: 09.02.2016).

[3] Официальный сайт компании Qlik. [2014]. [Электронный ресурс] URL: http://www.qlik.com/ru (дата обращения: 16.02.2016); IBM Cognos. [2014]. [Электронный ресурс] URL: http://www-01.ibm.com/software/ru/analytics/cognos/ (дата обращения: 16.02.2016).

[4] Глоссарий терминов и определений (Glossary Terms and Definitions). ITIL V3 Glossary v0.92, 30 April, 2009. [Электронный ресурс] URL: http://www.itexpert.ru/rus/biblio/itil_v3/ITILV3_Glossary_Russian_v092_2009.pdf (дата обращения: 11.12.2015); ITIL [2011]. [Электронный ресурс] URL: http://www.itil.co.uk/ (дата обращения: 11.12.2015); CobiT cop. 2011. [Электронный ресурс] URL: http://www.isaca.org/cobit (дата обращения: 11.12.2015).

[5] ГОСТ Р ИСО/МЭК 15504–1–2009. Информационная технология. Оценка процессов. Часть 1: Концепция и словарь. Введ. 2009-09-14. М.: Стандартинформ, 2010.

[6] Там же; ГОСТ Р ИСО/МЭК 15504–2–2009. Информационная технология. Оценка процесса. Часть 2: Проведение оценки. Введ. 2009-12-09. М.: Стандартинформ, 2010; ГОСТ Р ИСО/МЭК 15504–3–2009. Информационная технология. Оценка процесса. Часть 3: Руководство по проведению оценки. Введ. 2009-12-09. М.: Стандартинформ, 2010; ГОСТ Р ИСО/МЭК 15504–4–2012.

Информационная технология. Оценка процесса. Часть 4: Руководство по применению для улучшения и оценки возможностей процесса. Введ. 2014-01-01. М.: Стандартинформ, 2014.

[7] ГОСТ Р ИСО/МЭК 15504–1–2009. Информационная технология. Оценка процессов. Часть 1: Концепция и словарь. С. 7.

[8] ГОСТ Р ИСО 9000-2008. Системы менеджмента качества: Основные положения и словарь.

[9] ГОСТ Р ИСО/МЭК 15504–1–2009. Информационная технология: Оценка процессов. Часть 1: Концепция и словарь. С. 8.

[10] ГОСТ Р ИСО/МЭК 15504–2–2009. Информационная технология. Оценка процесса. Часть 2: Проведение оценки; ГОСТ Р ИСО/МЭК 15504–3–2009. Информационная технология. Оценка процесса. Часть 3: Руководство по проведению оценки.

[11] ГОСТ Р ИСО/МЭК 15504–1–2009. Информационная технология. Оценка процессов. Часть 1: Концепция и словарь.

[12] *Эккерсон У.У.* Панели индикаторов как инструмент управления: ключевыми показателями эффективности, мониторинг деятельности, оценка результатов: Пер. с англ. М.: Альпина Бизнес Букс, 2007. С. 31.

[13] *Каплан Р.С., Нортон Д.П.* Сбалансированная система показателей: От стратегии к действию. М.: Олимп Бизнес, 2013; *Фридаг Х., Шмидт В.* Сбалансированная система показателей: Пер. с нем. М.: Омега-Л, 2011.

[14] Magic Quadrant for Business Intelligence...

Ю.И. Воронова

Математическое моделирование временных рядов в условиях кластеризации волатильности

В работе рассмотрена проблема оценки волатильности цен открытых паевых инвестиционных фондов с помощью GARCH и EGARCH-процессов. Очевидным достоинством применения EGARCH-модели перед результатами, получаемыми по GARCH, является возможность учесть знак волатильности. Этот эффект достигается путем включения функции $g_t\left(\varepsilon_{t-1}\right)$, которая на отрицательном и положительном участке ε_t позволяет процессу для условной дисперсии асимметрично откликаться на увеличение и падение цены актива. Кроме того, исследование содержит подходы с оценкой фрактальной структуры временных рядов. Получены численные результаты прогнозов с использованием локальной аппроксимации 1-го и 2-го порядков. Приведен вывод матрицы дополнительных параметров B для локальной аппроксимации 2-го порядка.

Ключевые слова: волатильность, паевой фонд, GARCH, куртозис, EGARCH, аппроксимация, прогнозирование.

Выполним оценку и составим прогноз открытого паевого инвестиционного фонда «Сбербанк – Телекоммуникации и Технологии». Паевой фонд по своему экономическому смыслу – это средства инвесторов, которые переданы на доверительное управление определенной компании. Для существующего ОПИФ управляющей компанией является структурное подразделение банка «Сбербанк» – АО «Сбербанк: управление Активами». Компания управляет линейкой фондов, девятнадцать из которых являются открытыми. Структура фондов представлена различным набором активов: долговые обязательства отечественных и иностранных эмитентов, финансовый сектор, недвижимость, высокотехнологичный сектор экономики и другие. На доходность паевых инвестиционных фондов (ПИФ) влияют различные экономические факторы: мировые фондовые индексы (РТС, S&P500, DowJones, NASDAQ NIKKEI, Euro Stoxx 600, FTSE, Hang Seng и др.), государствен-

ная политика (например, ставка рефинансирования Центрального банка, государственная поддержка предприятий, государственные заказы, политические события), курсовая разница в моменты ввода и вывода капитальных средств из фондового рынка.

ОПИФ «Сбербанк – Телекоммуникации и Технологии» нацелен на долгосрочный прирост капитала путем инвестирования в акции преимущественно российских компаний связи. Динамика изменения цен пая с даты основания фонда 11.10.2006 г. по 25.02.2016 г. представлена на рис. 1.

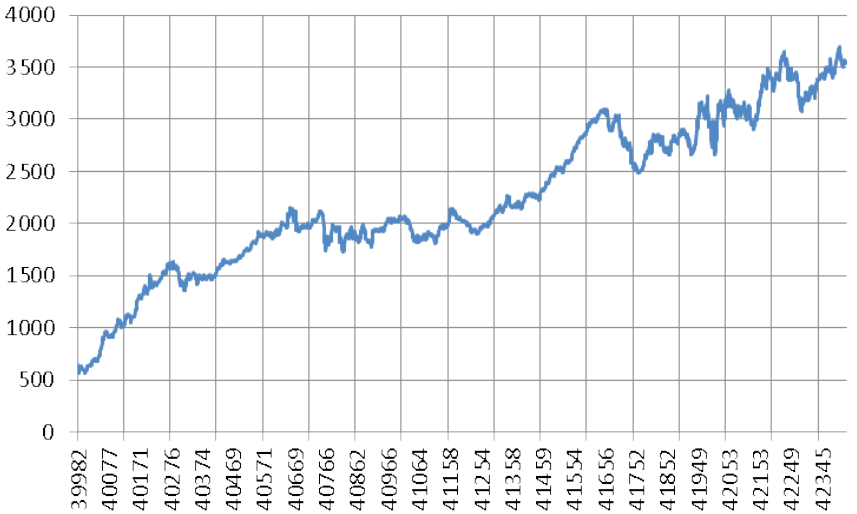


Рис. 1. Динамика цены пая ОПИФ «Сбербанк – Телекоммуникации и технологии» в период 2009–2010 гг.

Фонд создан для инвесторов, желающих увеличить вес данного сектора в своем портфеле. Фонд инвестирует в диверсифицированный в рамках одного сектора портфель, который включает акции сотовых операторов, региональных компаний фиксированной связи, альтернативных операторов, компаний медиасектора и сегмента информационных технологий, а также компании, связанные с добычей драгоценных металлов (предпочтение отдается российским компаниям)[1].

Выполним преобразование исходного ряда цен паев в ряд индексов цен, используя следующую формулу:

$$Y_t = \ln \frac{p_{t+1}}{p_t}, \qquad (1)$$

где p_t – цена пая в момент времени t.

На рисунке 2 отчетливо можно наблюдать высокую волатильность, что характерно для финансовых временных рядов. В этом случае для прогноза доходности мы не можем использовать традиционные модели временных рядов, такие как модель АРСС (ARMA), нелинейная, множественная регрессия, в силу того что в этих моделях предполагается постоянство дисперсии, т. е. гомоскедастичность.

Наличие гетероскедастичности в данном финансовом ряде было установлено вышеперечисленными тестами.

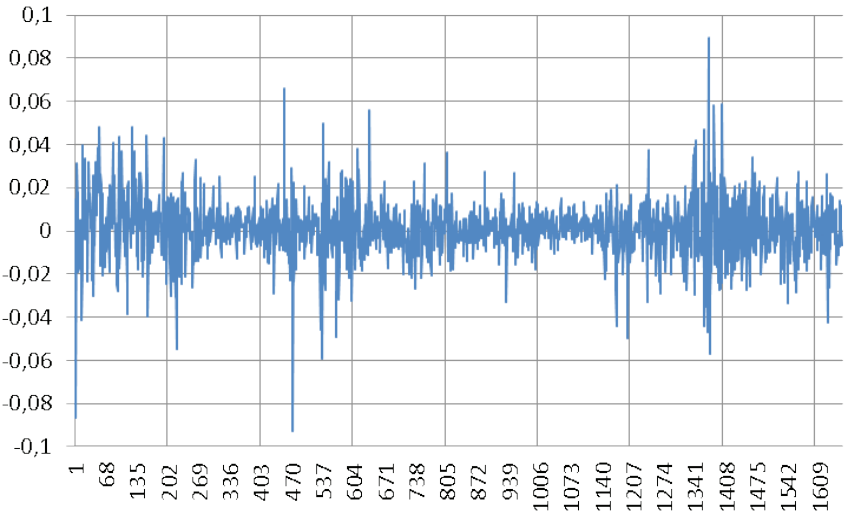


Рис. 2. График индекса цены ОПИФ
«Сбербанк – Телекоммуникации и технологии»

В связи с этим рассмотрим модели условной гетероскедастичности: GARCH, EGARCH. Наиболее популярными моделями для анализа финансовых рядов являются данные модели 1-го порядка.

Модель $GARCH(p,q)$ задается следующей формулой.

$$\sigma_t^2 = K + \sum_{k=1}^{p} \beta_k \sigma_{t-k}^2 + \sum_{j=1}^{q} \alpha_j \varepsilon_{t-j}^2 . \qquad (2)$$

Для корректного определения условной дисперсии должны выполняться ограничения вида:

$$K > 0; \quad \beta_k \geq 0, k = 1 \div p; \quad \alpha_j \geq 0, j = 1 \div q \quad . \qquad (3)$$

Рассчитаем безусловную дисперсию GARCH-процесса, предполагая, что он стационарен. Для этого возьмем математические ожидания от обеих частей уравнения для условной дисперсии по формуле, представленной ниже.

$$\sigma^2 = \frac{K}{1 - \sum_{k=1}^{p} \beta_k - \sum_{j=1}^{q} \alpha_j}. \qquad (4)$$

С точки зрения безусловной дисперсии GARCH-процесс гомоскедастичен. Для того чтобы дисперсия была конечной, требуется соблюдение следующего неравенства:

$$\sum_{k=1}^{p} \beta_k + \sum_{j=1}^{q} \alpha_j < 1. \qquad (5)$$

Тогда для модели $GARCH(1,1)$

$$\sigma_t^2 = K + \beta_1 \sigma_{t-1}^2 + \alpha_1 \varepsilon_{t-1}^2 . \qquad (6)$$

$$\sigma^2 = \frac{K}{1 - \alpha_1 - \beta_1}, \qquad (7)$$

где $\alpha_1 + \beta_1 < 1$.

Прогноз условной дисперсии на момент $t + \tau$ составит

$$\sigma_{t+\tau}^2 = K + (\beta_1 + \alpha_1) \sigma_{t+\tau-1}^2 . \qquad (8)$$

Оценивание параметров GARCH-модели выполним посредством максимизации функции максимального правдоподобия.

С целью оценить остроту вершины и толщину хвостов волатильности построим график куртозиса. С выводом формулы, описывающей куртозис, можно ознакомиться в[2]. Графики куртозиса для процесса GARCH (1.1) представлены на рис. 3.

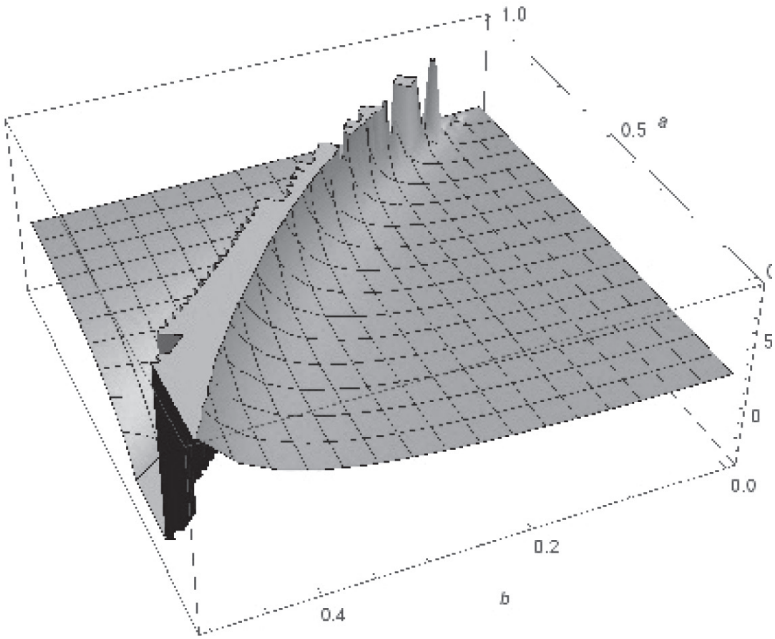


Рис. 3. График куртозиса для процесса *GARCH* (1.1)

После расчетов прогноз волатильности для инвестиционного паевого фонда на дальнейший месяц имеет следующий вид (см. рис. 4).

По графику видно, что волатильность монотонно растет и приближается к значению σ^2, которое может быть найдено по формуле (4). Но данная модель не предоставляет возможности определить знак волатильности. С этой проблемой хорошо справляется EGARCH, которая рассмотрена ниже.

Для повышения гибкости исходная GARCH-модель была расширена в разных направлениях. Первоначальная спецификация GARCH-модели предполагает, что реакция на шок не зависит от знака шока, а является функцией только от его размера. Но один из фактов финансовой волатильности говорит о том, что она стремит-

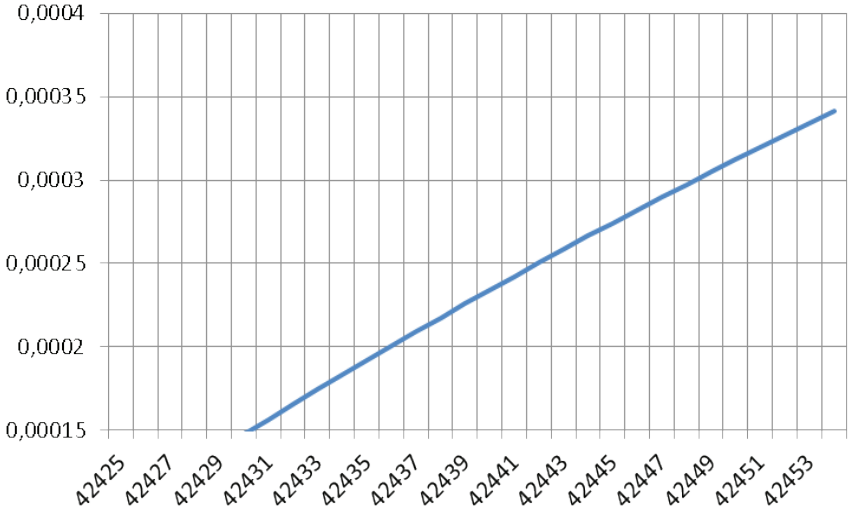


Рис. 4. Прогноз волатильности при использовании модели *GARCH* (1.1)

ся быть выше на падающем рынке, чем на растущем. Асимметричное воздействие новостей на волатильность называют эффектом рычага[3].

Асимметричные модели, одной из которых является модель EGARCH, дают объяснение этому эффекту.

В экспоненциальной GARCH-модели (EGARCH), предложенной Nelson (1991), σ_t^2 впервые зависит как от размера, так и от знака лагированных шоков[4]. Модель представлена формулой (9).

$$\ln(\sigma_t^2) = K + \sum_{t=1}^{q} \alpha_t (\phi z_{t-1} + \psi(|z_{t-1}| - \mathrm{E}[|z_{t-1}|])) + \sum_{t=1}^{p} \beta_t \ln(\sigma_t^2). \qquad (9)$$

В формуле (1) $\alpha_1 \equiv 1$, а $\mathrm{E}[|z_t|] = \sqrt{2/\pi}$, в том случае, если z_t является нормально распределенной случайной величиной с параметрами $(0,1)$. На величины K, α_t и β_t не накладываются ограничения неотрицательности. По построению функция $g(\varepsilon_t)$ – случайная последовательность с нулевым средним. Компоненты $\theta\varepsilon_{t-1}$ и $\gamma(|\varepsilon_{t-1}| - \mathrm{E}[|\varepsilon_{t-1}|])$ также имеют нулевое среднее. На множестве $0 < \varepsilon_t < \infty$ функция $g(\varepsilon_t)$ линейна по ε_t с углом наклона $\theta + \gamma$,

а на множестве $-\infty < \varepsilon_t < 0$ линейна с углом наклона $\theta - \gamma$. Таким образом, $g(\varepsilon_t)$ позволяет процессу для условной дисперсии σ_t^2 асимметрично реагировать на увеличение и падение цены активов.

Оценивая параметры с помощью надстройки «Поиск решения» в MS Excel, были получены следующие значения для исследуемого временного ряда $\theta = 0,99$ и $\gamma = 5,73 \times 10^{-6}$. Подставив полученные значения в функцию $g(\varepsilon_t)$, определим ее значения. Перепишем формулу (9) в виде:

$$\ln(\sigma_t^2) = K + \sum_{t=1}^{q} \alpha_t g_t(\varepsilon_{t-1}) + \sum_{t=1}^{p} \beta_t \ln(\sigma_{t-1}^2). \qquad (10)$$

Для процесса *EGARCH* (1.1), как и ранее для *GARCH* (1.1) идентифицированы коэффициенты *K*, α_1 и β (см. табл. 1).

Таблица 1

Параметры идентификации модели *EGARCH* (1.1)

K	α_1	β
0,01	1	–0,06

Подставив эти коэффициенты в формулу (11), получим значения логарифмов волатильности временного ряда. График прогноза логарифмов волатильности на несколько дней вперед представлен на рисунке 5.

На графике (рис. 5) видно, что волатильность растет с положительным знаком. В силу того что прогнозирование цены ОПИФ «Сбербанк – Телекоммуникации и технологии» осуществляется на период прошедшего времени, для которого характерна тенденция к росту, а явных скачков цен не наблюдается. Если бы мы наблюдали явные изменения цен пая, то прогноз логарифма волатильности имел бы пилообразный вид. Так, например, пилообразный вид волатильности можно наблюдать в фондах, базирующихся на торговле энергоресурсами, что в условиях мировой экономической конъюнктуры вокруг избытка предложения углеводородов оказывает значительное влияние на формирование кластеризации волатильности цен. Это отличие и объясняется особенностью модели EGARCH, которое описано выше.

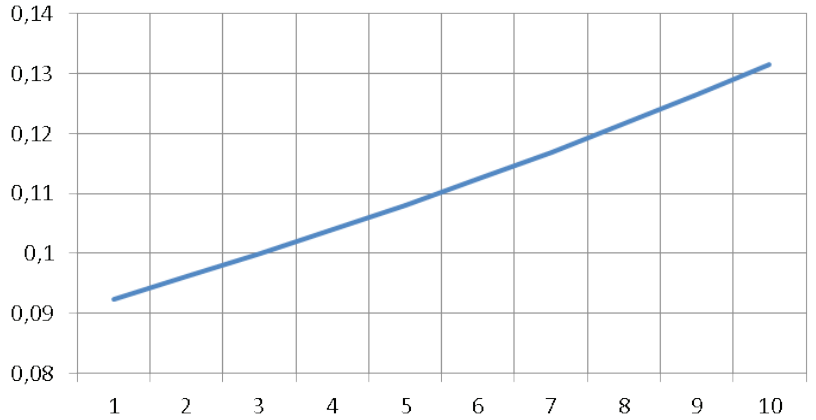


Рис. 5. Прогноз логарифмов волатильности на несколько дней при использовании процесса *EGARCH* (1.1)

Зная логарифмы волатильности, мы можем перейти от них к значениям цены пая, преобразовав некоторые формулы. С помощью этих преобразований получились прогнозные значения цен пая на 10 дней, которые представлены в табл. 2.

Таблица 2

Прогнозные значения на 10 дней (в руб.)

Дата	Прогноз
25.02.2016	3531.81
26.02.2016	3541.45
27.02.2016	3565.73
28.02.2016	3605.54
29.02.2016	3662.02
01.03.2016	3736.62
02.03.2016	3831.10
03.03.2016	3947.64
04.03.2016	4088.93
05.03.2016	4258.22

Для сравнения на рис. 7 представлены графики прогнозных значений и реальных данных на это время.

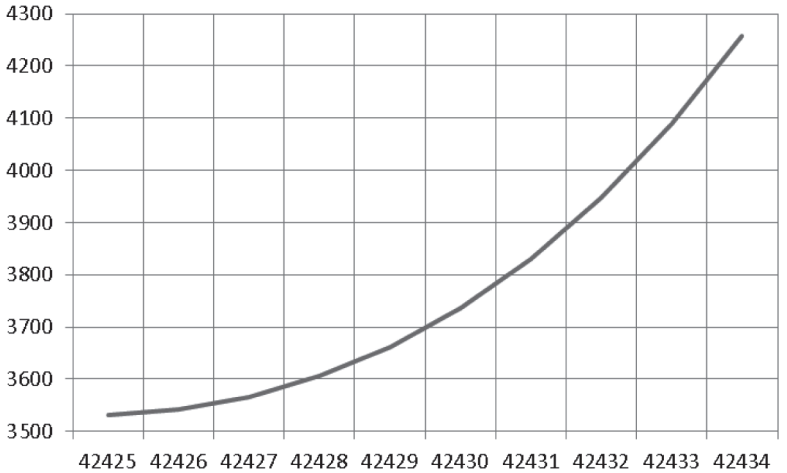


Рис. 6. График прогнозных значений цены пая
ОПИФ «Сбербанк – Телекоммуникации и Технологии»

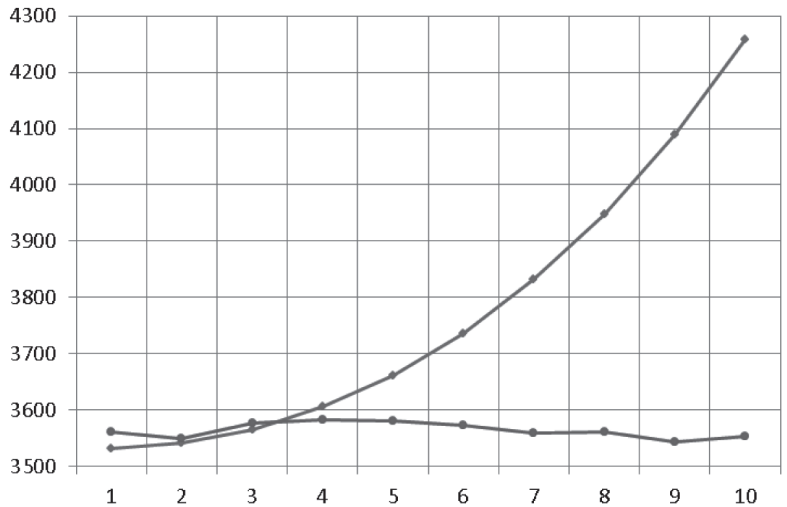


Рис. 7. График прогнозных и реальных значений цены пая
ОПИФ «Сбербанк – Природные ресурсы»
(растущая кривая – прогнозные значения; кривая, пролегающая
под прогнозом – реальные наблюдения цены пая)

Как видно на рисунке, прогнозные значения близки к реальным данным, особенно в первые дни. Это говорит о том, что с помощью модели EGARCH можно получить прогноз с достаточно высокой точностью. Но следует отметить, что финансовые временные ряды рекомендуется прогнозировать на короткие сроки. Данное обстоятельство связано со скорой сменой значений влияющих факторов на формирование цены пая. Указанную рекомендацию можно пронаблюдать на рис. 6, где отчетливо видно, как прогноз с 5 дня в значительной степени отклоняется от реального положения на фондовом рынке.

Одной из методик анализа событий, происходящих на рынке, которая выделяется своей простотой и оригинальностью, является фрактальный анализ. Фактически не существует точного определения понятия «фрактал». Фракталы характеризуются свойством самоподобия и фрактальной размерностью, которую необходимо знать для построения прогноза. Численное значение фрактальной размерности определяется с помощью R/S анализа, предложенного Херстом. Подробное описание этапов данного анализа изложено в книге Петерса[5].

Показатель Херста дал результат $H = 0{,}6129 \pm 0{,}148$. Оценка показателя Херста имеет большую погрешность, это можно объяснить сильной зашумленностью ряда цен, поэтому нельзя утверждать, что ряд имеет фрактальное распределение. Но тем не менее Петерс склоняется к тому, что ряд персистентен, так как среднее значение H все-таки больше 0,5.

Для определения фрактальной размерности необходимо воспользоваться формулой

$$D = 2 - H. \tag{12}$$

В результате получим размерность $D = 1{,}3871$. Узнав размерность, можно осуществить прогноз, используя локальную аппроксимацию.

В соответствии с теорией Такенса–Мане приемлемое описание фазового пространства можно получить, если взять вместо реальных переменных p-мерные векторы задержек из значений ряда в последовательные моменты времени. При выполнении условия $p \geq 2D + 1$[6].

Построим матрицу задержек:

$$\{x_1, x_2, \ldots x_N\} \to X_{p(N-p+1)} = \begin{pmatrix} x_p & x_{p+1} & \ldots & x_N \\ \ldots & \ldots & \ldots & \ldots \\ x_2 & x_3 & \ldots & x_{N-p+2} \\ x_1 & x_2 & \ldots & x_{N-p+1} \end{pmatrix} \tag{13}$$

Затем определяем вид локального представления, наиболее распространенный вариант – локальная аппроксимация первого порядка (далее $LA(1)$) (14).

$$x_{t+1} = a_0 + x^T{}_t a, \tag{14}$$

где a – матрица параметров представления.

Кроме этого, используются еще 2 варианта: линейная аппроксимация нулевого порядка (LA(0)) (15) и второго порядка (LA(2)) (16).

$$x_{t+1} = a_0, \tag{15}$$

$$x_{t+1} = a_0 + x_t^T a + x_t^T B x_t, \tag{16}$$

где B – матрица дополнительных параметров.

Примером использования линейной аппроксимации нулевого порядка служит прогноз температуры воздуха. Один из способов прогноза температуры на следующий день состоит в том, чтобы, найдя, в какой из предшествующих дней температура была максимально близкой к сегодняшней, взять в качестве прогноза температуры на завтра ее величину в следующий за найденным день[7].

Используя аппроксимацию первого порядка (14), параметр a_0 найдем по примеру, описанному выше, а матрицу параметров a – по следующим преобразованиям.

$$x_t^T a = x_{t+1} - a_0 E, \tag{17}$$

$$(x_t^T)^{-1} x_t^T a = (x_t^T)^{-1}(x_{t+1} - a_0 E), \tag{18}$$

$$a = (x_t^T)^{-1}(x_{t+1} - a_0 E). \tag{19}$$

При использовании аппроксимации второго порядка (16) неизвестную матрицу B можно найти по следующим преобразованиям.

$$x_{t+1} = a_0 + x_t^T a + x_t^T B x_t, \tag{20}$$

$$(x_t^T)^{-1} x_t^T B x_t (x_t)^{-1} = (x_t^T)^{-1} x_{t+1} - a_0 E - x_t^T a)(x_t)^{-1}, \tag{21}$$

$$B = (x_t^T)^{-1}(x_{t+1} - a_0 E - x_t^T a(x_t)^{-1}. \tag{22}$$

На рис. 8 представлены графики прогноза при использовании локальной аппроксимации нулевого и первого порядка, а также график реальных данных за этот период.

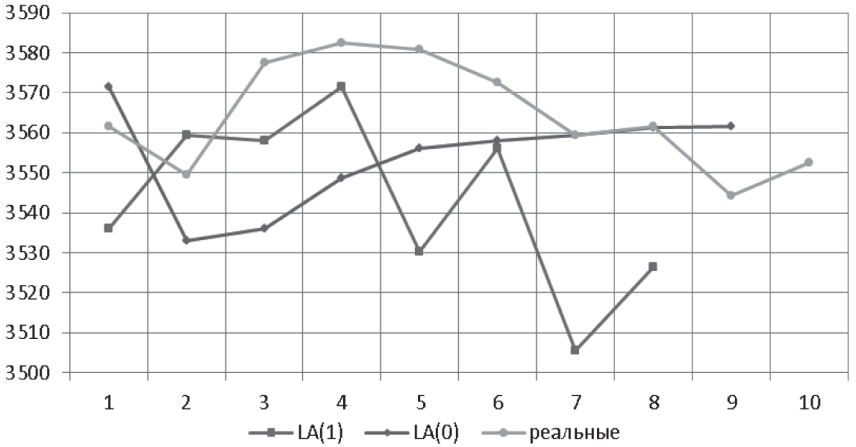


Рис. 8. Прогноз ОПИФ «Сбербанк – Телекоммуникации и Технологии» на период с 25.02 по 05.03.2016 г.

В табл. 3 отражены прогнозные значения по аппроксимации первого и нулевого порядка.

Таблица 3

Прогнозные значения ОПИФ «Сбербанк – Телекоммуникации и Технологии» (в руб.)

Дата	$LA(1)$	$LA(0)$	Исторические наблюдения
25.02.2016	3536.1	3571.6	3561.6
26.02.2016	3559.3	3532.9	3549.6
27.02.2016	3558.0	3536.1	3577.5
28.02.2016	3571.6	3548.8	3582.6
29.02.2016	3530.3	3556.0	3580.9
01.03.2016	3556.0	3558.0	3572.5
02.03.2016	3505.6	3559.3	3559.5
03.03.2016	3526.4	3561.4	3561.5

Прогнозные значения по аппроксимации нулевого порядка отличаются от реальных данных в среднем на 17,66 руб., а аппроксимации первого порядка на 27,7 руб.

Средняя ошибка аппроксимации по первому прогнозу (аппроксимация первого порядка) составляет 0,78%, а по второму прогнозу (аппроксимация нулевого порядка) – 0,5%, что говорит о неплохих результатах. Также графики прогнозов имеют схожую тенденцию с графиком реальных данных за это время.

Для сравнения результатов на рис. 9 представлены графики прогнозов EGARCH, LA (0), LA (1).

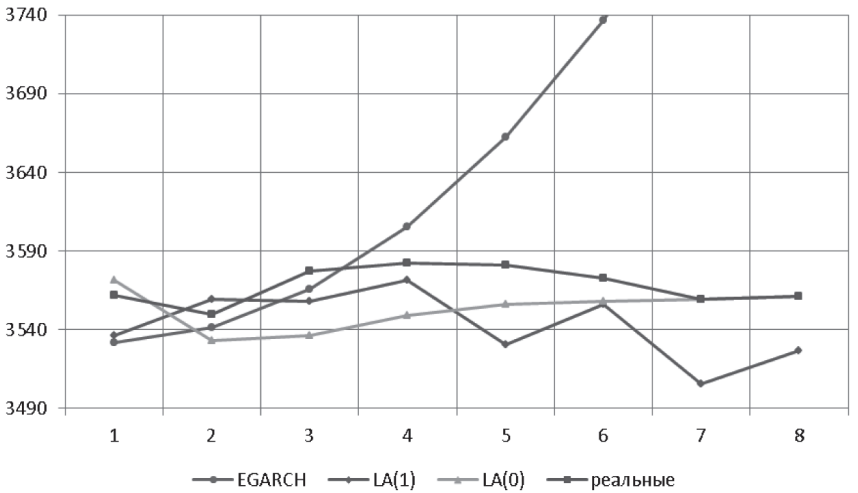


Рис. 9. Прогнозы *EGARCH* (1,1), *LA* (0), *LA* (1)

По графику видно, что в первые дни все варианты прогноза достаточно близко расположены к реальным данным. Но модель EGARCH дает адекватный прогноз лишь на небольшое количество дней. Локальные аппроксимации первого и нулевого порядка тоже с ростом количества дней отклоняются сильнее от реальных данных, но примерно повторяют их тенденцию.

Примечания

[1] Сайт «Сбербанк – Управление активами». [Электронный ресурс] URL: http://www.sberbank-am.ru (дата обращения: 01.09.2016)

[2] *Молоденов К.В.* ARCH- и GARCH-модели временных рядов: дипломная работа. ... 230401.65 / Науч. рук. З.И. Баженова. М., 2014. [Электронный ресурс] URL: https://miem.hse.ru/data/2014/06/09/1324317113/Диплом.pdf

[3] *Росси Э.* Одномерные GARCH-модели: Обзор // Квантиль. 2010. № 8. С. 167.

[4] Там же.

[5] *Петерс Э.* Фрактальный анализ финансовых рынков: Применение теории Хаоса в инвестициях и экономике. М.: Интернет-трейдинг, 2004.

[6] *Лоскутов А.Ю.* Анализ временных рядов: Курс лекций. М.: МГУ, 2010.

[7] Там же.

О.В. Казарин, М.М. Репин

Модель процесса мониторинга состояния информационной безопасности платежной системы

Процесс мониторинга состояния информационной безопасности платежной системы является основой для оценки и анализа рисков информационной безопасности.

Важным аспектом задачи по мониторингу состояния информационной безопасности платежной системы является необходимость оценки взаимосвязей между инициирующими событиями и их влияния на уязвимости платежной системы.

Данные взаимосвязи могут быть описаны с помощью логико-вероятностных моделей, применение которых рассматривается в настоящей работе.

Ключевые слова: платежная система, мониторинг информационной безопасности, логико-вероятностные модели, риск информационной безопасности, инициирующие события.

На стадии эксплуатации платежной системы (далее – ПС) оценку и анализ рисков информационной безопасности (далее – ИБ) проводят на основе определенных сценариев с использованием результатов мониторинга потенциальных уязвимостей ПС, особенностей эксплуатации, компетентности и состава обслуживающего персонала, данных об актуальных угрозах и нештатных ситуациях в ПС (далее – НШС).

Под НШС понимается ситуация, при возникновении которой произошло нарушение штатного функционирования информационно-вычислительных, телекоммуникационных, инженерных систем, систем связи, систем и средств защиты информации, ПС и технологии обработки платежных документов, повлекшее нарушение регламента обработки платежной информации или предоставления отчетности.

Процесс возникновения нештатных ситуаций в ПС

Рассмотрим процесс возникновения НШС. Пусть $V = \{v_1, \dots, v_n\}$ – множество уязвимостей ПС, $E = \{e_1, \dots, e_k\}$ – множество событий в ПС, $I = \{i_1, \dots, i_m\}$ – множество инцидентов ИБ в ПС, $SNS = \{sns_1, \dots, sns_l\}$ – множество сценариев НШС, NS – НШС. На рис. 1 представлен пример процесса возникновения НШС. Событие e_2, связанное с уязвимостью v_2, совместно с событием e_3, не связанным с существующими уязвимостями, порождают инцидент i_2, в свою очередь, подпадающий под сценарий НШС sns_1 и реализующий данную НШС. Аналогично можно описать представленную НШС по сценарию sns_{i-1}. События могут не являться инцидентом ИБ. На рис. 1 данный случай представлен на примере события e_{k-1}.

Таким образом, решение задачи по мониторингу состояния ИБ ПС осложняется необходимостью не только проводить анализ рисков ИБ, но и оценивать взаимосвязи между инициирующими событиями, степень их влияния на уязвимости ПС.

Рис. 1. Процесс возникновения НШС в ПС

Использование сценарного подхода к процессу возникновения НШС позволяет применить для его описания логико-вероятностные модели. Особенности их применения рассматриваются в следующем разделе.

Логико-вероятностная модель процесса мониторинга ИБ в ПС

Постановка задачи. Существующие методы оценки и управления операционными рисками, в том числе и рисками ИБ[1], не предоставляют механизмов, позволяющих описывать сложные зависимости между объектами анализа (событиями, инцидентами, уязвимостями и т. д.), а также связь внутренних и внешних событий, инициирующих риск ИБ.

Данные зависимости могут быть описаны с помощью логико-вероятностных (далее – ЛВ) моделей, показывающих высокую эффективность в решении задач по экономическим направлениям, в том числе при оценке кредитного риска, риска портфеля ценных бумаг[2].

Таким образом, задачу построения модели процесса мониторинга состояния ИБ ПС можно сформулировать следующим образом. Необходимо построить ЛВ-модель процесса мониторинга ИБ ПС. Логико-вероятностная модель процесса мониторинга ИБ ПС должна быть комплексной и включать в себя модели мониторинга обеспечения ИБ ПС и обеспечения безопасности платежных технологий с учетом возможности как внутренних, так и внешних событий, инициирующих НШС.

Структура событий процесса мониторинга ИБ ПС. Задачей процесса мониторинга ИБ ПС является своевременное выявление событий, которые могут инициировать риски возникновения НШС.

Реализация рисков в ПС, включающих также риски ИБ, может иметь два вида последствий, в том числе и одновременных. Первое последствие – это нарушение процесса функционирования ПС, непрерывность которого является одним из важнейших условий для проведения клиентских платежей. Вторым последствием является потеря денежных средств клиентом из-за неправильной обработки электронных платежных сообщений, содержащих данные о платежах. Нарушение процесса непрерывного функционирования, в свою очередь, может быть вызвано как реализацией угроз ИБ, так и ошибками системного программного обеспечения ПС.

Для построения ЛВ-модели процесса мониторинга ИБ ПС, по аналогии с подходом, применяемым для финансовых рисков[3], рассмотрим НШС в качестве сложного события Y, состоящего из объединения логической (Л) операцией *И* внутренних Y_{in} и внешних Y_{out} производных событий.

В свою очередь, внутренние и внешние производные события могут вызываться инициирующими событиями с Л-связью ИЛИ из групп Y_s (некорректная работа средств и систем защиты информации в ПС) и Y_{pay} (нарушение платежных технологий). В каждом из событий из групп Y_s и Y_{pay} для внутренних производных событий Y_{in} выделяют события Y_{ins_1}, ... , Y_{ins_n}, Y_{inpay_1}, ... , Y_{inpay_n}, объединенные Л-связью ИЛИ. Внешнее производное событие Y_{out} вызывает события Y_{outs_1}, ... , Y_{outs_n}, Y_{outpay_1}, ... , Y_{outpay_n} , объединенные Л-связью ИЛИ. Структура событий процесса мониторинга ИБ ПС представлена на рис. 2.

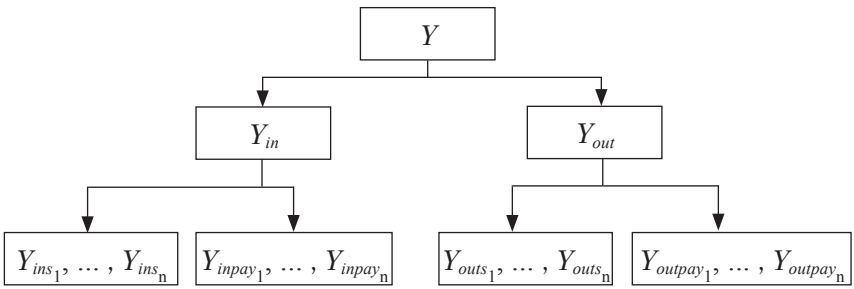


Рис. 2. Структура событий процесса мониторинга ИБ ПС

Производные и инициирующие события ЛВ-модели процесса мониторинга информационной безопасности в ПС. Опишем для общего случая события, мониторинг которых позволит определить наличие нарушений ИБ ПС (см. рис. 3, в котором для упрощения приведены только индексы в обозначении событий).

В качестве основного события Y_1 будем рассматривать общий процесс мониторинга. Событие Y_1 появляется от действия внутреннего производного события Y_2 и внешнего Y_3. Событие Y_3 – производное событие внешних инициирующих событий, включающее в себя события Y_8 и Y_9.

Y_8 – контроль взаимоотношений с внешними организациями: Y_{10} – контроль соблюдения лицензионных требований и наличия лицензий у внешних организаций, Y_{11} – контроль ведения договорной работы с внешними организациями.

Y_9 – контроль платежного процесса при взаимодействии с внешними организациями: Y_{12} – мониторинг статуса клиента, Y_{13} – мониторинг статуса (корректности) электронных платежных сообщений клиента, Y_{14} – мониторинг ликвидности клиента.

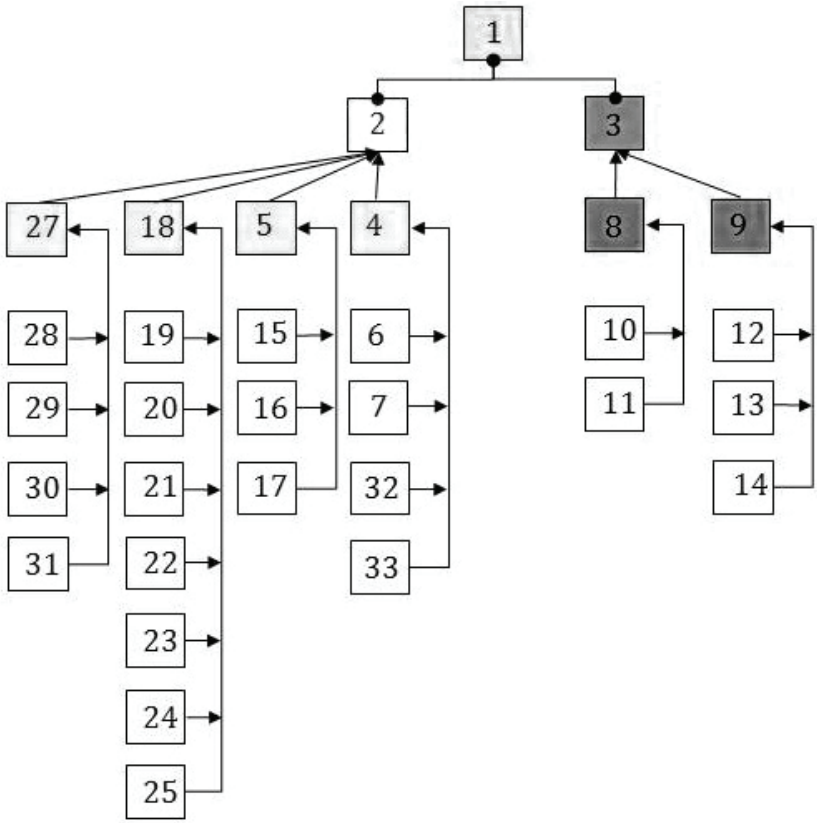


Рис. 3. Структурная модель процесса мониторинга ИБ в ПС

Y_2 – производное событие внутренних инициирующих событий, включающее в себя события:

Y_4 – контроль действий пользователей ПС и объектов информационной инфраструктуры ПС: Y_6 – контроль средств ввода-вывода информации, Y_7 – контроль работы в подсистемах ПС, Y_{32} – контроль работы с сетью Интернет, Y_{33} – контроль входных/выходных данных.

Y_5 – контроль функционирования компонент ПС: Y_{15} – контроль присутствия эксплуатационного персонала на рабочих местах, Y_{16} – контроль статуса функционирования ИТ-сервисов, Y_{16} – контроль функционирования средств и систем защиты информации.

Y_{18} – контроль заданных настроек ПС: Y_{19} – контроль настроек безопасности, согласно стандартам, Y_{20} – паспортный контроль объектов информационной инфраструктуры ПС, Y_{21} – регистрация и мониторинг событий ИТ-сервисов, Y_{22} – регистрация и мониторинг событий средств и систем защиты информации, Y_{23} – регистрация, учет и контроль используемых носителей информации, Y_{24} – контроль выполняемых критичных операций в ПС, Y_{25} – контроль систем автоматизированного мониторинга и корреляции событий.

Y_{27} – контроль целостности: Y_{28} – контроль целостности архивов и резервных копий, Y_{29} – контроль целостности сред функционирования средств криптографической защиты информации, серверов, автоматизированных рабочих мест, Y_{30} – контроль модификаций программного обеспечения ПС, Y_{31} – контроль целостности регистрационных журналов.

В свою очередь, для наиболее критичных инициирующих событий можно построить индивидуальное дерево событий, отражающее процесс его возникновения.

Рассмотрим одно из важнейших событий для платежных систем Y_9 – контроль платежного процесса при взаимодействии с внешними организациями (см. рис. 4). При получении платежных сообщений от клиента важным аспектом является контроль его корректности Y_{13}. Для Y_{13} можно определить следующие инициирующие события с учетом того, что электронное сообщение (далее – ЭС) представляет собой одиночное сообщение или пакет сообщений в соответствии с альбомом «Унифицированные форматы электронных банковских сообщений»: Y_{34} – контроль корректности конверта ЭС (на соответствие указанному альбому), Y_{35} – контроль корректности электронной подписи отправителя и ее принадлежности и даты формирования, Y_{36} – контроль корректности ЭС/пакета ЭС, Y_{37} – контроль дублирования ЭС/ пакета ЭС, Y_{38} – контроль общей суммы платежей в пакете ЭС (если поступил пакет).

Кортежи для описания производных событий модели процесса мониторинга ИБ в ПС. Для обеспечения гибкости представленной структурной модели введем описание производных событий в виде кортежей. Производные события будут являться значением функции, аргументами которой являются инициирующие события.

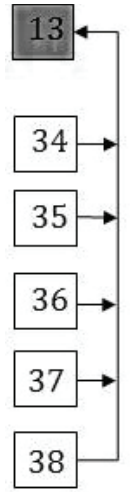


Рис. 4. Структурная модель процесса контроля корректности входящих платежных сообщений ПС

Например:
1(2, 3);
2(27, 18, 5, 4);
3(8, 9);
27(28, 29, 30, 31);
18(19, 20, 21, 22, 23, 24, 25);
5(15, 16, 17);
4(6, 7, 32, 33);
8(10, 11);
9(12, 13, 14).

В записи производных кортежей знак Л-операции опущен, так как он может варьироваться в зависимости от постановки задачи. Также следует отметить, что наличие определенных факторов не является однозначным свидетельством инцидента ИБ (ранее – НШС) и соответствующие им инициирующие события имеют определенную вероятность и являются случайными совместными и независимыми событиями.

Прогнозирование финансовых потерь. При осуществлении процесса мониторинга важно оценить возможные финансовые потери от реализации рисков в ПС.

Рассмотрим подход к анализу возможных потерь на примере процесса контроля корректности входящих платежных сообщений ПС.

Фрагмент логической модели данного процесса имеет следующий вид.

$$Y = \bar{Y}_{34} \wedge \bar{Y}_{35} \wedge \bar{Y}_{36} \wedge \bar{Y}_{37} \wedge \bar{Y}_{38} \vee \bar{Y}_{34} \wedge \bar{Y}_{35} \wedge \bar{Y}_{36} \wedge \bar{Y}_{37} \wedge \bar{Y}_{38} \vee \bar{Y}_{34} \wedge \bar{Y}_{35} \wedge \bar{Y}_{36} \wedge Y_{37} \wedge Y_{38} \vee \bar{Y}_{34} \wedge \bar{Y}_{35} \wedge Y_{36} \wedge \bar{Y}_{37} \wedge \bar{Y}_{38} \vee \bar{Y}_{35} \wedge \bar{Y}_{36} \wedge \bar{Y}_{37} \wedge \bar{Y}_{38} \cdots$$

Логическую модель процесса контроля в минимальной дизъюнктивной нормальной форме можно представить следующим образом: $Y = Y_{34} \vee Y_{35} \vee Y_{36} \vee Y_{37} \vee Y_{38}$.

Возможные финансовые потери от рисков реализации НШС можно вычислить по следующей формуле.

$$Q_{13} = P_{34} Q_{34} + P_{35} Q_{35} + P_{36} Q_{36} + P_{37} Q_{37} + P_{38} Q_{38},$$

где $Q_{34} \cdots Q_{38}$ – финансовые ресурсы, которые могут быть потеряны при реализации соответствующего инициирующего события; $P_{34} \cdots P_{38}$ – риски реализации инициирующих событий, под которыми понимается вероятность потери финансовых ресурсов.

В данном примере под финансовыми ресурсами, которые могут быть потеряны, понимаются суммы, направляемые банками клиентов в платежных распоряжениях, соответственно в зависимости от этапа контроля под угрозой могут находиться как отдельные платежные документы, так и пакеты платежей (в случае внутреннего нарушителя).

В том случае, если в банк поступает подложный платежный документ, возникает риск предъявления банку претензий клиента на данную сумму, если данный платеж будет проведен.

Существенное отличие данного подхода заключается в том, что риск возникновения основного события рассчитывается в результате Л-операций со значениями риска инициирующих событий. Значения риска инициирующих событий, например $P_{34} \cdots P_{38}$, основаны на результатах комплексного анализа различных оценок[4]. Также стоит отдельно отметить, что формула расчета финансовых потерь имеет ту же структуру, что и формула Базельского комитета для расчета резервирования под операционный риск[5].

В статье приведена модель возникновения НШС, на основе которой предложена структурная ЛВ-модель процесса мониторинга ИБ ПС, а также отдельно рассмотрен процесс мониторинга безопасности платежного процесса, для которого приведена формула расчета возможных потерь.

Предложенная ЛВ-модель процесса мониторинга ИБ ПС позволит описывать сложные зависимости между объектами анализа (событиями, инцидентами, уязвимостями и т. д.), а также связь

внутренних и внешних событий, инициирующих риски ИБ, как в контексте обеспечения безопасности платежного процесса, так и по направлению обеспечения ИБ ПС в целом.

Использование ЛВ-моделей при описании процессов по обеспечению ИБ позволяет исключить неопределенности, возникающие в процессе оценки влияния различных факторов на уровень ИБ ПС.

Примечания

[1] *Бухтин М.А.* Методика и практика управления операционными рисками в коммерческом банке. М.: ИБД АРБ, 2006; *Сазыкин Б.В.* Управление операционным риском в коммерческом банке. М.: Вершина, 2008; *Михеев В.А., Кузнецов А.В., Репин М.М.* Способ определения степени уязвимости автоматизированной информационной системы в отношении конкретных методов реализации угроз безопасности информации // Вопросы защиты информации. 2013. № 1. С. 20–25; Обеспечение информационной безопасности организаций банковской системы Российской Федерации: Методика оценки рисков нарушения информационной безопасности: Рекомендации в области стандартизации Банка России. РС БР ИББС-2.2-2009. Дата введения 01.01.2010. Приняты и введены в действие распоряжением Банка России от 11 ноября 2009 г. № Р-1190; *Астахов А.М.* Искусство управления информационными рисками. М.: ДМК Пресс, 2010; *Петренко С.А., Симонов С.В.* Управление информационными рисками: Экономически оправданная безопасность. М.: ДМК Пресс, 2005; *Петренко С.А.* Анализ рисков в области защиты информации. СПб.: Афина, 2009.

[2] *Соложенцев Е.Д.* Сценарное логико-вероятностное управление риском в бизнесе и технике. СПб.: Бизнес-пресса, 2004.

[3] *Карасева Е.И., Степанов А.Г.* Логико-вероятностная модель операционного риска банка // Информационно-управляющие системы. 2011. № 2. С. 77–83.

[4] *Бедрединов Р.Т.* Управление операционными рисками банка: Практические рекомендации. М.: Альпина, 2014.

[5] Международная конвергенция измерения капитала и стандартов капитала: новые подходы типа. [Электронный ресурс] URL: http://www.cbr.ru/today/ms/bn/bz_1.pdf (дата обращения: 10.05.2016).

М.М. Репин

Модели риска возникновения нарушений информационной безопасности в платежной системе

Процесс обеспечения раннего предупреждения рисков информационной безопасности в платежной системе является основным для определения необходимых управляющих воздействий по минимизации данных рисков.

Важным аспектом задачи предупреждения рисков является моделирование процесса их возникновения.

Данные модели могут быть описаны различными способами, в том числе и с помощью логико-вероятностных моделей, применение которых рассматривается в настоящей работе.

Ключевые слова: платежная система, ключевые индикаторы риска, логико-вероятностные модели, риск информационной безопасности, инициирующие события.

В процессе функционирования платежной системы (далее – ПС) могут возникать различные нештатные ситуации в ПС (далее – НШС), в том числе связанные с информационной безопасностью ПС. Учитывая тот факт, что область информационной безопасности в ПС имеет расширенные границы и включает в себя обеспечение безопасности платежных технологий, целесообразно рассматривать процесс возникновения НШС в целом, не акцентируя внимание только на классических областях обеспечения информационной безопасности.

Под НШС понимается ситуация, при возникновении которой произошло нарушение штатного функционирования информационно-вычислительных, телекоммуникационных, инженерных систем, систем связи, систем и средств защиты информации, ПС и технологии обработки платежных документов, повлекшее нарушение регламента обработки платежной информации или предоставления отчетности.

НШС можно разделить на три типа:

– НШС 1 типа – нештатная ситуация, влияющая на начало, ход или завершение операционного дня и/или осуществление (завершение) электронных расчетов в текущем операционном дне;
– НШС 2 типа – нештатная ситуация, не влияющая на начало, ход и завершение операционного дня, осуществление электронных расчетов в текущем операционном дне, но влияющая на решение других задач, реализуемых структурными подразделениями;
– НШС 3 типа – нештатная ситуация, не влияющая на начало, ход и завершение операционного дня, осуществление электронных расчетов в текущем операционном дне, а также решение других задач, реализуемых структурными подразделениями.

Рассмотрим процесс возникновения НШС в платежной системе.

Пусть $V = \{v_1, \ldots, v_n\}$ – множество уязвимостей ПС, $E = \{e_1, \ldots, e_k\}$ – множество событий в ПС, $I = \{i_1, \ldots, i_m\}$ – множество инцидентов ИБ в ПС, $NS = \{sns_1, \ldots, sns_l\}$ – множество сценариев НШС, NS – НШС. Например, событие e_2, связанное с уязвимостью v_2, совместно с событием e_3, не связанным с существующими уязвимостями, порождают инцидент i_2, в свою очередь, попадающий под сценарий НШС sns_1 и реализующий данную НШС. Аналогично можно описать представленную НШС по сценарию sns_{l-1}. События могут не являться инцидентом ИБ. Более подробно данный случай на примере события e_{k-2} проиллюстрирован в работе[1].

Использование сценарного подхода к процессу возникновения НШС позволяет применить для его описания логико-вероятностные модели, а также сценарный подход к анализу рисков возникновения НШС.

Возникновение НШС могут вызвать различные инциденты, связанные с объектами информационной инфраструктуры ПС, которые могут быть инициированы рядом факторов. Данные факторы могут быть описаны как ключевые индикаторы рисков в ПС и применены при проведении сценарного анализа риска (см. рис. 1).

Рис. 1. Процесс сценарного анализа рисков возникновения НШС

Под ключевыми индикаторами риска понимаются показатели или параметры, которые отражают актуальный уровень рисков возникновения событий и инцидентов в ПС, являющихся инициирующими событиями для НШС и повышающих риск возникновения НШС.

В качестве основных параметров индикаторов рисков целесообразно рассматривать[2]:

– предмет индикатора (предмет оценки);
– способы получения значений индикатора (формула расчета индикатора);
– пороговые значения индикатора;
– источники информации о состоянии индикатора;
– регулярность контроля индикатора;
– периодичность пересмотра индикатора.

Для примера опишем некоторые из верхнеуровневых факторов (ключевых индикаторов), влияющих на уровень риска возникновения НШС.

X_1 – процент неидентифицированных входящих электронных сообщений (далее – ЭС). Повышение данного показателя может свидетельствовать о наличии ошибок в системах клиентов, либо о попытках тестирования ПС.

X_2 – процент ЭС, забракованных из-за ошибок в их структуре или при наличии некорректного содержимого. Повышение процента подобных ЭС повышает риск проведения несанкционированных платежей и может свидетельствовать о наличии ошибок в системах клиентов или попытках проведения атак на ПС.

X_3 – неисправность серверов ПС (криптосерверов, серверов баз данных, файловых серверов и т. п.). Наличие ошибок в работе серверов ПС может повышать риски возникновения НШС, связанных с корректным функционированием ПС в целом, включая процессы обработки платежей, клиринга и др.

X_4 – неисправность каналов связи и сетевого оборудования. Наличие ошибок при передаче ЭС создает предпосылки для некорректной обработки платежной информации, ошибок при осуществлении клиринговых процессов и повышает риск ошибок функционирования ПС в целом.

X_5 – неисправность функционирования средств и систем защиты информации в ПС. Данные факторы влияют на такие риски, как осуществление несанкционированного доступа к объектам информационной инфраструктуры ПС, компрометация платежной информации и иные инциденты, связанные с нарушением ИБ ПС.

Таким образом, можно выделить множество $X = \{X_1 \cdots X_J\}$ – факторов, повышающих риски возникновения НШС. В то же время данные факторы могут сами являться НШС для подсистем ПС.

Сценарии ошибок функционирования объектов информационной структуры ПС позволяют построить граф-модель риска возникновения НШС[3].

Пусть общему состоянию ПС G соответствуют состояния ее подсистем $S = \{S_1 \cdots S_d\}$, а факторам $X = \{X_1 \cdots X_f\}$ случайные события, обозначаемые логическими переменными. НШС (итоговое событие) произойдет, если произойдет любое одно, два или все из событий множества. Данные производные события могут вызываться инициирующими событиями (факторами) $X = \{X_1 \cdots X_f\}$. Построим обобщенную граф-модель возникновения НШС (см. рис. 2). Граф-модель может содержать не только логические связи OR, но и AND, NOT, а также различные циклы.

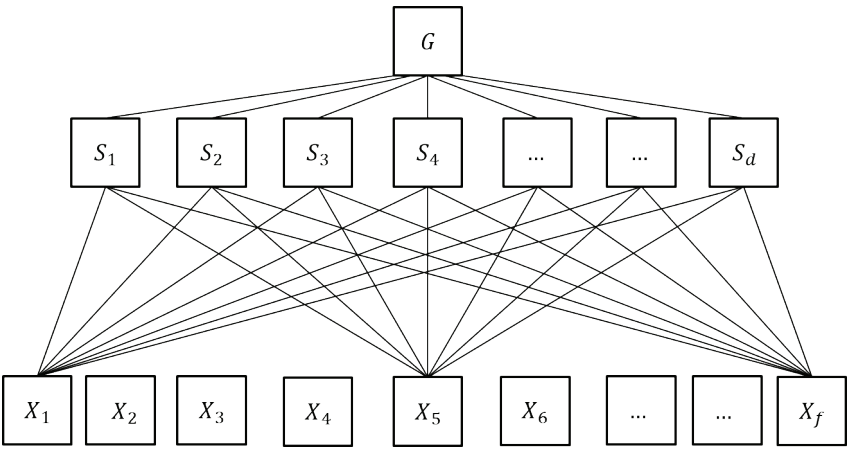


Рис. 2. Граф-модель риска НШС

На основе граф-модели риска можно записать логическую модель риска возникновения НШС:

$$G = S_1\{X_1 \cdots X_f\} \vee S_2\{X_1 \cdots X_f\} \vee S_d\{X_1 \cdots X_f\},$$

имеющую следующую ортогональную форму:

$$G = S_1 \vee S_2 \bar{S}_1 \vee S_3 \bar{S}_2 \bar{S}_1 \vee \cdots$$

Тогда описание вероятностной модели риска возникновения НШС можно представить как

$$P_r = P_1\{G_1 = 1\} = P_1 + P_2\{1 - P_1\} + P_3\{1 - P_2\}\{1 - P_1\} + ...,$$

где P_1, P_2, P_3, ... , P_d – вероятности событий S_1, S_2, S_3, ... , S_d.

В статье приведена модель возникновения НШС, на основе которой предложена структурная, логическая и вероятностная модели риска возникновения НШС.

Рассмотрен сценарный подход к анализу рисков возникновения НШС. Приведены примеры факторов риска (ключевых индикаторов), оказывающих влияние на общий риск возникновения НШС.

Предложенные модели возникновения НШС позволят описывать влияние факторов риска на подсистемы ПС и уровень риска возникновения НШС в целом, а также связь внутренних и внешних событий, инициирующих риски возникновения НШС.

Использование предложенных моделей при описании процессов по предупреждению рисков возникновения НШС позволяет исключить неопределенности, возникающие в процессе оценки влияния различных факторов на уровень ИБ ПС в целом.

Примечания

[1] *Казарин О.В., Репин М.М.* Модель процесса мониторинга состояния информационной безопасности платежной системы // в настоящем номере.

[2] *Бедрединов Р.Т.* Управление операционными рисками банка: практические рекомендации. М.: Альпина, 2014.

[3] *Соложенцев Е.Д.* Сценарное логико-вероятностное управление риском в бизнесе и технике. СПб.: Бизнес-пресса, 2004.

В.С. Кузнецов

Модель защиты облачного сервиса на основе модели открытой среды OSE/RM

В статье предложен алгоритмический подход к построению модели защиты облачного сервиса. В качестве основы представления облачной системы автором выбрана модель открытой среды OSE/RM, которая позволяет систематизировать и обосновать выбор механизмов защиты.

Для демонстрации возможности практического применения предложенного алгоритма построения модели защиты строится его модифицированное расширение, позволяющее адаптивно выполнять верификацию модели защиты облачной среды.

Ключевые слова: модель защиты, облачный сервис, модель открытой среды, верификация модели защиты.

В настоящее время разрабатываются разнообразные подходы к обеспечению безопасности информационных систем. Существует масса средств их реализации как программными и аппаратными механизмами, так и организационными мерами. Особую актуальность обретает системный подход к обеспечению информационной безопасности. В работе предлагается в качестве основного средства систематизации использовать эталонную модель POSIX OSE/RM, которая позволяет обосновать выбор адекватных механизмов защиты и сформулировать алгоритм построения модели защиты облачного сервиса.

Согласно определению IEEE POSIX 1003.0, открытой информационной системой (далее – ОИС) называется система, которая реализует открытые спецификации на интерфейсы, сервисы (услуги среды) и поддерживаемые форматы данных, достаточные для того, чтобы дать возможность должным образом разработанному прикладному программному обеспечению быть переносимым в широком диапазоне систем с минимальными изменениями, взаимодействовать с другими приложениями на локальных и удаленных системах и взаимодействовать с пользователями в стиле, который облегчает переход пользователей от системы к системе.

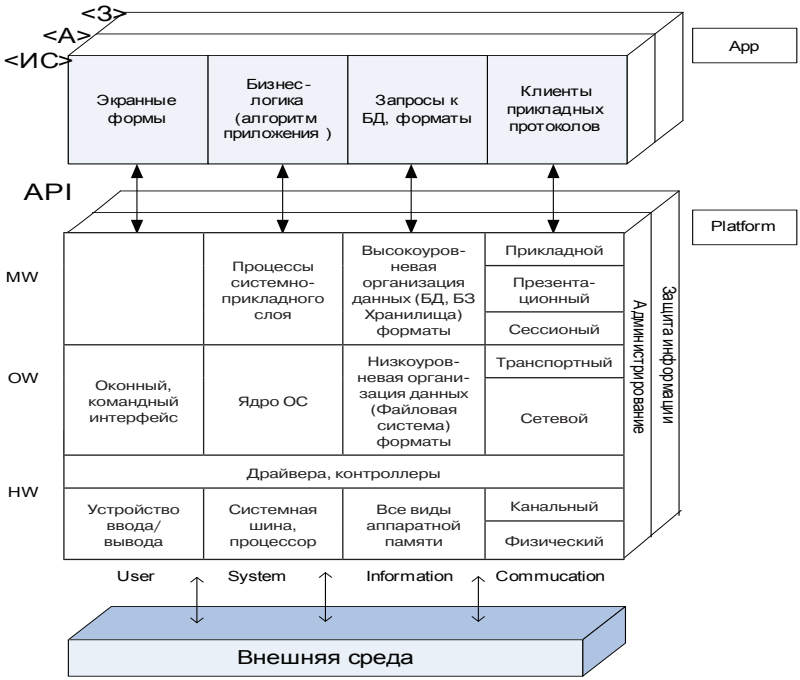


Рис. 1. Концептуальная модель OSE/RM

Подходы, описанные в стандарте[1], продолжают активно применяться, что дает основания использовать указанную модель при решении задач, связанных с обеспечением информационной безопасности (далее – ИБ).

Модель ОИС (рис. 1) представляется сочетанием платформенной и прикладной компонент, а также проекций базовой плоскости <ИС> на плоскость защиты <З> и администрирования <А>. Функциональное обслуживание представлено следующими видами услуг[2]: услуги, реализуемые операционной системой, услуги интерфейса «человек–машина», услуги организации данных, услуги, реализуемые столбцом System, сетевые услуги.

Кроме перечисленных видов услуг, существуют дополнительные, встроенные во все основные услуги: защиты информации, административного управления, а также набор инструментальных средств.

Данная модель реализует сервисный подход к представлению информационной системы (ИС), который на сегодняшний день

является наиболее прогрессивным. Его идея заключается в том, что ИС в целом представляется иерархией сервисов: прикладная компонента App – средство реализации бизнес-сервисов, которыми пользуются конечные пользователи, платформенная компонента – совокупность системных сервисов, необходимых для функционирования приложений. Если сервис – это используемый кем-то объект, то он должен опубликовать свой интерфейс (способ обращения к нему) для своих независимых пользователей. Системные сервисы предоставляются посредством API-функций, структурированных в соответствии с референсной функциональностью колонок модели OSE/RM.

Взгляд на ИС с позиции представления ее как средства реализации бизнес-процессов органично вписывается в современную парадигму развития вычислительных средств, парадигму, в которой на смену классическим ИС с ограниченным периметром и заданной заранее топологией приходят системы облачных вычислений. Облачные вычисления, согласно определению NIST[3], это модель обеспечения повсеместного и удобного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам – как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами и/или обращениями к провайдеру. На сегодняшний день облачные вычисления представляют собой новую парадигму информационных технологий. В западных странах деятельность всех участников информационного взаимодействия в рамках технологии облачных вычислений регламентирована в достаточной степени, что обеспечивает прозрачность и повышает эффективность данной технологии.

Потребитель услуг облачного провайдера, ориентируясь на потребности своих бизнес-процессов, арендует необходимые вычислительные мощности либо программное обеспечение. Таким образом, потребитель видит ИС, решающую его прикладные задачи, исключительно как совокупность бизнес-процессов, абстрагируясь от аппаратных ограничений. Поскольку бизнес-процессы потребителя выполняются на стороне провайдера облачных вычислений, остро встает вопрос защиты данных. С точки зрения защиты, представление ИС как совокупности бизнес-процессов говорит о том, что свойства, обеспечивающие безопасность бизнес-процессов, должны быть распространены на «клетки» всех плоскостей модели OSE/RM (рис. 2)[4]: т. е. для реализаций «клеток» базовой плоскости модели должны обеспечиваться свойства безопасности,

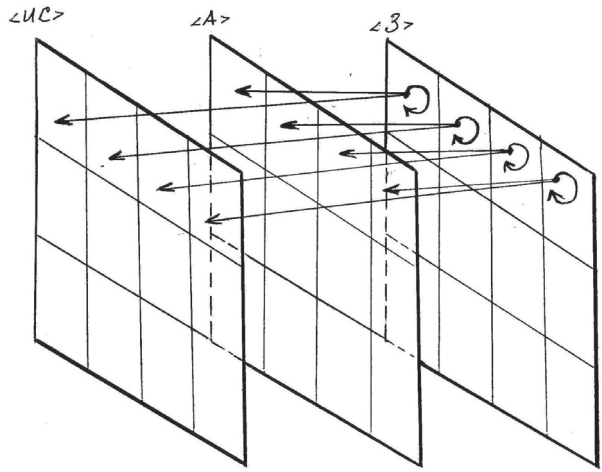


Рис. 2. Обеспечение безопасности клеток модели OSE/RM

аналогично для реализаций «клеток» плоскости администрирования <А> и защиты <З>.

В работе[5] автором продемонстрирована принципиальная возможность использования модели OSE/RM для описания облачной системы. Главной особенностью, отличающей модель OSE/RM классической ИС от модели облачного сервиса, является взаимодействие ИС потребителя облачных услуг и ИС провайдера. Бизнес-процессы потребителя облачных услуг выполняются как на стороне принадлежащих ему ИС, так и на стороне провайдера облачных услуг. В результате модель OSE/RM должна аккумулировать в себе (рис. 3) модели ИС провайдера и потребителя.

Таким образом, задача защиты информации в облачной системе эквивалентна задаче защиты набора бизнес-процессов, реализующих облачный сервис, на протяжении всех «клеток» его расположения в модели OSE/RM (рис. 3), поскольку информационные атаки в рамках ОИС представляются аналогичным образом в виде набора цепочек[6].

Оригинальный стандарт[7] описывает функции плоскости защиты достаточно поверхностно. ИБ в стандарте только обозначена как совокупность межкатегорийных защитных сервисов, что не дает возможности использовать референсное представление функциональности данной плоскости модели при построении модели защиты. Подходы, предложенные в стандарте, были расширены

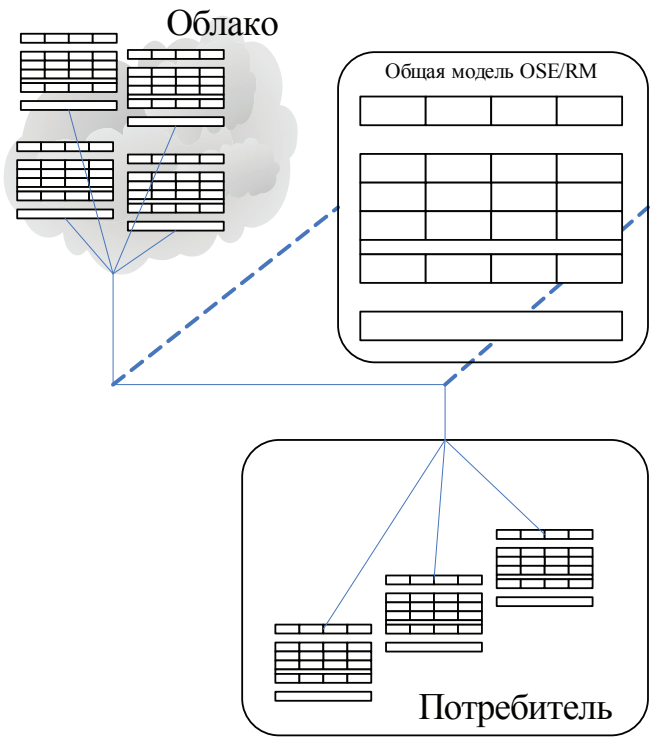


Рис. 3. Модель облачного сервиса

рядом авторов[8], что дает возможность использовать референсное представление плоскости защиты для решения прикладных задач ИБ.

Для обеспечения ИБ ОИС представим облачный сервис как совокупность бизнес-процессов. Любой бизнес-процесс, выполняемый в ОИС, реализует 4 вида операций над данными: хранение данных, обработка данных, передача данных (через носители информации), передача данных (через сеть). Всякая операция над данными однозначно определяется набором «клеток» модели OSE/RM, участвующих в ее функционировании.

Всякий механизм защиты реализуется в определенном наборе «клеток» модели ОИС. «Клетки» данного набора определяются целевым назначением механизма защиты. Необходимо отметить, что механизмы защиты являются сложными сущностями. Каждый механизм защиты может быть осуществлен каким-либо методом,

а каждый метод представляет собой программную или аппаратную реализацию некоторого алгоритма, который обеспечивает конфиденциальность, целостность или доступность. Определим *модель защиты облачного сервиса* как совокупность механизмов защиты, реализованных в рамках конкретной ИС.

Рассмотрим модель ОИС в виде, представленном на рис. 4.

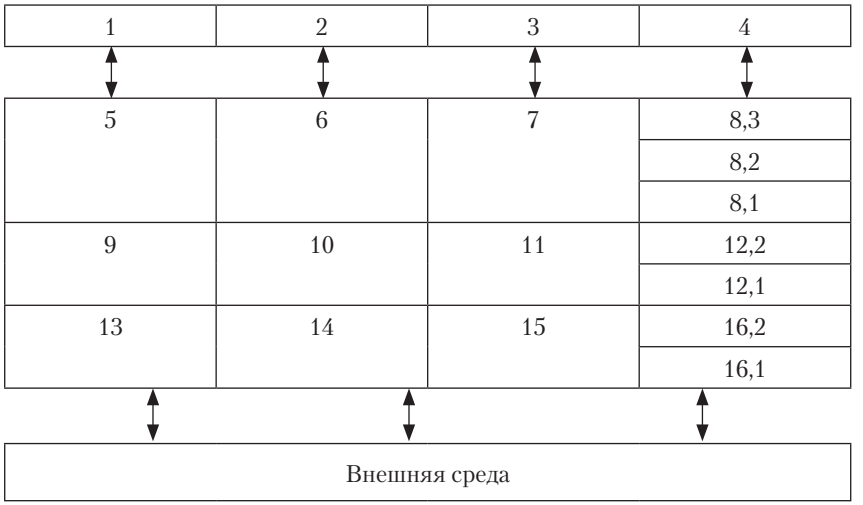


Рис. 4. Упрощенный вид OSE/RM

Для решения задачи построения модели защиты облачного сервиса определим следующие объекты (нумерация соответствует предложенной на рис. 4 модели):

– операции над данными O: $O = \{o_1, o_2, \ldots, o_n\}$, $o_i \in \{1,16\}$;
– бизнес-процесс B: $B = O_i \rightarrow \ldots \rightarrow O_j$, $i, j \in \{1,4\}$;
– механизм защиты Mx: $Mx = \{m_1, m_2, \ldots, m_n\}$, $m_i \in \{1,16\}$;
– облачный сервис S: $S = \mathrm{U}B_i$, $B_i \cap B_j \neq 0$.

Используя введенные определения, можно предложить следующий алгоритм.

Вход: $S = \mathrm{U}B_i$, $B_i \cap B_j \neq 0$, $Mx = 0$.

Шаг 1. Выбрать бизнес-процесс B_1, построить для него $B_1 = O1_i \rightarrow \ldots \rightarrow O1_j$, $i, j \in \{1,4\}$;

Шаг 2. На основе множества, полученного на шаге 1, сформировать множество цепочек вида $O1 = \{o1_1, o1_2, \ldots, o1_n\}$, $o1_i \in \{1,16\}$;

Шаг 3. Сформировать множество механизмов защиты $Mx_1 = \{m1_1, m1_2, ..., m1_n\}$, $m1_i \in \{1,16\}$ для множества цепочек, полученных на шаге 2, причем множество считается окончательно сформированным, если Mx_1 есть биекция $O1$;

Шаг 4. $Mx = Mx \cup Mx_1$, если обработаны все входящие B_i – то выход, иначе, шаг 1;

Выход: Модель защиты ИС $Mx = \cup Mx_i$.

Верификация модели защиты облачной системы.

В качестве иллюстрации продемонстрируем, как алгоритм построения модели защиты ИС может быть использован для выполнения верификации существующей модели защиты для заданного облачного сервиса. Далее автором предлагается модификация алгоритма построения модели защиты с целью выполнения верификации модели защиты облачного сервиса. В алгоритме использованы следующие условные обозначения.

Mx_B – верифицируемая модель защиты, представляет из себя совокупность механизмов защиты.

Алгоритм верификации модели защиты.

Вход: $S = \cup B_i$, $Mx_B = \cup Mx_i$.

Шаг 1. Выбрать бизнес-процесс B_1, построить для него $B_1 = O1_i \rightarrow ... \rightarrow O1_j$, $i, j \in \{1,4\}$;

Шаг 2. На основе множества, полученного на шаге 1, сформировать множество цепочек вида $O1 = \{o1_1, o1_2, ..., o1_n\}$, $o1_i \in \{1,16\}$;

Шаг 3. Сформировать множество механизмов защиты $Mx_1 = \{m1_1, m1_2, ..., m1_n\}$, $m1_i \in \{1,16\}$ для множества цепочек, полученных на шаге 2, причем множество считается окончательно сформированным, если Mx_1 есть биекция $O1$;

Шаг 4. $Mx = Mx \cup Mx_1$, если обработаны все входящие B_i – то выход, иначе, шаг 1;

Выход: Если модель защиты ИС $Mx = \cup Mx_i$, построенная в процессе работы алгоритма, совпадает с верифицируемой моделью защиты ($Mx_B = Mx$), то верифицировать модель защиты, иначе считать верифицируемую модель защиты неоптимальной.

Подход к созданию модели защиты на основе строгого описания защищаемой системы моделью OSE/RM, предложенный в работе, дает ряд преимуществ:

– формируется условный защищаемый периметр, определяемый функционированием бизнес-процессов потребителя облачных услуг;
– обосновывается выбор механизмов защиты и необходимое их количество;
– представляется однозначным образом база, необходимая для проведения верификации модели защиты.

Не теряя основных преимуществ облачных систем, таких как децентрализованность, произвольное изменение топологии и др., можно обеспечить информационную безопасность целевой системы.

Примечания

[1] ISO/IEC TR 14252-96. Information technology. Guide to the POSIX Open System Environment (OSE). 1996.

[2] *Бойченко А.В., Кондратьев В.К., Филинов Е.Н.* Основы открытых информационных систем / Под ред. В.К. Кондратьева. М.: ЕОАИ, 2004.

[3] NIST Cloud Computing Standards Roadmap / National Institute of Standards and Technology, Special Publication 500–291. 2011. July. https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

[4] *Бойченко А.В., Лукинова О.В.* Применение модели POSIX OSE/RM при построении подсистем информационной безопасности // Интеллектуальные системы (AIS'10); Интеллектуальные САПР (CAD-2010): Тр. междунар. науч.-практ. конф. Т. 2. М.: Физматлит, 2010. С. 473–476.

[5] *Кузнецов В.С.* Интерпретация облачных вычислений как открытой информационной системы. Материалы III Всероссийской молодежной конференции по проблемам информационной безопасности «Перспектива 2013». (Таганрог, 9–12 июля 2013 г.). – Таганрог, 2013. С. 171–177.

[6] *Кузнецов В.С., Лукинова О.В.* Представление информационных угроз на основе модели открытой среды // Научно-технический вестник информационных технологий механики и оптики. 2013. № 4 . С. 138–143.

[7] ISO/IEC TR 14252-96.

[8] См. примеч. 2, 4, 6.

Г.А. Шевцова, А.А. Мозгов

Особенности защиты информации в выставочной деятельности

В статье представлены проблемные аспекты подготовки участия организации в выставочной деятельности, имеющей в обращении конфиденциальную информацию. Недостаточность разработки темы информационной безопасности в сфере выставочной деятельности влечет за собой слабую нормативно-правовую базу, которая необходима для регулирования вопросов защиты информации в этой сфере.

Ключевые слова: выставочная деятельность, уязвимость безопасности конфиденциальной информации, защита информации в выставочной деятельности, безопасность предоставления выставочных услуг.

Выставки обладают комбинированными свойствами продвижения товаров и услуг на рынок, и потому выставка – один из наиболее эффективных маркетинговых инструментов. С помощью выставок эффективно решаются задачи представления и продвижения товаров и услуг, новейших достижений во всех (социальной, экономической, научной) сферах деятельности, как отдельных организаций, так и целых регионов и даже государств. Выставки представляют эти достижения широкому кругу лиц, среди которых есть как обыватели, так и специалисты. При этом одна из важнейших особенностей выставок заключается в том, что на выставках создаются и продаются не материальные продукты, а информация о товарах и услугах и их особенностях. То есть выставки – это информационные площадки, центры сосредоточения информации о научных, экономических, культурных и управленческих достижениях, новейших товарах и услугах, их достоинствах и преимуществах[1].

В условиях конкуренции, сложившихся в свете изменений, происходящих в современной мировой экономике, при возрастающей потребности в широком представлении достижений не только отдельных организаций, но и отдельных стран, информация, циркулирующая в сфере выставочной деятельности, обретает особую

ценность, переходя в разряд стратегических ресурсов организаций, государств, общества.

В условиях такой конкуренции организациям, стремящимся, например, к усилению своего влияния на определенных рынках сбыта, или же к поиску новых рынков сбыта и способов выхода на эти рынки, следует учитывать значение и ценность информации о продвигаемых товарах и услугах. Именно выставки позволяют наиболее эффективно решить сразу целый ряд задач, сопутствующих процессу продвижения товаров и услуг на определенных рынках сбыта[2]. Так, в рамках одной выставки можно одновременно провести презентацию новых товаров и услуг организации, совместив эту работу с работой по выпуску рекламной продукции для данных товаров и услуг, предпринять шаги по выведению их на международные рынки, изучить сопутствующий спрос на различных рынках. При этом свою продукцию можно продемонстрировать не только целевой аудитории, но и посетителям, не входящим в ее состав.

Выставки решают для организации не только задачу эффективного распространения рекламных материалов между максимальным количеством потенциальных покупателей, но и дают возможность для работы в области поиска новых партнерских связей и заключения различных соглашений, реализации решений имидж-рекламы[3]. Можно с уверенностью утверждать, что для любой организации участие в выставке – это один из наиболее эффективных способов заявить о себе и расширить партнерские связи.

Информация, оглашаемая на выставках, имеет для организации зачастую колоссальное значение. Это обусловлено несколькими факторами. В первую очередь – значениями регулярности проходящих выставок, а конкретнее – периодами относительного затишья и пустоты в рекламной деятельности, имеющими место в периоды между выставками. А также тем, что выставки охватывают огромные аудитории потенциальных потребителей экспонируемых товаров и услуг. В этих условиях наиболее оптимальным решением является демонстрация новинок организации, инновационных решений и ноу-хау. Иными словами, когда выставка по соответствующей тематике проходит лишь раз в год, или даже раз в несколько лет, имеет смысл демонстрировать на такой выставке лишь самую новую продукцию организации. Логично, что часто информация о таких новинках, готовящихся иногда даже специально к датам выставок, является конфиденциальной, принадлежащей к разряду коммерческой тайны. Кроме того, выставочная деятельность является и сама по себе, и также в связке с иной деятельностью по обмену информацией с внешней средой – рекламной

и издательской, опционально, сопровождается переговорными процессами, создающими дополнительные уязвимости безопасности конфиденциальной информации. В силу этих особенностей выставочной деятельности, а также в силу значимости оглашаемой на выставке информации задача защиты информации в выставочной деятельности является не просто актуальной, но стоит весьма остро для любой организации.

Выставочная деятельность является предметом научных исследований экономики, социологии, политологии, психологии, юриспруденции и международных отношений. Однако несмотря на значительный объем литературы во многих областях научных исследований, многие вопросы организации защиты информации в выставочной деятельности не были в достаточной степени освещены, а деятельность по защите информации в выставочной сфере, в процессе подготовки и участия организаций в выставках изучена слабо. Это отчасти обусловлено тем, что все еще слабо изучены сами выставки – и как специфические организации, и как экономический и культурный феномен, и как маркетинговый инструмент.

Большая часть опубликованных материалов на темы, касающиеся выставок, либо не затрагивает вопросы защиты информации, либо затрагивает их поверхностно. Меж тем вопросы защиты информации в выставочной деятельности охватывают не только сферы технического оснащения и организационных мер по поддержанию режима конфиденциальности в процессе рекламной и издательской деятельности, но и вопросы маркетинга, управления, кадрового оснащения и подготовки персонала.

Недостаточная разработанность темы защиты информации в сфере выставочной деятельности влечет за собой недостаточную полноту теоретической базы по данной тематике, что, в свою очередь, отражается на качестве предлагаемых практических решений, которые рекомендуется применять для решения задач защиты информации в сфере выставочной деятельности. Это одна из главных фундаментальных проблем защиты информации в сфере выставочной деятельности на сегодняшний день.

Эта проблема тесно связана и находится практически в прямой зависимости от другой основной проблемы – руководители организаций-экспонентов при подготовке к выставкам чаще всего недооценивают серьезность угроз безопасности информации, которые могут возникать в процессе выставочной деятельности, и соответственно пренебрегают мерами защиты информации.

Тем более остро, в свете обозначенных проблем, стоят проблемы, связанные с человеческим фактором, с действиями персонала.

Независимо от уровня подготовки персонала человеческий фактор, всегда имеющий место в процессе выставочной деятельности, оставляет возможность реализации таких угроз конфиденциальности информации, как незапланированное разглашение информации, составляющей коммерческую тайну, и даже банальная кража или утеря носителей информации, в том числе самих выставочных экспонатов.

А между тем одна из важнейших особенностей выставок заключается в том, что в процессе подготовки и участия в выставках происходит интенсивный обмен информацией между организацией и внешней средой. Даже при наличии у организации действующей системы защиты информации в процессе выставочной деятельности может возникать множество дополнительных каналов утечки конфиденциальной информации, множество дополнительных условий для реализации угроз конфиденциальности информации, ее целостности, доступности. Кроме того, информация, обрабатываемая в процессе выставочной деятельности, предназначается для оглашения, а значит, к моменту оглашения должны быть решены и задачи сохранения ее достоверности, своевременности, полноты. Угрозы безопасности информации могут возникать на всех этапах выставочной деятельности.

Такая опасность обусловлена в первую очередь многообразием видов деятельности, сопутствующих процессу участия организации в выставках, что соответственно добавляет множество дополнительных факторов, влияющих на условия поддержания режима информационной безопасности.

В частности, условия наибольшей опасности для конфиденциальности информации на этапе подготовки к выставке создает процесс производства рекламы. Этот процесс характеризуется наиболее интенсивным обменом потенциально и фактически конфиденциальной информацией как с внешней средой, так и внутри организации. Специфика процесса производства рекламной продукции в выставочной деятельности заключается в многообразии целей, которые преследуются при производстве этих материалов. Они могут использоваться как непосредственно в рекламной деятельности, так и в качестве элементов оформления выставочного стенда, в качестве материалов, используемых при публикации пресс-релизов, или для передачи их представителям специализированной прессы. Это верно как для организаций, рекламирующих свою собственную деятельность, так и для подрядчиков и субподрядчиков, экспонирующих на выставках продукцию своих заказчиков или разрабатывающих рекламные материалы для других организаций.

Так как на этом этапе информация, несомненно, содержит конфиденциальную составляющую, то угрозы нарушения конфиденциальности, целостности и доступности информации могут быть реализованы с наибольшим ущербом. Проведение экспертизы этих материалов на предмет наличия в них конфиденциальной информации и последующее составление перечней конфиденциальной информации, содержащейся в этих материалах, является необходимостью. Пренебрежение мерами защиты информации на этапе производства рекламы гарантированно создает условия для нарушения конфиденциальности информации и несанкционированного оглашения конфиденциальной информации.

При этом остро стоит необходимость решения задач контроля над деятельностью рекламопроизводителя, независимо от того, является ли он третьим лицом, которому была передана информация, или же реклама разрабатывается с использованием ресурсов самой организации. По окончании этапа разработки рекламной продукции и ее производства рекламоносители не должны содержать информацию, составляющую коммерческую тайну организации. При этом важно не допустить искажения достоверности информации, которая будет отображена на рекламоносителях.

Процесс контроля является достаточно трудоемким и подразумевает заключение различных договоров с рекламопроизводителями, в том числе и договоров о неразглашении, обязывающих компании или сотрудников, занимающихся производством рекламы, охранять конфиденциальность переданной им информации.

Необходимость действовать в правовом поле для обеспечения защиты конфиденциальности своей информации в процессе ведения выставочной деятельности открывает еще одну фундаментальную проблему как в сфере защиты информации в выставочной деятельности, так и в сфере ведения выставочной деятельности в общем, проблему, присущую этой сфере в Российской Федерации.

Крайне слаба нормативно-правовая база, которая необходима, чтобы регулировать вопросы выставочной деятельности. По степени нормативной обеспеченности законодательство Российской Федерации в сфере регулирования выставочной деятельности значительно отстает как относительно ситуации в других отраслях, так и относительно соответствующих сфер законодательства других стран. Иными словами, российское законодательство в сфере ведения выставочной деятельности не актуализировано относительно международных законов и соглашений, соответственно которым осуществляется сотрудничество в этой сфере с другими странами. Оно оторвано от современных реалий развития и функционирования рынка выставочных и рекламно-выставочных услуг и мероприятий.

В частности, отсутствуют как Федеральный закон о выставочной или выставочно-ярмарочной деятельности, так и комплекс национальных стандартов, регламентирующих требования к качеству и безопасности предоставления выставочных услуг. Иными словами, отсутствует единая система регулирования выставочной деятельности, а существующая система не соответствует сложившейся иерархии и структуре нормативных и правовых документов, регулирующих деятельность в основных отраслях экономики.

К сожалению, явные проблемы с законодательным обеспечением в сфере выставочной деятельности обусловливают и специфику работы в этой сфере. Руководителю организации-экспонента при подготовке к участию в выставке и непосредственно при участии приходится руководствоваться целым рядом различных законов, относящихся к различным сферам законодательства. Каждый из этих законов регулирует малую часть того, что в целом составляет единый процесс подготовки к выставке.

В силу такой неоднородности законодательной базы, а также в силу отсутствия единых механизмов контроля в правовой сфере, в том числе касательно информационной безопасности, некоторые правовые методы защиты информации в сфере выставочной деятельности применять на практике оказывается весьма сложно. Это касается, например, составления отдельных договоров об охране экспонатов, составляющих коммерческую тайну, с оргкомитетами выставочных площадок. С одной стороны, это должно было бы быть распространенной практикой, но в реальности оргкомитет выставочной площадки чаще всего отвечает за охрану выставочных экспонатов лишь косвенно, заключая договоры об оказании охранных услуг с частными охранными организациями. Выходит, что экспоненту пришлось бы, в худшем случае, заключать отдельный договор с охранной организацией, ответственной за поддержание пропускного режима на территории выставки. Кроме того, экспоненту пришлось бы составлять отдельные списки экспонатов и материалов, составляющих коммерческую тайну, и раскрывать их и оргкомитету, и охранной организации, а значит, заключать и соглашения о неразглашении – все это является весомой дополнительной нагрузкой и на материальные, и на человеческие ресурсы организации. Соотношение затрат ресурсов и получаемой выгоды говорит не в пользу таких правовых решений. Поэтому многие экспоненты предпочитают решать вопросы охраны своих экспонатов с помощью ресурсов своих собственных выставочных стендов.

Кроме того, нужно принимать во внимание специфику работы с определенными видами тайн. При этом в тексте основополагающего в вопросах защиты коммерческой тайны закона – закона

«О коммерческой тайне» – не упоминаются слово «выставка» или словосочетание «выставочная деятельность». Тем не менее механизмы обеспечения конфиденциальности защищаемой информации, описанные в этом законе, могут быть использованы не только на стадии отбора информации, которая будет разглашена в процессе непосредственного участия в выставке, но и при контактах с контрагентами. Например, при заключении договоров с организациями, ответственными за подготовку рекламных материалов, а также с другими организациями, сотрудничество с которыми необходимо для организации, желающей экспонировать свою продукцию на выставке.

Для выставочной деятельности существуют и другие нюансы, уникальные исключительно для этого вида деятельности. Наличие таких особенностей обусловлено тем, что в ходе выставки информацию можно получить не только посредством изучения специально подготовленных печатных и иных рекламных материалов, но и осматривая сами экспонаты, а также беседуя с задействованным в работе на стендах персоналом. В частности неотъемлемыми частями выставочного процесса являются такие виды деятельности, как промышленный шпионаж и изучение продукции конкурентов. Поэтому в процессе участия в выставке, организации, в целях защиты конфиденциальной информации, следует проявлять осторожность не только в выборе выставочных образцов, но и в выборе способа их презентации, а также в подборе персонала и составлении должностных инструкций.

Особое место в процессе подготовки к выставке занимают такие задачи, как выбор типа выставочного стенда и согласование режима работы стенда. При проектировании выставочного стенда закладывается система технической защиты информации. Ориентиром при этом является то, какая конфиденциальная информация и в каком виде должна быть предоставлена для оглашения в режиме ограниченного доступа, если такая возможность предусмотрена. При этом информация о конфигурации системы защиты, закладываемой в проект выставочного стенда, в процессе подготовки к выставочной деятельности также может считаться конфиденциальной информацией, подлежащей защите.

Уникальность выставочных условий, в которых осуществляется выставочная деятельность персонала организации и ее выставочного стенда, является еще одной особенностью выставок, крайне важной при рассмотрении вопросов защиты информации. В первую очередь, сам выставочный стенд – это конструкция, собираемая с нуля на территории выставочных площадей всего за несколько дней. Это хрупкие конструкции, предназначенные, в первую

очередь, для размещения рекламных материалов и эффективной демонстрации экспонатов. Даже если система защиты информации заложена в проект выставочного стенда, его функционал никак не будет способен полностью отвечать всем требованиям, предъявляемым к режимным помещениям, в которых производится обработка конфиденциальной информации или хранение носителей конфиденциальной информации. В первую очередь, хрупкость конструкции выставочных стендов обусловливает невозможность организации достаточно эффективной системы контроля физического доступа, включающей в себя контрольно-пропускные пункты и эффективные средства запирания дверей. Поэтому в условиях выставки особенно актуальными становятся угрозы безопасности информации, обусловленные слабыми мерами по ограничению доступа, применяемыми к носителям конфиденциальной информации. Особенно это актуально для стендов, на которых производится оглашение информации, предназначенной для ограниченного распространения.

Отчасти эта проблема решается посредством размещения на стенде выставочного персонала в необходимом количестве и составлением четких должностных инструкций, в которых вопросы защиты конфиденциальности информации и защиты носителей информации должны быть раскрыты. Не стоит забывать, однако, что в условиях выставочной суеты повышается и риск ошибок персонала.

Еще одной особенностью выставочной деятельности является то, что в процессе непосредственного участия в выставке состав угроз и приоритет, отдаваемый тем или иным угрозам, значительно меняется. Так, угрозы нарушения конфиденциальности информации остаются действительными только для отдельных видов информации и связанных с ними носителей. Речь идет, конечно, о рекламных материалах, предназначенных для закрытых показов, а также об определенных экспонатах, утеря которых может повлечь за собой финансовые потери в силу утечки конфиденциальной информации, содержащейся в этих экспонатах. При этом утеря носителя такой информации в результате его необратимых повреждений – не такая большая проблема, так как ущерб от такой утери будет нанесен только качеству выставочного процесса. Это нежелательно, но не катастрофично. Остальные материалы, к моменту опубликования в рамках выставки, в подавляющем большинстве своем уже не содержат никакой конфиденциальной информации.

При всех проблемах, косвенно или напрямую касающихся работы персонала, процессу подбора персонала для участия в выставке следует уделять особое внимание. В том числе и потому, что персонал стенда в условиях выставки является одновременно и инст-

рументом для сдерживания угроз безопасности информации, и источником этих угроз.

Кроме квалифицированных и компетентных работников компании, уполномоченных в процессе выставки решать различные вопросы, для эффективной работы стендов необходимо также огромное количество промоперсонала. Зачастую такой персонал набирается PR-менеджером в рекламных агентствах, которые предоставляют также и супервайзеров, следящих за работой промоутеров. Так как в отношении участников выставки конкурентами могут быть использованы меры агентурной разведки – вербовка, покупка конфиденциальной информации, выведывание информации под каким-либо благовидным предлогом, то на подготовительном этапе состав участников выставки должен быть включен в состав конфиденциальных сведений. Относительно этой информации также актуальны все те угрозы нарушения конфиденциальности информации, что и для любой другой. Кроме того, при разработке системы защиты информации выставочного стенда и при рассмотрении возможных угроз безопасности информации на выставочном стенде внештатный промо-персонал, нанятый для работы на стенде необходимо рассматривать и как потенциальных внешних, и как потенциальных внутренних нарушителей.

Особенности работы с персоналом выставочного стенда – это также особенность выставочной деятельности, которую следует учитывать при решении вопросов защиты информации.

Отдельно стоит отметить сложности проведения переговоров в условиях выставки. Кроме проблемы предоставления второй участвующей в переговорах стороне определенной информации, существует также и проблема сокрытия разглашаемой в процессе переговоров информации от третьих лиц, что соотносится в условиях выставки с определенными сложностями.

В первую очередь, информация, разглашаемая второй стороне, не должна содержать сведений, составляющих коммерческую тайну и других сведений, не предназначенных для разглашения. Угроза неправомерного ознакомления с защищаемой информацией является главной в этом процессе. В данном случае угроза может быть реализована только внутренним нарушителем. То же справедливо и для такой сферы, как работа с посетителями, осуществляемая персоналом стенда в процессе непосредственного участия в выставке.

В соответствии с особенностями выставочного процесса, наибольшие трудности вызывает именно проблема организации закрытого переговорного процесса в условиях выставки. Эта проблема решаема, если выставочная площадка располагает собственным помещением, предназначенным для переговоров, которое

соответствует всем требованиям как безопасности в целом и защиты информации в частности, предъявляемым к помещениям такого типа. Однако если выставочная площадка не может предоставить такое помещение, то проблему необходимо решать средствами конструкции выставочного стенда или иными средствами. Противодействие угрозам неправомерного ознакомления с защищаемой информацией также стоит в этом вопросе на первом месте. Угрозы могут быть реализованы как внутренним, так и внешним нарушителем, при условии слабости или полного отсутствия системы контроля физического доступа, организованной на выставочном стенде.

Хотя каналов утечки информации и возможных угроз существует множество, но на практике в условиях выставочной деятельности большинство из них так и остается лишь потенциальными угрозами. Главная особенность защиты информации в выставочной деятельности кроется именно в том, что существует необходимость адаптировать организационные меры и инженерно-технические средства защиты информации к выставочным условиям, накладывающим ограничения на возможности использования отдельных мер и средств. Но это касается не только средств защиты информации, но и средств ее неправомерного съема – использование таких средств в условиях выставки сопряжено с определенными трудностями, преодолеть которые чаще всего не представляется возможным.

К таким сложностям относится, например, проблема невозможности скрытного использования многих и многих средств съема информации, ввиду того что потенциальный нарушитель всегда находится на виду у большого числа людей – посетителей выставки. Кроме того, чтобы использовать средства съема информации, их нужно сначала пронести на территорию выставки, что тоже вызывает затруднение. Так, на любой выставке, открытая она или закрытая, всегда организованы и действуют контрольно-пропускные пункты, снабженные системами обнаружения запрещенных предметов у посетителей – арочные или портативные металлодетекторы. Кроме того, часто производится досмотр ручной клади посетителей. Обыкновенно работники службы охраны компании-организатора или собственной службы охраны площадки также патрулируют территорию выставки. Все это затрудняет использование нарушителем технических средств съема информации даже в условиях равнодушия к происходящему у рядовых посетителей выставки.

Если соблюдены условия применения определенных организационных мер защиты информации, можно утверждать, что

инсайдерская информация или коммерческая тайна, раскрываемая на выставке, будет относиться только к продукции, представляемой на выставке, и не будет иметь серьезного коммерческого веса. То есть информация, раскрываемая в процессе участия компании в выставке, чаще всего не является достаточно ценной, чтобы оправдать использование сложных и дорогостоящих технических средств. Все вероятные угрозы реализуются нарушителем с низким потенциалом, чаще всего действующим из собственных корыстных интересов.

Кроме того, не стоит забывать, что на выставках разглашается информация, которая и предназначена для обнародования. Рекламная литература, фото- и видеоматериалы, материалы для презентаций и другие источники информации проходят несколько стадий отбора в процессе подготовки к участию в выставке и не являются носителями конфиденциальной информации. И здесь меры защиты информации, принимаемые на стадии подготовки к выставке, безусловно, являются очень действенными.

Таким образом, количество реальных угроз информационной безопасности, которые могут быть реализованы в процессе выставочной деятельности, а также их уровень сводятся к приемлемому минимуму самими условиями, в которых проходит выставочная деятельность. Значит, основными задачами защиты информации в сфере рекламной и выставочной деятельности являются отбор информации для оглашения и грамотное применение комплекса мер по обеспечению охраны конфиденциальности информации в процессе подготовки компании к выставке. Существует целый ряд мер, способствующих противодействию угрозам нарушения конфиденциальности информации, возникающим при подготовке и участии в выставочной деятельности, проведении переговоров и работе с посетителями. Так, контроль над охраной конфиденциальности информации осуществляется по трем направлениям принимаемых мер – правовым, организационным и техническим. Но все они служат одной цели – созданию и поддержанию политик разграничения доступа и контролю следования работников этим политикам.

Примечания

[1] ГОСТ Р 53103–2008 «Деятельность выставочно-ярмарочная. Термины и определения». [Электронный ресурс] URL: http://www.rags.ru/stroyka/text/56921/ (дата обращения: 07.09.2016).

[2] Распоряжение Правительства РФ от 31.07.2013 г. № 411-РП «О Московском городском совете по конгрессно-выставочной деятельности»; Положение о Московском городском совете по конгрессно-выставочной деятельности. [Электронный ресурс] URL: http://mosopen.ru/document/411_rp_2013-07-31 (дата обращения: 07.09.2016).

[3] Постановление губернатора Московской области от 28.12.1998 г. № 406-ПГ «Об утверждении Положения о выставочно-ярмарочной деятельности администрации Московской области». [Электронный ресурс] URL: https://www.lawmix.ru/moscow-obl/320 (дата обращения: 07.09.2016).

Д.А. Иванов, А.П. Никитин

Метод текстозависимой аутентификации по голосу

В данной работе был предложен метод биометрической аутентификации пользователя по параметрам его голоса. В качестве основных параметров разрабатываемой модели были выбраны индивидуальные особенности скорости и длительности произношения отдельных элементов речи.

При разработке алгоритма сравнения образцов голоса было обнаружено, что анализ скорости и длительности произношения отдельных элементов речи в текстозависимой процедуре аутентификации пользователя сводится к нахождению процентного содержания совпадающих по содержимому и местоположению отрезков записи с учетом изменяемости общей длины произносимой парольной фразы (сравнение наборов мелчастотных кепстральных коэффициентов).

Ключевые слова: биометрика, аутентификация по голосу, метод мелчастотных кепстральных коэффициентов

В большинстве работ при решении задачи распознавания диктора используются параметры в виде коэффициентов кепстра. Кепстральные коэффициенты вычисляются по огибающей спектра, полученного через преобразование Фурье, с помощью гребенки фильтров. Также возможно вычисление по передаточной функции речевого тракта, найденной методом линейного предсказания.

Для процедуры аутентификации по голосу следует использовать свойства, обладающие высокой индивидуальностью[1]. Частотные характеристики отдельных звуков хотя и обладают большим разнообразием, однако из-за явления аккомодации нахождение и выделение самих звуков в случайной записи осложнено, а сами акустические параметры голоса пользователя при произношении некоторых звуков могут не отражать анатомию речевого тракта[2].

Следует отметить, что относительные скорости произношения звуков, определенные в данной работе как отношение длительности выделенного звука (элемента речи) к длительности всего выбран-

ного отрезка речи, хотя и являются вариативными от состояния человека в спокойной обстановке, имеют относительно небольшую изменяемость для одного индивида[3].

Поэтому в данной работе рассматривается текстозависимый вариант метода биометрической аутентификации. Для него можно однозначно определять относительные скорости произношения отрезков речи.

В данной работе были выбраны следующие параметры для проведения процедуры аутентификации: спектральные характеристики парольной фразы и ее отрезков, относительные скорости произношения отрезков фразы, как включающие в себя индивидуальные особенности артикуляции пользователя. Спектральные характеристики самой фразы в данном случае используются для проверки самого пароля.

Следует учитывать, что дальнейшее увеличение частоты дискретизации по достижению значения 32 000 Гц увеличивает точность распознавания только пользователей с высоким, профессионально поставленным голосом. В действительности основной диапазон человеческой речи 80–6000 Гц, причем значения меньше 160 Гц в основном достигаются низкими мужскими голосами. Частоты в диапазоне 6000–16 000 Гц в основном заполняются согласными звонкими или «щелкающими» звуками, учет данного диапазона также увеличивает точность распознавания голоса.

В зависимости от сферы применения следует учитывать и объем анализируемых данных, в общем случае пропорциональный произведению частоты дискретизации, глубины звучания и длительности записи. На рисунке 1 показаны графики зависимости размера односекундной записи от частоты дискретизации для различных значений глубины звучания.

Для увеличения скорости и точности процедуры аутентификации пользователя из записи следует вырезать не содержащие информацию отрезки в начале и конце записи.

Метод мел-частотных кепстральных коэффициентов (далее MFCC – Mel-frequency cepstral coefficients) извлечения признаков является одним из самых распространенных как в системах распознавания дикторов, так и в системах распознавания речи[4]. Он обладает следующими особенностями:

– благодаря использованию спектра сигнала, при дальнейшем анализе учитывается его волновая природа;
– спектр проецируется на мел-шкалу, мел является психофизической единицей высоты звука, это позволяет учитывать особенности восприятия человека и выделять наиболее значимые в речи частоты, а следовательно, содержащие больший объем инфор-

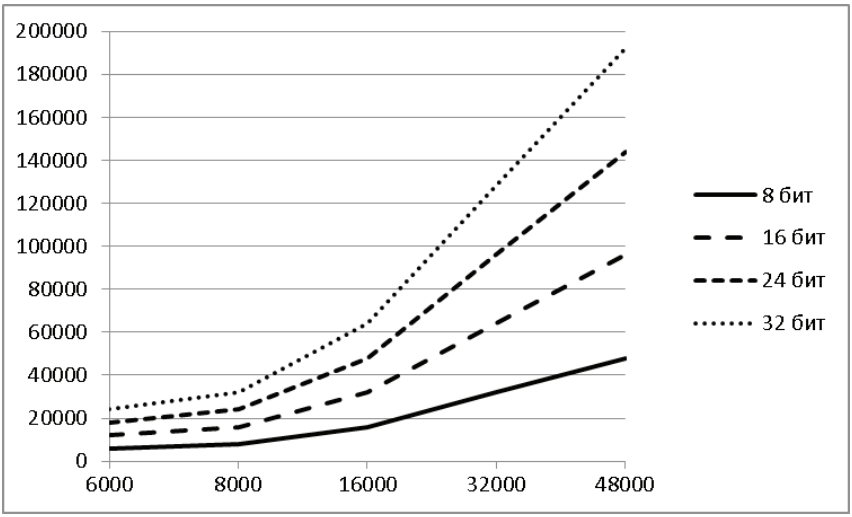


Рис. 1. График зависимости размера односекундной записи от частоты дискретизации для различных значений глубины звучания

мации об особенностях пользователей;

– количество вычисляемых коэффициентов ограничивается разработчиком системы, что позволяет масштабировать объем анализируемых данных.

На вход алгоритма подается последовательность отсчетов участка сигнала (фреймов), исследуемого на данной итерации, x_0, ... , x_{N-1}. К данной последовательности применяется весовая функция и затем дискретное преобразование Фурье. Весовая функция используется для уменьшения искажений в Фурье-анализе, вызванных конечностью выборки. На практике в качестве весовой функции обычно используется окно Хэмминга, которое имеет вид, отраженный в формуле 1.

$$w_n = 0,54 - 0,46 \times \cos\left(2\pi \frac{n}{N-1}\right), \qquad (1)$$

где n = 0, ... , N – 1, N — длина фрейма, выраженная в отсчетах. На рисунке 2 показано графическое представление спектра сигнала, полученного с использованием окна Хемминга.

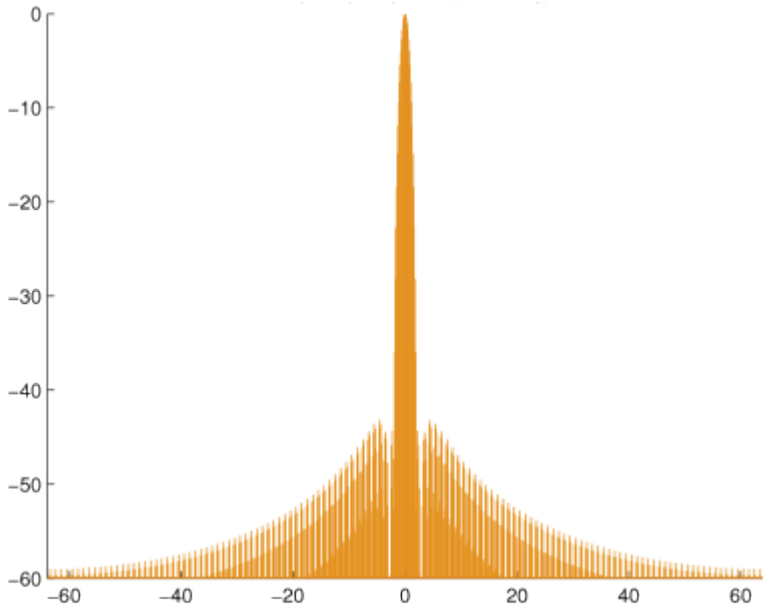


Рис. 2. Графическое представление спектра сигнала, полученного с использованием окна Хемминга

Тогда дискретное преобразование Фурье взвешенного сигнала можно записать в виде формулы (2).

$$X_k = \sum_{n=0}^{N-1} x_n w_n e^{\frac{-2\pi i}{N} kn}, \qquad (2)$$

где $k = 0, \ldots, N-1$, причем X_k – зависимость магнитуды сигнала от его частоты, такое представление ДПФ и называется оконным преобразованием Фурье.

Полученное представление сигнала в частотной области разбивают на диапазоны с помощью банка (гребенки) треугольных фильтров. Количество фильтров рекомендуется подбирать равным выбранному количеству мел-частотных кепстральных коэффициентов. Границы фильтров рассчитывают в шкале мел.

Перевод в мел-частотную область осуществляют по формуле (3).

$$B(f) = 1127 \times \ln\left(1 + \frac{f}{700}\right). \qquad (3)$$

Тогда, $B^{-1}(b) = 700(e^{\frac{b}{1127}} - 1)$ – обратное преобразование.

Пусть N_{FB} – количество фильтров, (f_{low}, f_{high}) – исследуемый диапазон частот. Тогда данный диапазон переводят в шкалу мел, разбивают на N_{FB} равномерно распределенных перекрывающихся диапазонов и вычисляют соответствующие границы в области линейных частот. Чтобы наложить полученную шкалу на спектр сигнала, необходимо использовать пропорцию (формула (4)).

$$f(j) = \left[\frac{F_d}{N} j \right], \tag{4}$$

где F_d – частота дискретизации, j = 0, ... , $N/2$.

Тогда фильтры будут иметь следующий вид (формула (5)):

$$H_m(k) = \begin{cases} 0 & k < f(m-1), \\ \dfrac{k - f(m-1)}{f(m) - f(m-1)} & f(m-1) \le k < f(m), \\ \dfrac{f(m+1) - k}{f(m+1) - f(m)} & f(m) \le k \le f(m+1), \\ 0 & k > f(m+1), \end{cases} \tag{5}$$

где m = 0, ... , N_{FB} – порядковый номер фильтра.

Фильтры применяются к энергии спектра. После применения фильтров полученные значения логарифмируются, это позволяет понизить чувствительность коэффициентов к шумам. Таким образом, промежуточные результаты будут вычисляться по формуле (6):

$$S(m) = \log\left(\sum_{k=0}^{N-1} \left| X_k \right|^2 * H_m(k) \right). \tag{6}$$

Заключительным этапом в вычислении MFCC-коэффициентов является дискретное косинусное преобразование (формула (7)).

$$c(i) = \sum_{m=0}^{N_{FB}-1} S(m) \cos\left(\frac{\pi i \left(m + \frac{1}{2} \right)}{N_{FB}} \right), \tag{7}$$

где i = 0, ... , N_{FB}– порядковый номер MFCC-коэффициента.

Коэффициент $c(0)$ обычно не используется, так как представляет собой энергию сигнала.

Создание карты пользователя состоит из выработки следующего набора данных.

– Уникальный идентификатор пользователя.
– Длина, частота дискретизации и глубина звучания очищенной записи. В случае использования одинакового оборудования с общими параметрами записи образца во время регистрации пользователя и процедуры аутентификации частота дискретизации и глубина звучания будут общими для всей системы.
– Набор мел-частотных кепстральных коэффициентов для фрейма, равного по длине всей очищенной записи. Такое решение позволяет сравнить акустические параметры пароля, это, во-первых, не требует применения алгоритмов распознавания речи для сравнения паролей, а во-вторых, дает нам возможность судить об общем совпадении манеры произношения пароля.
– Массив наборов мел-частотных кепстральных коэффициентов для фреймов заданной длины с половинным перекрытием.

Для проведения процедуры аутентификации пользователь вводит свой идентификатор и произносит парольную фразу. По идентификатору из базы данных извлекается карта пользователя.

Для полученной записи от начала последовательно со сдвигом на одно значение вправо производится расчет мел-частотных кепстральных коэффициентов для фреймов. После расчета каждого набора коэффициентов производится сравнение расстояния между полученными значениями и значениями первого набора коэффициентов из карты пользователя до нахождения его первого минимума (последующие минимумы в общем случае могут обозначать начало второго слова). Аналогичным образом находится конец записи.

Далее происходит обрезка дорожки по полученным значениям, расчет набора MFCC для всей записи и его сравнение с набором из карты пользователя.

Проводится сравнение длины полученной после обрезки записи со значением из карты пользователя, исходя из отношения длин выбирается степень перекрытия фреймов для расчета массива наборов MFCC (при разнице длин, равной половине значения из карты пользователя, рекомендуется запросить повторный ввод образца голоса, данное событие может сигнализировать о нахождение пользователя в состоянии стресса, наркотического или алкогольного опьянения и о прочих отклонениях от адекватного поведения).

Набор MFCC можно рассматривать как координаты точки в пространстве, тогда для сравнения двух фреймов достаточно

рассчитать расстояние между двумя наборами коэффициентов. Для этого воспользуемся формулой (8).

$$d = \sqrt{\sum_{n=1}^{N_{FB}} \left(mfcc_1(n) - mfcc_2(n) \right)^2} , \quad (8)$$

где $mfcc_1(n)$ – коэффициент с порядковым номером n, принадлежащий набору i.

Следующим этапом сравнения полученной записи с картой пользователя является последовательный расчет MFCC и нахождение ближайших наборов для всех наборов из карты, сравнение относительного положения наиболее близких пар.

Если расстояние между двумя наборами MFCC меньше заданного коэффициента (учет погрешности), фреймы можно считать равными. Сравнение относительного положения происходит с погрешностью на половину среднего арифметического от значений перекрытия фреймов (половинное перекрытие при расчете наборов коэффициентов для карты).

Вывод о подлинности производится на основании сравнения отношения количества совпавших по относительному положению фреймов к их общему количеству с выбранным пороговым значением.

Таким образом, алгоритм работы можно разбить на две части: создание карты пользователя и процедура аутентификации.

Создание карты пользователя:

– запись парольной фразы;
– очистка записи от отрезков, не несущих полезной информации;
– расчет и сохранение общих частотных характеристик парольной фразы на основе выработки общего набора MFCC;
– расчет и сохранение наборов MFCC для фреймов;
– присваивание уникального идентификатора выработанной карте.

Процедура аутентификации:

– считывание идентификатора пользователя;
– запись образца парольной фразы;
– открытие карты пользователя;
– нахождение начала и конца парольной фразы на основании данных из карты. В случае неудачи при проведении процедуры производится отказ от предоставления доступа;
– производится очистка записи с целью выборки отрезка, предположительно содержащего парольную фразу;
– расчет общих частотных характеристик проверяемого отрезка образца и сравнение с данными из карты пользователя. При пре-

вышении контрольного значения производится отказ от предоставления доступа;
- поиск схожих фреймов и расчет их относительного положения;
- расчет процента найденных, схожих по значению и относительному положению, фреймов. Сравнение с пороговым значением предоставления прав доступа. При недостижении порогового значения производится отказ от предоставления доступа;
- предоставление прав доступа пользователю.

В основу разработанного прототипа программной реализации были положены следующие параметры:

1) исследуемый диапазон принят за 32–16 000 Гц;
2) все записи производятся с частотой дискретизации 32 000 Гц и глубиной звучания 32 бита. Такая частота дискретизации позволяет по теореме Котельникова восстановить без искажений основной диапазон частот речи для анализируемой записи. Глубина звука выбирается исходя из условий задачи, для проверки модели оптимально использовать максимально доступное значение. Такой шаг увеличит точность расчета наборов MFCC;
3) длина фрейма выбирается меньшей или равной половине значения $sl = \frac{60}{t * s}$, где sl – средняя длительность звука, t – средний темп речи (слов в минуту), s – среднее количество звуков в слове. Для русского языка соответственно: sl =70 мс. Таким образом, длина фрейма при данных условиях не должна превышать 1129 семплов, выберем ее равной 1024 семпла;
4) в расчетах MFCC используется 24 фильтра.

Для проверки корректности предложенного метода были проведены следующие эксперименты с разной длиной записи (525–812 мс):

1) проведение процедуры аутентификации пользователя;
2) симуляция атаки на процедуру аутентификации (нарушитель знает пароль пользователя);
3) симуляция ошибки пользователя в парольной фразе;
4) симуляция атаки на процедуру аутентификации (нарушитель не знает пароль пользователя).

С целью оптимизации сравнения записей в случаях, когда обнаруживалось, что процент совпадения записей меньше пятидесяти одного, дальнейшее сравнение и расчет точного значения процента совпадения не проводились.

Во время экспериментов было обнаружено, что суждение об общей правильности произнесенной парольной фразы на основе вычисления расстояния между наборами MFCC для двух полных записей не обладает достаточной точностью. По этой причине от данной проверки пришлось отказаться.

Также с помощью экспериментов 3 и 4 было выяснено, что при выполнении условий достаточности различия действительного и произнесенного экземпляра пароля, а также корректного выбора порогового значения процента совпадения записей, ошибок при выполнении процедуры аутентификации выявлено не было. Стоит заметить, что необходимая степень различия для данного исхода не выявлялась.

При проведении экспериментов с образцами женских голосов был определен чрезмерный рост вероятности ошибки первого рода, природа данного явления содержится в особенности конкретных мел-частотных фильтров, определяющих бóльшую точность расчета MFCC в низких частотах.

В таблице представлены вероятности ошибок первого и второго рода при различных выборках участников и пороговых значениях процента совпадения записей.

Таблица

Вероятности ошибок первого и второго рода (в %)

Выборка	Пороговое значение	Вероятность ошибки I рода	Вероятность ошибки II рода
Все	55	36.(66)	2.(27)
	51	30	11.(36)
Без женских голосов	55	16.(66)	0
	51	16.(66)	8.(33)

На точность процедуры аутентификации пользователя по голосу с помощью приведенной выше модели системы аутентификации в большей степени влияют следующие факторы:

– длина парольной фразы;
– частотный состав звуков, составляющих парольную фразу.

Как показали эксперименты, точность распознавания диктора зависит, прежде всего, от длины парольной фразы и работы артикуляционных органов во время произношения парольной фразы. Для уменьшения влияния данных факторов при выработке карты пользователя следует использовать методы нейронных сетей и

машинного обучения. Также в карты пользователя следует внести диапазон анализируемых частот с учетом ограничений, рассчитанных на основании пола пользователя.

Для учета различий между программно-аппаратными средствами при записи проверочной информации и проведении процедуры аутентификации авторами рекомендуется применение методов «компенсации канала».

Примечания

[1] *Островский А.А., Жариков Д.Н., Лукьянов В.С., Попов Д.С.* Динамические методы биометрической аутентификации // Известия Волгоградского государственного университета. 2010. Т. 6.

[2] *Рамишвили Г.С.* Автоматическое опознавание говорящего по голосу. М.: Радио и связь, 1981.

[3] *Кедрова Г., Анисимов Н., Захаров Л.* Сопоставительное МРТ-исследование артикуляционных моделей гласных звуков в разных языках // Вестник Московского государственного лингвистического университета. Серия «Языкознание». 2012. Т. 13.

[4] *Сорокин В.Н., Вьюгин В.В., Тананыкин А.А.* Распознавание личности по голосу: Аналитический обзор // Информационные процессы. 2012. Т. 12.

Я.П. Башуев, В.Р. Григорьев

Методы деанонимизации в социальных сетях

Работа посвящена исследованию важнейшего направления анализа социальных сетей – разработке методов деанонимизации акторов этих сетей. Целью работы является проведение сравнительного анализа существующих методов и моделей деанонимизации пользователей и разработка модифицированного алгоритма деанонимизации на основе предложенной методики объединения вершин социального графа. Показано, что использование процедуры объединений вершин в графе позволяет осуществить эффективное разделение задачи на эквивалентные подзадачи и тем самым добиться резкого сокращения размерности проводимых вычислений.

Ключевые слова: социальные сети, деанонимизация скрытых пользователей.

Введение

В последние 15 лет происходит беспрецедентный рост информационно-коммуникационных технологий, и в первую очередь социальных сервисов сети Интернет. Плотность пользователей Интернета увеличилась почти в семь раз в период с 2000 до 2015 г. – с 6,5 до 43 процентов мирового населения[1]. Россия в настоящее время занимает 3-е место по объему генерируемого трафика в мире после США и Великобритании[2].

Важнейшей составляющей всего информационного пространства сети Интернет являются социальные сети (СС). По данным компании SimilarWeb, популярные социальные сервисы, такие как Facebook, VK и Google+, занимают лидирующие позиции по популярности среди других веб-сервисов[3]. На рис. 1 представлены данные по развитию основных социальных сервисов, изложенные в докладе директора по технологиям ЦРУ Айра Гас Хант (Ira Gus Hunt) о своем видении роли Big Data на службе ЦРУ, а также возникающих при этом задачах и методах их решения (конференция GigaOM Structure: Data 2013, 20 марта 2013 г., Нью-Йорк)[4].

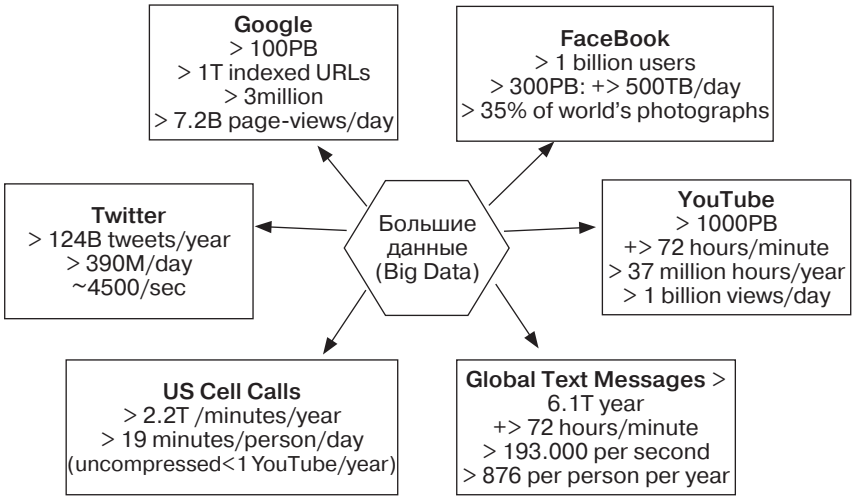


Рис. 1. Основные характеристики социальных телекоммуникаций, составляющих основу «больших данных» (Big Data)

Социальные сети предоставляют своим акторам технологическую платформу для общения и обмена информацией. Пользователи социальных сетей используют их для поиска новых знакомств, коммерческой деятельности, организации мероприятий. При этом они добровольно предоставляют провайдерам персональную информацию, например, номера мобильных телефонов, дату рождения, сообщают о своих увлечениях и интересах. Очевидно, что такая информация может собираться и использоваться сторонними приложениями для рассылки контекстной рекламы или проведения скрытых социальных исследований. В целях предотвращения использования своей персональной информации третьими лицами и недопущения их идентификации как физического лица некоторые пользователи (акторы) социальных сетей стали использовать различные методы сокрытия своего реального лица, получившие название методов анонимизации. Под анонимизацией понимается предоставление акторами СС ложных персональных данных или даже их удаление.

Однако следует особо отметить, что такого рода анонимная идентификация пользователей СС (их анонимизация) может использоваться третьей стороной для организации акций деструктивного характера, нарушающих конституционные законы стран, где они проводились. Неслучайно такого рода акции стали называть Twitter-революциями. События так называемой арабской весны в 2011 г.

(Тунис, Египет, Бахрейн, Ливия и др.)[5] и на Украине в 2013 г.[6] продемонстрировали разрушительную роль неподвластных национальной юрисдикции социальных ресурсов, которые стали инструментами организации так называемых цветных революций, которые, в свою очередь, «мягким» образом привели к реальной смене правящих в этих странах законно избранных исполнительных органов власти, т. е. попросту говоря привели к реальным переворотам в этих странах и изменению их политического курса на полностью проамериканский. Данные примеры показывают актуальность этой поставленной жизнью задачи реализации процедуры деанонимизации пользователей социальной сети.

1. Анализ существующих подходов к деанонимизации пользователей

1.1. Алгоритмы деанонимизации с использованием особенностей браузера

На настоящий момент существует несколько основных направлений реализации процедуры деанонимизации пользователей. Одним из направлений является идентификация конкретных пользователей. Обычно такие алгоритмы используют особенности браузеров в отображении информации, как, например, представлено в следующей работе[7].

Большинство социальных сетей имеют возможность объединения пользователей в группы, например, Facebook и VKontakte. Каждый пользователь $\upsilon \in V$ является членом n_υ групп, где $n_\upsilon \geq 0$. Будем представлять эту информацию в виде вектора $\Gamma(v) = (\Gamma g(v))_{g \in V}$ такого, что:

$$\Gamma g(v) = \begin{cases} 1, \text{ если } v \text{ является членом группы g} \\ 0, \text{ если } v \text{ не является членом группы g} \end{cases}$$

Историю браузера пользователя будем обозначать $ß_\upsilon$. Веббраузер содержит список страниц, которые недавно посетил пользователь. Каждый раз, когда пользователь посещает страницу ρ, ее URL Φ_ρ добавляется в $ß_\upsilon$. Необходимо учитывать, что записи устаревают. Таким образом, по истечении интервала τ URL, относящийся к странице ρ, удаляется из $ß_\upsilon$.

Предполагается, что существует возможность определить, какие страницы из заданного набора пользователь υ посетил. Таким

образом, нарушитель может вычислить для заданного пользователя υ функцию $\sigma_\upsilon(\Phi_\rho)$, которая определена следующим образом.

$$\sigma_\nu\left(\Phi_\rho\right)=\begin{cases}1, \text{ если } \Phi_\rho \in \beta_\nu \\ 0, \text{ если } \Phi_\rho \notin \beta_\nu\end{cases}.$$

Второе предположение заключается в том, что злоумышленник может получить информацию о членах, представляющих интерес *м* групп для заданной социальной сети *S*. Хотя наличие информации о всех группах необязательно, атака, описанная в работе[8], является более эффективной при увеличении числа известных групп.

Информацию об истории браузера пользователя можно получить за счет особенностей отображения гиперссылок браузерами. В современных браузерах ссылки, которые пользователь посетил (т.е. которые находятся в истории браузера), отображаются другим цветом по сравнению с остальными ссылками[9]. С помощью javascript можно узнать, какие ссылки отображаются по-другому и тем самым вычислить функцию $\sigma_\upsilon(\Phi_\rho)$[10].

Большинство социальных сетей обладают одинаковой базовой структурой. Каждый пользователь имеет в сети профиль, который содержит информацию о нем. Взаимодействие пользователя с социальной сетью осуществляет веб-приложение. Это взаимодействие осуществляется с помощью гиперссылок. В примере, представленном на рис. 2, приведены варианты таких гиперссылок.

```
(1) http://www.facebook.com/home.php?ref=home
(2) http://www.facebook.com/ajax/profile/picture/upload.php?id=[userID]
(3) http://www.facebook.com/group.php?gid=[groupID]&v=info&ref=nf
(4) https://www.xing.com/net/[groupID]/forums
(5) http://www.amazon.com/tag/[groupID]/
(6) http://community.ebay.de/clubstart.htm?clubId=[groupID]
```

Рис. 2. Типы гиперссылок в популярных социальных сетях

Как видно из рис. 2, гиперссылки зачастую содержат информацию о пользователе или всей группе. Таким образом, используя историю браузера, можно вычислить, какие группы посещал пользователь, и получить частичный вектор.

После получения частичного вектора посещенных групп атака злоумышленника может продолжиться по одному из двух путей.

Первый способ является более медленным, но более надежным. Используя информацию о членстве в группах, генерируется список кандидатов *C* из объединения всех членов $\{u\}_k$ групп, для которых $\Gamma_k(v) = 1$, т. е. $C = \cup (u)_k$: $\Gamma_k(v) = 1$. Тогда к этому множеству

применяется базовая атака для каждого элемента множества C, т. е. используется базовая атака для определения, является ли ее цель v одним из пользователей из списка кандидатов C.

Второй способ быстрее: используется список кандидатов, состоящий из пересечения множеств всех $\{u\}_k$ для k, из которых $\Gamma_k(v) = 1$. И снова базовая атака используется для проверки: является ли один из пользователей из C целью атаки.

Для работы данного алгоритма необходимо заставить пользователя перейти по ссылке на страницу, которая соберет необходимую информацию об истории браузера. Этот факт является основным недостатком данного алгоритма. Алгоритм требует сбора большого количества информации о группах пользователей целевой социальной сети, что не всегда представляется возможным. Например, социальная сеть ВКонтакте ограничивает количество доступных запросов в секунду[11].

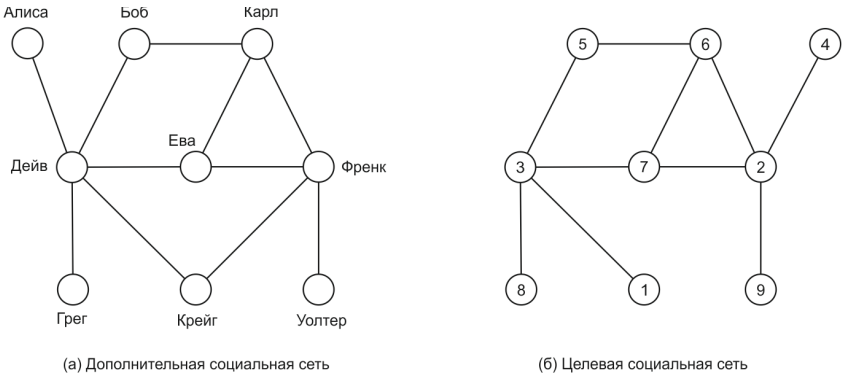
Также большим недостатком этого подхода является невысокая точность предложенного алгоритма. Результатом работы алгоритма является выявление множества пользователей, которые состоят в тех же группах, что и целевой пользователь.

1.2. Алгоритмы деанонимизации с использованием второстепенной социальной сети

В настоящее время одним из основных направлений работ по разработке моделей деанонимизации пользователей социальной сети является разработка алгоритмов, использующих дополнительные данные для идентификации отдельных пользователей, которые извлекаются исходя из анализа других социальных сетей. Данные алгоритмы позволяют провести массовую идентификацию пользователей в заданной социальной сети. Рассмотрим пример, показанный на рис. 3.

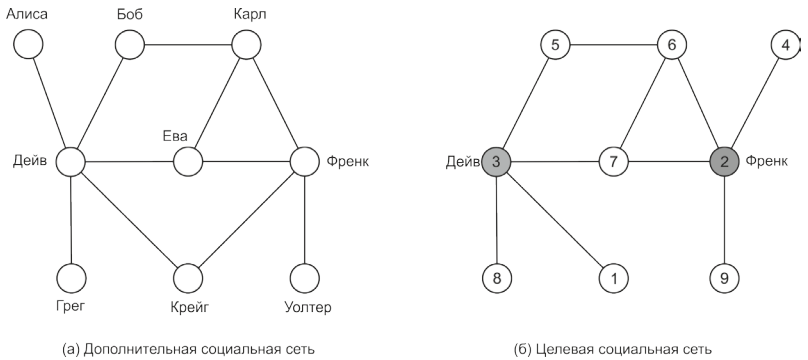
В данном примере необходимо определить имена пользователей на рис. 3б, используя доступную информацию из сети, представленной на рис. 3а. Исходя из имеющейся начальной информации, можно определить, что пользователь 2 – это, с большой вероятностью, Френк, а пользователь 3 – это Дейв, так как они имеют наибольшую степень в данном графе (рис. 4).

Исходя из новой информации, можно определить, что пользователи 6 и 7 это соответственно Карл и Ева, так как их соединения с уже известными вершинами уникальны в данном примере (рис. 5). Таким же образом можно определить, что пользователь 5 это Боб.



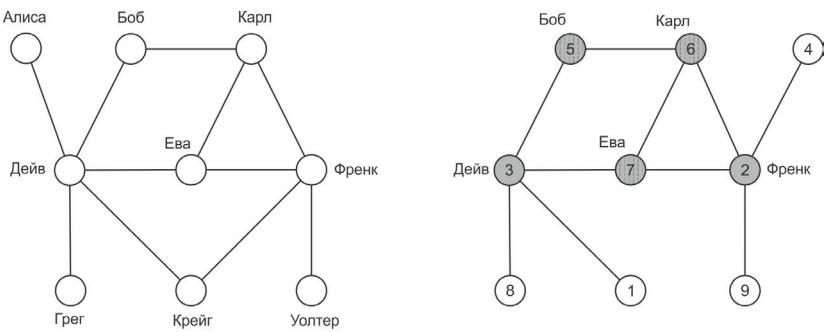
(а) Дополнительная социальная сеть (б) Целевая социальная сеть

Рис. 3. Иллюстрация доступной информации о социальных сетях в виде графов



(а) Дополнительная социальная сеть (б) Целевая социальная сеть

Рис. 4. Идентифицированные пользователи



(а) Дополнительная социальная сеть (б) Целевая социальная сеть

Рис. 5. Идентифицирован второй набор пользователей

Дальнейшая идентификация пользователей с использованием только структурных особенностей графа невозможна, так как оставшиеся вершины не имеют уникальных соединений с остальным графом. В работе[12] разработан алгоритм, который использует атрибуты вершин и ребер графа для нахождения соответствий. Подробности работы алгоритмов с дополнительными данными и модели модифицированной социальной сети рассмотрим на примере работы[13].

Графом социальной сети назовем направленный граф $G = (V, E)$, где V – множество вершин, представляющих пользователей, а E – множество ребер, представляющих отношение пользователей в социальной сети[14]. Элементы множеств V и E имеют наборы атрибутов из множеств X и Y соответственно[15].

Графом $G_{tar} = (V_{tar}, E_{tar})$ назовем граф целевой анонимной социальной сети, а графом $G_{src} = (V_{src}, E_{src})$ назовем граф дополнительной информации (граф дополнительной социальной сети). Очевидно, что для работы алгоритма необходимо, чтобы множество пользователей, представляемых вершинами графов, имело не пустое пересечение. Положим $\tilde{V}_{tar} \subseteq V_{tar}$, $\tilde{V}_{src} \subseteq V_{src}$) множества вершин, соответствующих пользователям, находящимся как в социальной сети G_{tar}, так и в G_{src}. Таким образом, алгоритм, используя входные значения (G_{tar}, G_{src}) и инициализирующее множество отображений μ_0: $V_{src} \to V_{tar}$, находит отображение μ_0: $\tilde{V}_{src} \to \tilde{V}_{tar}$, соответствующее истинному отображению μ_G.

Для определения новых отображений вершин используются различные методы задания веса каждого кандидата на отображение. Например, в работе[16] используется мера близости векторов атрибутов, присущих пользователю социальной сети. В рассматриваемом примере используются структурные свойства графа.

Для каждого отображения определяется вес, который пропорционально зависит от количества уже найденных отображений в соседних вершинах. Очевидно, что отображения, соединяющие вершины с большим количеством уже идентифицированных соседей, имеют большую вероятность оказаться правильными.

Общая схема работы алгоритма:

1. Инициализировать начальные отображения μ_0.
2. Вычислить множество всех соседей V_{nbrs} вершин, для которых отображение известно.
3. Для всех вершин $v \in V_{nbrs}$, используя заданную меру веса, определить лучшего кандидата.
4. Повторять пункты 2–3, пока не перестанут находиться новые отображения.

Эффективность работы алгоритма характеризуется мерой идентификации:

$$R(\mu) = \frac{\sum_{v \in \tilde{V}src} s(v, \mu)}{\left|\tilde{V}_{src}\right|}, \text{ где}$$

$$s(v, \mu) \begin{cases} 0, \nexists \mu(v) \\ 1, \mu(v) = \mu_G(v) \\ -1, \mu(v) = \mu_G(v) \end{cases}$$

Представленное семейство алгоритмов позволяет, при наличии входных данных, провести массовую идентификацию пользователей целевой социальной сети. Точность таких алгоритмов составляет около 75% при условии наличия достаточного количества данных[17,18].

Основными недостатками такого вида алгоритмов являются неочевидность нахождения инициализирующих отображений и их количество. Число начальных отображений, необходимых для эффективной деанонимизации, растет пропорционально размеру сети, что делает идентификацию больших графов затруднительной. Для нахождения отображения для конкретной вершины нужно сравнить атрибуты этой вершины с атрибутами каждой еще не идентифицированной вершины. Это приводит к квадратичному росту времени работы, что является большим недостатком алгоритма в целом.

1.3. Постановка задачи

Как было показано выше, существующие алгоритмы массовой деанонимизации обладают рядом недостатков, которые сильно ухудшают работу этих алгоритмов при больших размерах социальных сетей. На основе анализа существующих алгоритмов были сформулированы следующие задачи:

– создать алгоритм, позволяющий упростить процедуру деанонимизации больших графов социальных сетей;
– улучшить с помощью этого алгоритма существующие подходы к решению задачи деанонимизации;
– создать программное обеспечение, демонстрирующее возможности предложенного подхода.

2. Модель алгоритма деанонимизации пользователей на основе алгоритма построения объединений вершин

Как было показано в предыдущем разделе, существующие алгоритмы деанонимизации используют известные заранее отображения между двумя социальными сетями для расширения известных фрагментов сети на основе сравнения локальных свойств (например, количество и атрибуты идентифицированных соседей) вершин каждого графа. Такие методы требуют большого количества начальных отображений и неустойчивы к большому количеству отличий (например, вершины и ребра, которые есть в одном графе и которых нет в другом). Также с ростом масштаба сети локальные структурные свойства графа дублируются все чаще, делая задачу построения отображений на основе локальных свойств невыполнимой.

В данной работе предлагается модифицированный метод деанонимизации на основе выполнения алгоритма объединения выделенных вершин для дефрагментации постановочной задачи деанонимизации на меньшие подзадачи, решение которых возможно с помощью уже существующих методов деанонимизации.

2.1. Необходимые определения

В целях построения модифицированного алгоритма деанонимизации скрытых пользователей социальных сетей введем следующие определения.

Определение 1. Графом социальной сети назовем ненаправленный граф $G = (V, E)$, где V – множество вершин, представляющих пользователей, а E – множество ребер, представляющих отношение пользователей в социальной сети[19].

Определение 2. Объединением вершин будем называть множество сильно связанных между собой вершин, с минимальным количеством связей с вершинами вне множества[20].

Определение 3. Структурой объединений графа G называется множество $C = \{c_1, c_2, \ldots, c_k\}$, где c_i – объединение вершин, $c_i \neq \emptyset$ и $c_i \cap c_j = \emptyset \ \forall i \neq j, \ i, j \in \overline{1, k}$.

2.2. Алгоритм построения объединений вершин

Для построения объединений вершин графа связей социальной сети в данной работе за основу взят алгоритм InfoMap[21]. Данный алгоритм позволяет быстро найти объединения вершин с высоким качеством разбиения.

Качество разбиения, которое получается при применении таких алгоритмов, измеряется мерой модулярности. Модулярность разбиения – это скалярная величина, лежащая между –1 и 1, которая измеряет плотность соединений внутри множеств разбиения в сравнении с соединениями между множествами разбиения. Также эта мера используется для построения алгоритмов разбиений.

В случае взвешенного графа модулярность определяется формулой:

$$Q = \frac{1}{2m}\sum_{i,j}\left[A_{ij} - \frac{k_i k_j}{2m}\right]\delta(c_i, c_j),$$

где A_{ij} – вес ребра между i и j, $k_i = \sum_j A_{ij}$, сумма весов ребер инцидентных i, c_i – объединение, к которому принадлежит i, функция $\delta(u, v) = 1$, если $u = v$ и 0 в других случаях и $m = \frac{1}{2}\sum_{i,j} A_{ij}$.

Алгоритм разделен на два этапа, повторяющихся итеративно. При подготовке к работе алгоритма каждую вершину графа определяют в отдельное объединение, т. е. перед началом работы алгоритма количество объединений равно количеству вершин.

На первом этапе работы алгоритма для каждой вершины i рассматриваются соседи j вершины i и вычисляется изменение модулярности, которое произойдет, если вершину i добавить в объединение, содержащее вершину j. После этого вершина i добавляется в объединение с максимальным изменением модулярности, но только если изменение положительно. Первый этап заканчивается, когда достигнут локальный максимум модулярности, т. е. ни одно перемещение вершины не может дать положительное изменение модулярности. Изменение модулярности ΔQ при переносе вершины i в объединение C для первого этапа легко вычисляется по формуле

$$\Delta Q = \left[\frac{\left(\Sigma_{in} + k_{i,in}\right)}{2m} - \left(\frac{\Sigma_{tot} + k_i}{2m}\right)^2\right] - \left[\frac{\Sigma_{in}}{2m} - \left(\frac{\Sigma_{tot}}{2m}\right)^2 - \left(\frac{k_i}{2m}\right)^2\right],$$

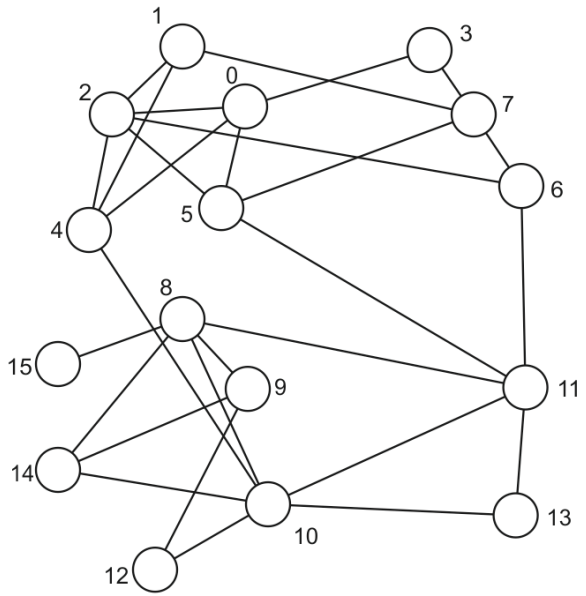


Рис. 6. Граф, в котором нужно выделить объединения

где $\sum_{in}$ – сумма весов ребер внутри C, $\sum_{tot}$ – сумма весов ребер, инцидентных вершинам в C, k_i – сумма весов ребер, инцидентных вершине i, $k_{i,\ in}$ – сумма весов ребер, идущих от i до вершин в C, m – сумма всех весов в графе.

Второй этап алгоритма заключается в построении нового графа, состоящего из вершин, представляющих объединения, найденные на первом этапе. Для этого веса ребер между новыми вершинами задаются суммой весов ребер между вершинами двух объединений. После завершения второго этапа к новому графу можно снова применить данный алгоритм. Эти действия проводятся до тех пор, пока не прекратятся изменения и не будет достигнут максимум модулярности.

Рассмотрим работу алгоритма на примере графа, изображенного на рис. 6.

На первой стадии алгоритма вершины будут распределены по объединениям. Из рисунка видно, что всего объединений 4 (на рис. 7 они окрашены разными цветами).

К графу, изображенному на рисунке 7, применяется второй этап алгоритма, в результате получается второй граф, вершинами которого являются объединения, полученные на первом этапе.

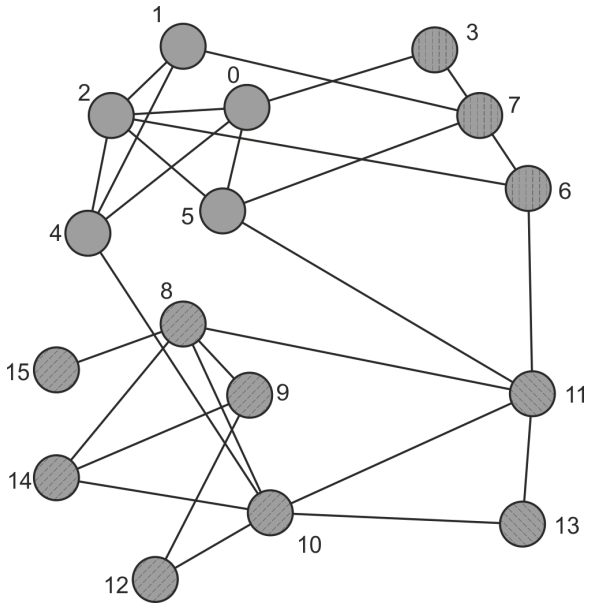


Рис. 7. Граф после первого этапа алгоритма

После первой итерации алгоритма получилось 4 объединения, два из которых имеют значительно меньший вес. Поэтому при применении алгоритма во второй раз останется два объединения большого веса (рис. 9).

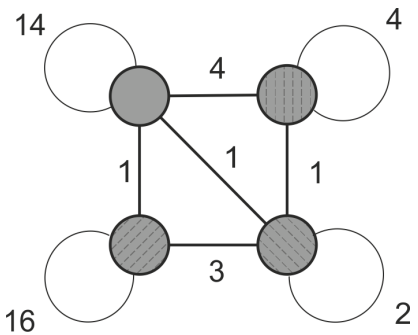


Рис. 8. Результат работы второго этапа реализации алгоритма

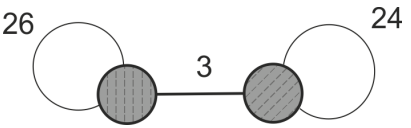


Рис. 9. Вторая итерация алгоритма

2.3. Алгоритм деанонимизации сети на основе реализации процедуры построения объединений

Основным преимуществом использования объединений в графе является эффективное разделение задачи на эквивалентные подзадачи. После применения алгоритма из параграфа 2.2 к имеющимся графам возможно построить отображения объединений между двумя графами и затем начать строить отображения между вершинами графов в каждом отдельно взятом объединении. Для этого процесса возможно также применять существующие алгоритмы деанонимизации[22]. Рисунки 10–14 иллюстрируют последовательность выполнения этапов работы предложенного алгоритма.

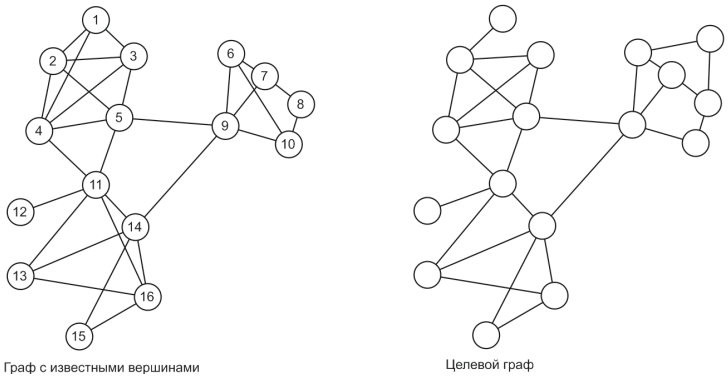


Рис. 10. Начальное состояние графов

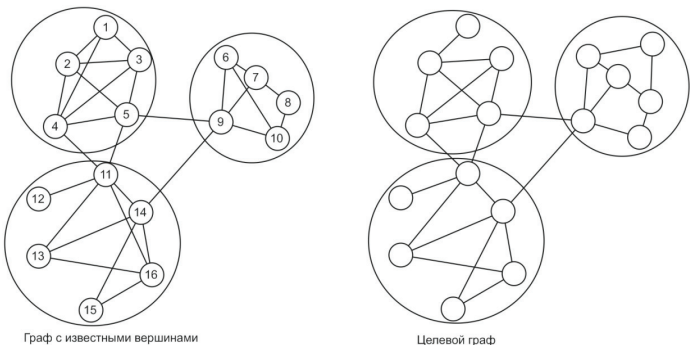


Рис. 11. Построение объединений в графах

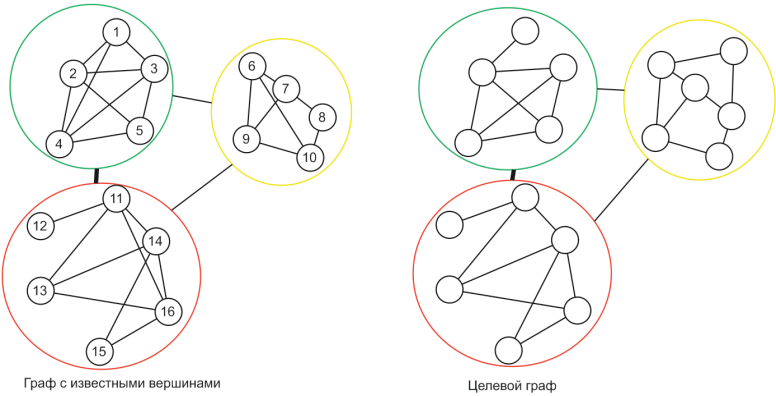


Рис. 12. Построение отображений между графами

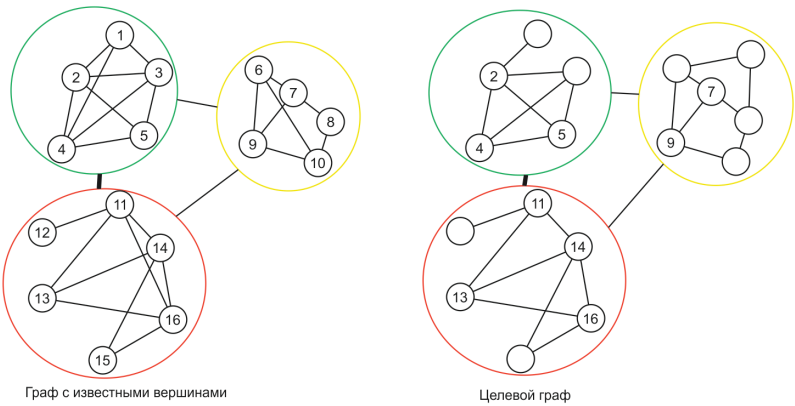


Рис. 13. Идентификация вершин в объединениях

Таким образом, предложенный модифицированный алгоритм состоит из четырех этапов.

1. Построение объединений с помощью InfoMap алгоритма.
2. Нахождение совпадающих пар объединений.
3. Локальная идентификация вершин в отдельных объединениях.
4. Применение алгоритма деанонимизации, не зависящего от числа объединений.

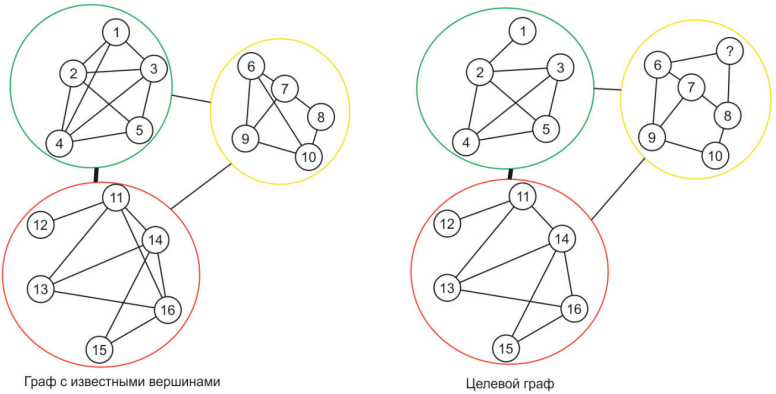


Рис. 14. Результат применения алгоритма деанонимизации

2.4. Отображения объединений

После применения к графам рассматриваемых СС алгоритма InfoMap, необходимо идентифицировать начальные отображения вершин. Затем объединения, которым принадлежат данные вершины, можно отобразить друг в друга. В результате этого процесса могут возникать конфликты, так как вершины в дополнительном графе могут принадлежать разным объединениям, а в основном одному объединению. Для разрешения конфликта идентификации объединения достаточно подсчитать количество идентифицированных вершин для каждого кандидата-объединения и выбрать то, для которого количество вершин максимально.

После того как некоторое количество объединений идентифицировано, строятся высокоуровневые графы объединений. Вершинами данных графов являются объединения, ребрами будут ребра между вершинами, принадлежащими разным объединениям и весом ребер будет количество соединений из одного объединения в другое. Пример построения таких графов показан на рисунках 8 и 9.

К полученным графам применяется модифицированный NS-алгоритм. Графы, полученные из целевой и дополнительной сети, будем обозначать G_1^* и G_2^* соответственно. Множество известных пар вершин будем обозначать M^*.

Как и в оригинальном NS-алгоритме, на каждом шаге алгоритма случайным образом выбирается вершина μ^* из множества сосе-

дей вершин, принадлежащих M^*. Затем для каждой вершины-кандидата из целевого графа вычисляется мера похожести:

$$S(\mu^*, v^*) = \frac{\Sigma(p^*, q^*) \in N(\mu^*, v^*)\left(1 - \left|\sqrt{\omega(\mu^*, \rho^*)} - \sqrt{\omega(q^*, v^*)}\right|\right)}{\sqrt{d(\mu^*)d(v^*)}},$$

где $N(\mu^*, \nu^*)$ – множество идентифицированных соседей вершин μ^* и υ^*, $\omega(\mu^*, \rho^*)$ – вес ребра между вершинами μ^* и ρ^*, $d(\mu^*)$ – степень вершины.

2.5. Локальная идентификация вершин

Полученные в параграфе 2.4 отображения между объединениями позволяют идентифицировать дополнительные вершины с помощью принципа «разделяй и властвуй». Для каждой пары сопоставленных объединений C_1 и C_2 будем рассматривать два подграфа G_{C1} и G_{C2}, содержащих в себе вершины, принадлежащие соответствующим объединениям, и ребра, инцидентные им. Мощность множеств вершин данных графов существенно меньше основного графа, поэтому для каждой вершины можно вычислить локальный коэффициент кластеризации.

Коэффициент кластеризации вершины υ_i определяет, насколько подграф, содержащий эту вершину и все k_i ее соседей, близок к полноте. Коэффициент можно выразить формулой

$$C_{vi} = \frac{2\left|\left(e_{jk} : v_j,\ v_k \in N_i,\ e_{jk} \in E\right)\right|}{k_i(k_i - 1)}$$

Данный параметр и степень вершины можно использовать для попарного сравнения вершин графов G_{C1} и G_{C2} для нахождения отображений. Для сравнения по этим двум параметрам будем использовать две меры близости:

$$D_d(v_i, v_j) = \frac{\left|d(v_i) - d(v_j)\right|}{\max\left(d(v_i), d(v_j)\right)},$$

$$D_{cc}(v_i, v_j) = \frac{\left|C_{v_i} - C_{v_j}\right|}{\max\left(C_{v_i}, C_{v_j}\right)}.$$

Пары вершин, для которых данные меры близки к 1, будем считать вершинами, принадлежащими одному пользователю. Таким образом, будет сопоставлено еще большее количество вершин и, тем самым, будет улучшен результат последнего этапа работы алгоритма.

2.6. Глобальная идентификация вершин

В результате выполнения предыдущих этапов предложенного алгоритма мы получили большое количество отображений из дополнительного графа в целевой. Используя эти отображения в качестве начальных, мы применяем глобальный алгоритм деанонимизации к имеющимся двум графам. В качестве меры похожести для данного этапа будем использовать похожесть идентифицированных соседей. Данный подход в совокупности с большим количеством известных отображений дает простую и быструю меру для получения новых пар[23].

Обозначим целевой анонимный граф как $G_1 = (V_1, E_1)$, а граф дополнительной информации как $G_2 = (V_2, E_2)$. Для каждой вершины u графа G_1 зададим множество $G_m^1(u)$ – множество всех соседей u, для которых найдено отображение в графе G_2. Аналогично для каждой вершины v графа G_2 зададим множество $G_m^2(u)$ – множество всех соседей v, для которых найдено отображение в графе G_1.

Обозначим множество идентифицированных вершин графа как $G_1 : V_S^*, \subseteq V_2$, вершины множества V_S имеют отображения в аналогичное множество графа $G_2 : V_S^* \subseteq V_2$. Определим операцию над этими множествами:

$$N_m^1(u) - N_m^2(v) = N_m^1(u) \setminus \left\{ u_i \in N_m^1(u) : u_i \to v_i \in V_s^*,\ v_i \in N_m^2(v) \right\}.$$

Т. е. операция является разностью множеств с учетом отображения между V_S и V_S^*. С помощью заданной операции можно определить меры различия окрестностей двух вершин[24]:

$$\Delta_1(u,v) = \frac{\left| N_m^1(u) - N_m^2(v) \right|}{\left| N_m^2(u) \right|},$$

$$\Delta_2(u,v) = \frac{\left| N_m^2(u) - N_m^1(v) \right|}{\left| N_m^2(u) \right|}.$$

Полученные меры принадлежат отрезку [0, 1] и равны нулю, если окрестности совпадают. Построим таблицу с количеством строк, равным количеству вершин без пары с соседями в V_i в графе G_1 и с количеством столбцов, равным аналогично количеству вершин без пары с соседями в V_S^* в графе G_2. На пересечении столбца u_i со строкой v_j будет стоять кортеж $(\Delta_1(u_i, v_j), \Delta_2(u_i, v_j))$.

Таблица

Построение таблицы из мер различия окрестностей двух вершин анонимного и дополнительного графов

Δ	u_1	u_2	...
v_1	$(\Delta_1(u_1, v_1), \Delta_2(u_1, v_1))$	$(\Delta_1(u_2, v_1), \Delta_2(u_2, v_1))$	
v_2	$(\Delta_1(u_1, v_2), \Delta_2(u_1, v_2))$	$(\Delta_1(u_2, v_2), \Delta_2(u_2, v_2))$	
...			

Для нахождения подходящего отображения значения обеих мер должны быть минимальными. Поэтому на каждом шаге алгоритма будет выбираться ячейка, для которой значения в кортеже минимальны для всех значений в той же строке и столбце. Выбранные таким образом пары считаются идентифицированными и добавляются во множества. Работа алгоритма продолжается до тех пор, пока не будут найдены все пары.

3. Описание практической части

Практическая часть данной работы была реализована на языке программирования Java 8. Использование данного языка программирования обусловлено следующими причинами:

1) работа имеет в первую очередь исследовательский характер, и никаких специальных требований по возможности интеграции в существующие решения не предъявлялось, в связи с чем выбор языков программирования определялся в основном простотой, гибкостью и скоростью разработки;
2) программы на языке Java исполняются на виртуальной машине Java, что предоставляет возможность запускаться на большинстве современных операционных систем. Также стандарт языка Java содержит в себе большое количество библиотек, что облегчает разработку.

Для работы с графами выбрана библиотека JUNG v2.0.1. Выбор данной библиотеки обусловлен следующими причинами:

1) библиотека JUNG является одной из самых быстрых библиотек по работе с графами и имеет подробную документацию;
2) в состав библиотеки входят средства для визуализации информации, содержащейся в графах;
3) структура библиотеки позволяет модифицировать стандартные возможности под нужды данной работы.

На рис. 15–18 изображены этапы работы алгоритма, предложенного в работе.

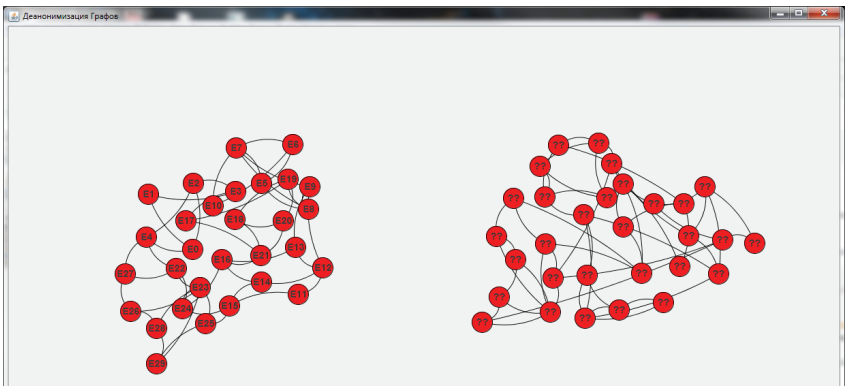


Рис. 15. Начальное состояние.
Слева – граф дополнительной информации,
справа – анонимизированный граф

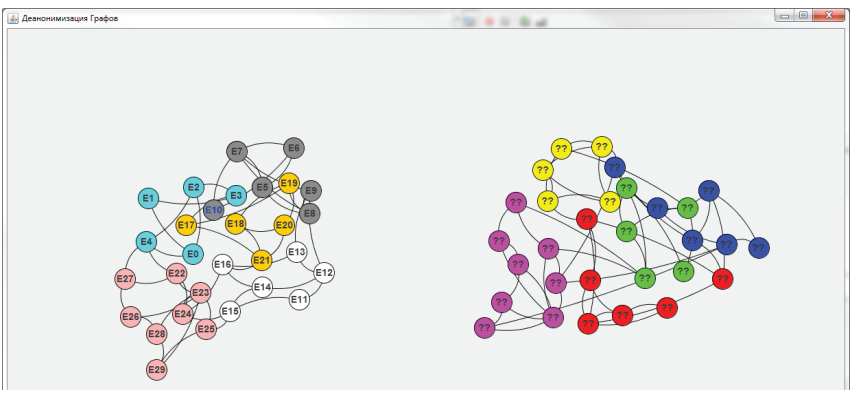


Рис. 16. Состояние программы
после выполнения алгоритма InfoMap

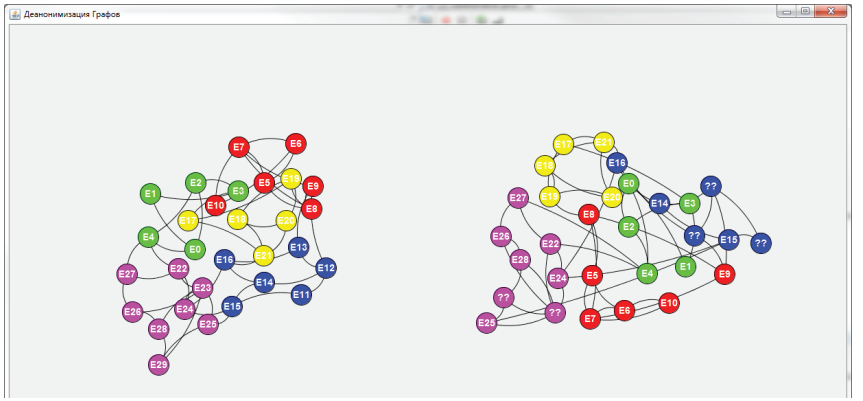


Рис. 17. Построенные отображения разбиений

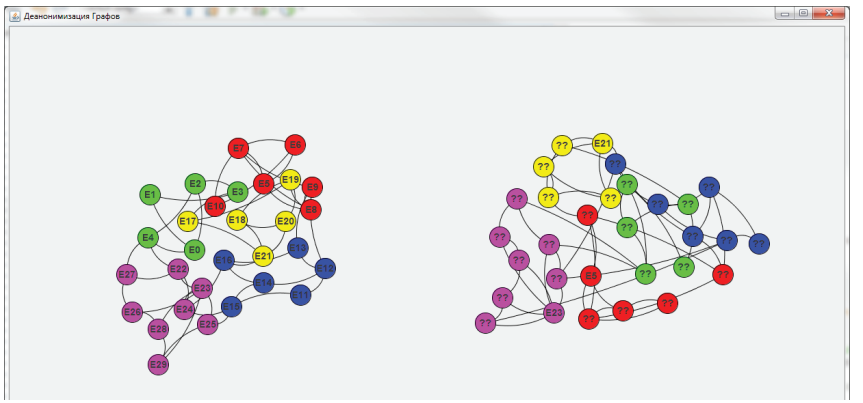


Рис. 18. Результат полной работы алгоритма

Разработанный программный модуль обладает следующими особенностями при практической реализации:

– входные данные и результаты сохраняются в распространенном формате GraphML;
– отображение результатов работы алгоритма осуществляется в графическом формате;
– реализована поддержка различных алгоритмов построения разбиений и поддержка различных методов деанонимизации пользователей социальной сети.

Заключение

В рамках данной работы были получены следующие результаты.

1. Исследованы существующие методы деанонимизации пользователей в социальных сетях.
2. Разработан алгоритм идентификации пользователей с использованием процедуры попарных разбиений.
3. Создан программный модуль, реализующий предложенный алгоритм.

Основной результат данной работы заключается в разработке нового подхода к оптимизации методов идентификации пользователей социальных сетей на основе построения алгоритма попарных разбиений. Предложенный алгоритм позволяет улучшить характеристики существующих реализаций технологии деанонимизации пользователей социальной сети, а также представляет теоретическую и практическую значимость для разработки систем моделирования информационных акций в социальных сетях.

Примечания

[1] Отчет по ИКТ Международного союза электросвязи за 2015 г. [Электронный ресурс] URL: http://www.itu.int/net/pressoffice/press_releases/2015/pdf/17-ru.pdf (дата обращения: 30.08.2016).

[2] Энциклопедия поисковых систем. [Электронный ресурс] URL: http://www.searchengines.ru/seoblog/similar_web_43_mirovogo_t.html (дата обращения: 30.08.2016).

[3] *Голицына А.* Общение заменило поиск // Ведомости. 2015. 11 сент. № 3915. [Электронный ресурс] URL: http://www.vedomosti.ru/technology/articles/2015/09/11/608342-sotsseti-i-messendzheri-oboshli-internet-poisk-i-prosmotr-saitov (дата обращения: 30.08.2016).

[4] ЦРУ – большие задачи и большие данные. На пути к созданию глобального информационного колпака. [Электронный ресурс] URL: https://habrahabr.ru/post/177433/

[5] *Стенин А.* Революция в Египте была раскручена через Facebook // РИА Новости от 12.02.2012. [Электронный ресурс] URL: http://ria.ru/world/20110212/333637995.html (дата обращения: 30.08.2016).

[6] *Алферов К.* Украинская Facebook-революция глазами очевидца // Газета.ru от 24.03.2014. [Электронный ресурс] URL: http://www.gazeta.ru/tech/2014/03/21_e_5959229.shtml (дата обращения: 30.08.2016).

[7] *Wondracek G., Holz T., Kirda E., Kruegel C.* A Practical Attack to De-anonymize Social Network Users: Technical Report TR-iSecLab-0110-001 (2013).

[8] Ibid.

[9] W3C Recommendation. CSS Reference. [Электронный ресурс] URL: http://www.w3.org/TR/CSS21/selector.html%23id-selectors (дата обращения: 30.08.2016).

[10] *Wondracek G., Holz T., Kirda E., Kruegel C.* Op. cit.

[11] Выполнение запросов к API ВКонтакте. [Электронный ресурс] URL: https://vk.com/dev/api_requests (дата обращения: 30.08.2016).

[12] *Narayanan A., Shmatikov V.* De-anonymizing social networks // IEEE Symposium on Security and Privacy. 2009. P. 173–187.

[13] *Simon B., Gulyás G., Imre S.* Analysis of Grasshopper, a Novel Social Network De-anonymization Algotithm // Periodica Polytechnica: Electrical Engineering and Computer Science. 2014. Vol. 58. No. 4. P. 161–173.

[14] Ibid.

[15] *Narayanan A., Shmatikov V.* Op. cit.

[16] Ibid.

[17] *Simon B., Gulyás G., Imre S.* Op. cit.

[18] *Narayanan. A., Shmatikov V.* Op. cit.

[19] *Simon B., Gulyás G., Imre S.* Op. cit.

[20] *Vincent D.* Blondel, Fast unfolding of communities in large networks. 2008.

[21] Ibid.

[22] См., например: *Simon B., Gulyás G., Imre S.* Op. cit; *Narayanan A., Shmatikov V.* Op. cit.

[23] *Wei Peng, Feng Li, Xukai Zou, Jie Wu.* A Two-stage Deanonymization Attack against Anonymized Social Networks // IEEE Transactions on Computers. 2014. Vol. 63. P. 290–303; Feb. 2014, doi:10.1109/TC.2012.202.

[24] Ibid.

В.А. Кирюхин

Алгоритм построения линейных блоковых двоичных кодов по заданному числу информационных символов и числу исправляемых ошибок

В статье предложен алгоритм построения линейных блоковых двоичных кодов по заданному числу информационных символов и числу исправляемых ошибок. Дана теоретическая оценка сложности предложенного алгоритма, произведено экспериментальное исследование времени работы. На основе анализа результатов работы предложенного алгоритма был сделан вывод о том, что параметры построенных кодов совпадают с параметрами кодов, найденных полным перебором. Было произведено сравнение параметров построенных кодов с параметрами некоторых известных в литературе кодов (БЧХ, Голея), которое показало, что в большинстве случаев параметры построенных кодов не уступают известным, а в остальных случаях незначительно хуже.

Ключевые слова: помехоустойчивое кодирование, линейные коды.

Большинство процессов, связанных с накоплением, хранением и передачей информации, протекают в условиях воздействия разнообразных помех, способных исказить хранимые и обрабатываемые данные. Для противодействия помехам необходимо использовать методы, позволяющие обнаруживать и корректировать подобные ошибки. С математической точки зрения задача сводится к построению так называемых помехоустойчивых кодов.

Одним из классов помехоустойчивых кодов являются блоковые коды, делящие информацию на фрагменты постоянной длины и обрабатывающие каждый из них в отдельности. Практически все используемые блоковые коды являются линейными. Это связано с тем, что нелинейные коды значительно труднее исследовать, и для них трудно обеспечить приемлемую сложность кодирования и декодирования.

Несмотря на большое количество литературы, связанной с линейными кодами, вопрос существования кода с заранее заданными

параметрами (n, k, t) является открытым. Очевидно, что использование алгоритма полного перебора для построения линейного кода неэффективно из-за высокой вычислительной сложности. В данной статье рассмотрен алгоритм поиска оптимального, с точки зрения длины кодового слова, линейного двоичного блокового кода при заданных k и t.

Необходимые теоретические сведения

Корректирующая способность линейного блокового (n, k)-кода (n, k) зависит от минимального кодового расстояния d_{min}, определяемого как наименьшее расстояние Хемминга между всеми парами кодовых слов. Известно, что d_{min} может быть вычислено как минимальный вес ненулевого кодового слова[1].

Для того чтобы код исправлял ошибки кратности t, должно быть выполнено соотношение $d_{min} = 2t + 1$.

Рассмотрим границы параметров кода. Если существует код с параметрами n, k, t, то верно неравенство $2^{n-k} \geq \sum_{l=0}^{t} \binom{n}{l}$ (Верхняя граница Хемминга)[2]. С другой стороны, существует (n, k)-код с d_{min}, равным, по меньшей мере, d, параметры которого удовлетворяют неравенству $\sum_{l=0}^{d-2} \binom{n}{l} \geq 2^{n-k}$ (Нижняя граница Варшамова–Гильберта)[3]. Таким образом, имеем соотношение $\sum_{l=0}^{2t-1} \binom{n}{l} \geq 2^{n-k} \geq \sum_{l=0}^{t} \binom{n}{l}$. Отсюда, при фиксированных k и t, можем найти n_{min} и n_{max} такие, что $n \in [n_{min}, n_{max}]$.

Линейный блоковый код можно задать с помощью порождающей матрицы $G_{k \times n}$, такой, что $\vec{u}G = \vec{v}$, где $\vec{u}$ – информационное слово длины k, $\vec{v}$ – кодовое слово длины.

Каждый линейный (n, k)-код эквивалентен систематическому, т. е. может быть задан с помощью матрицы $G_{k \times n} = \left(I_k P_{k \times (n-k)}\right)$, где I_k – единичная матрица.

Полный перебор и его вычислительная сложность

Воспользуемся тем, что перебирать необходимо только систематические коды. Будем рассматривать все возможные матрицы дополнений $P_{k\times(n-k)}$, и проверять, являются ли каждые $d-1$ ее строк линейно независимыми (достаточное условие того, что d_{min} кода равно d [4]). Если для минимально возможного n ни одной такой матрицы не существует − увеличим на единицу рассматриваемый n и снова попытаемся построить требуемую матрицу. Продолжим увеличение n до тех пор, пока матрица не будет найдена.

Оценим вычислительную сложность такого алгоритма. Число двоичных векторов длины n-k равно 2^{n-1}, число матриц, составленных из таких векторов, различных с точностью до перестановки строк, равно $C^k_{2^{n-k}}$. Проверим, что каждая строка из матрицы имеет вес больше $d_{min}-1$, каждая сумма по всем возможным парам строк имеет вес больше $d_{min}-2$ и т. д. Таким образом, необходимо проверить $C^1_k + C^2_k + ... + C^{min(2t,k)}_k$ комбинаций, это число можно оценить как 2^k. Сложность суммирования двух векторов и сложность проверки веса вектора будем считать константой. Следовательно, число операций, необходимых для проверки одной матрицы $P_{k\times(n-k)}$, будет пропорционально $\sum_{i=1}^{min(2t,k)} (i-1)C^i_k$. Приблизительная оценка этой суммы − $k2^k$. В итоге получаем $O\left(k2^k \sum_{n=n_{mix}}^{n_{max}} C^k_{2^{n-k}}\right)$.

Алгоритм

Как отмечалось выше, для построения линейного блокового кода достаточно найти матрицу дополнений $P_{k\times(n-k)}$. Будем пытаться построить матрицу дополнений начиная с $n = n_{min}$.

Матрица P состоит из k векторов длины $r = n-k$. Рассмотрим множество B двоичных векторов длины r. Мощность множества B равна 2^r.

Исходя из того что все векторы в матрице P различны и того что перестановка векторов будет давать эквивалентную порожда-

ющую матрицу, будем строить матрицу дополнений следующим образом:

– пронумеруем векторы, принадлежащие множеству B. Будем отбирать только те, чей вес больше $d_{min}-1$. Выберем первый – b_1;
– выберем (из следующих за первым) второй – b_2 таким образом, чтобы вес $\omega(b_1+b_2)\geq d_{min}-2$ («+» – сложение по модулю 2);
– выберем, из следующих за вторым, третий таким образом, чтобы $\omega(b_1+b_3)\geq d_{min}-2$, $\omega(b_2+b_3)\geq d_{min}-2$ и $\omega(b_1+b_2+b_3)\geq d_{min}-3$;
– на шаге i сумма любой пары векторов должна иметь вес не меньше $d_{min}-2$, сумма любой тройки не меньше $d_{min}-3$, аналогично до комбинаций из $d_{min}-1$ векторов, вес которых должен быть ненулевым.

Если нам удалось найти по такому принципу k векторов, мы нашли код с заданными параметрами. Можем выйти из алгоритма или перейти на предыдущий шаг для поиска других кодов с такими же параметрами.

Если k векторов найти не удалось, увеличим n на единицу, создадим заново множество B. Тем самым будем рассматривать векторы, отобранные ранее, в новом пространстве с увеличенным числом измерений, считая у них нулевой координату нового измерения.

Увеличивая n мы либо построим на каком-то шаге матрицу дополнений, либо n достигнет нижней границы Варшамова–Гильберта, код с таким n удовлетворяет требуемым параметрам, следовательно, матрица будет построена.

Построенный код будет удовлетворять требуемым параметрам k и t. Для того чтобы доказать это, покажем, что вес любого ненулевого кодового слова не меньше, чем $d_{min}=2t+1$.

Рассмотрим произвольный ненулевой вектор $\vec{u}$ длины k. Если его вес больше или равен d_{min}, то кодовое слово $\vec{v}=\vec{u}G_{k\times n}=\vec{u}\left(I_k P_{k\times(n-k)}\right)$ будет, очевидно, иметь вес не меньше d_{min}, так как $\vec{u}I_k=\vec{u}$. Если вес вектора $\vec{u}$ равен $x<d_{min}$, то вес вектора $\vec{v}$ будет определяться весом суммы какого-то набора x строчек из матрицы P. Вес этой суммы векторов будет больше или равен, чем $d_{min}-x$. Таким образом, $\omega(\vec{v})=\omega(\vec{u}I_k)+\omega\left(\vec{u}I_k P_{k\times(n-k)}\right)\geq x+d_{min}-x$, $\omega(\vec{v})\geq d_{min}$. В силу того что вектор выбран произвольно, соотношение $\omega(\vec{v})\geq d_{min}$ выполнено для любого кодового слова, следовательно, построенный код действительно удовлетворяет заданным параметрам.

Оценка сложности алгоритма

Дадим оценку сверху для вычислительной сложности алгоритма. Необходимо перебрать 2^{n-k} векторов. Максимальное значение n найдем из нижней границы Варшамова–Гильберта (В.–Г.) $\sum_{l=0}^{d-2}\binom{n}{l} \geq 2^{n-k}$. (Согласно результатам экспериментов значение n ближе к верхней границе Хемминга, см. рис. 1.)

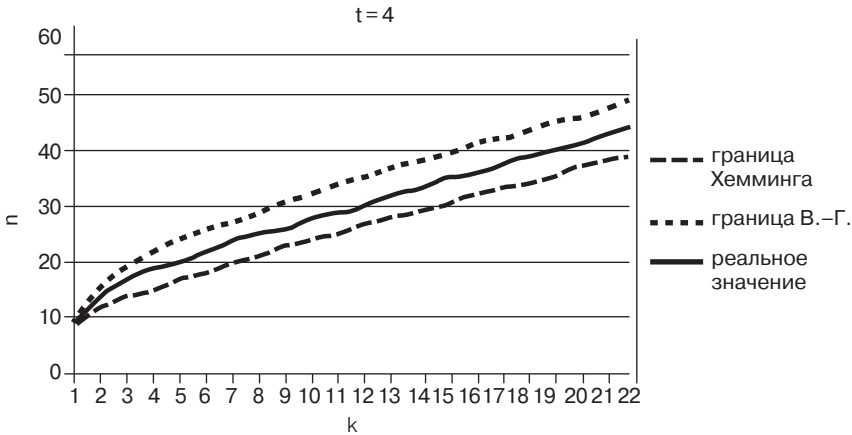


Рис. 1. Зависимость параметра n от k при $t = 4$

Для каждого рассматриваемого вектора нужно подсчитать его вес за счет использования вычисленной заранее таблицы весов и ограничения на длину вектора, время подсчета будет постоянным – $O(1)$. Если вес вектора подходит, проверим: может ли вектор принадлежать матрице дополнений? Для этого просуммируем его со всеми возможными комбинациями из уже отобранных векторов и вычислим вес полученных комбинаций. Максимальное число таких комбинаций равно $C_k^1 + C_k^2 + ... + C_k^{min(2t,k)}$, это число можно оценить как 2^k. (Естественно, число комбинаций будет принимать такое значение только к самому концу работы алгоритма.) Сложность операции сложения – $O(1)$, вычисление веса – $O(1)$. Таким образом, сложность проверки равна $O(2^k)$. Таким образом получаем, что необходимо перебрать 2^{n-k} векторов, часть из них будет отсеяна за счет проверки веса, для других надо осуществить проверку со сложностью $O(2^k)$. Вычислим число векторов в первой и во второй части. Общее число векторов 2^{n-k}, число векторов с весом, меньшим $d_{min}-1=2t$,

равно $C^0_{2^{n-k}} + C^1_{2^{n-k}} + ... + C^{2t-1}_{2^{n-k}}$. Таким образом, вычислительная сложность предложенного алгоритма – $O\left(\sum_{i=0}^{2t-1} C^i_{2^{n-k}} + 2^k \sum_{i=2t}^{k} C^i_{2^{n-k}}\right)$. Дадим оценку сверху, не учитывая отбор векторов с неподходящим весом, — $O\left(2^{n-k}2^k\right) = O\left(2^n\right)$, где $n \in \left[n_{min}, n_{max}\right]$, а n_{min} и n_{max} определяются из границ Хемминга и Варшамова–Гильберта. Нужно отметить, что при увеличении параметра t значение n становится ближе к n_{min}.

Экспериментальные результаты

Сравним скорость работы рассмотренного алгоритма и алгоритма полного перебора. Нужно отметить, что время работы алгоритма полного перебора в первую очередь зависит от того, насколько близко значение параметра n к минимальной границе. В случае если искомый код является совершенным (или близок к этому), т. е. $n = n_{min}$ и соответственно $2^{n-k} = \sum_{l=0}^{t} \binom{n}{l}$ – время алгоритма полного перебора гораздо меньше за счет отсутствия необходимости проверять огромное число вариантов с меньшими значениями n, для которых ни одного линейного кода не существует. У рассмотренного в текущей статье алгоритма такой зависимости нет. Время работы зависит только от значения n, при котором код может быть построен, а не зависит от n_{min}. В силу того что время работы алгоритма полного перебора гораздо больше, чем у предложенного алгоритма, не представляется возможным сравнивать время их работы при одинаково большом наборе параметров. Поэтому на рис. 2 и 3 график, соответствующий алгоритму полного перебора, охватывает меньше значений.

Рассмотрим график, показывающий зависимость времени работы алгоритма от заданных параметров k и t (рис. 4). Нужно сказать, что, например, при переходе от некоторых k к $k+1$ рост графика опережает рост 2^n; это объясняется тем, что рост параметра n не находится в линейной зависимости от k и t (рис. 5).

Одним из важнейших критериев сравнения алгоритмов является величина $R = \frac{k}{n}$ – скорость построенного кода. Как видно из

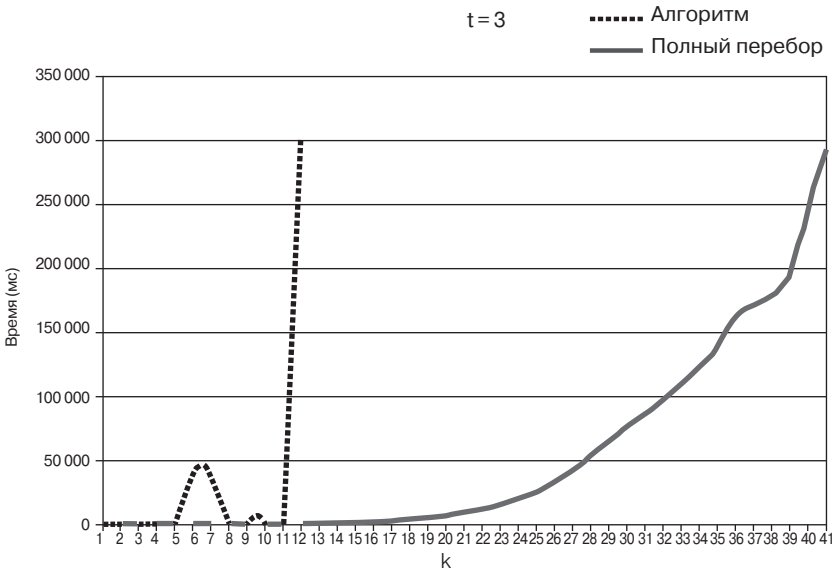


Рис. 2. Сравнение скорости работы двух алгоритмов при $t = 3$

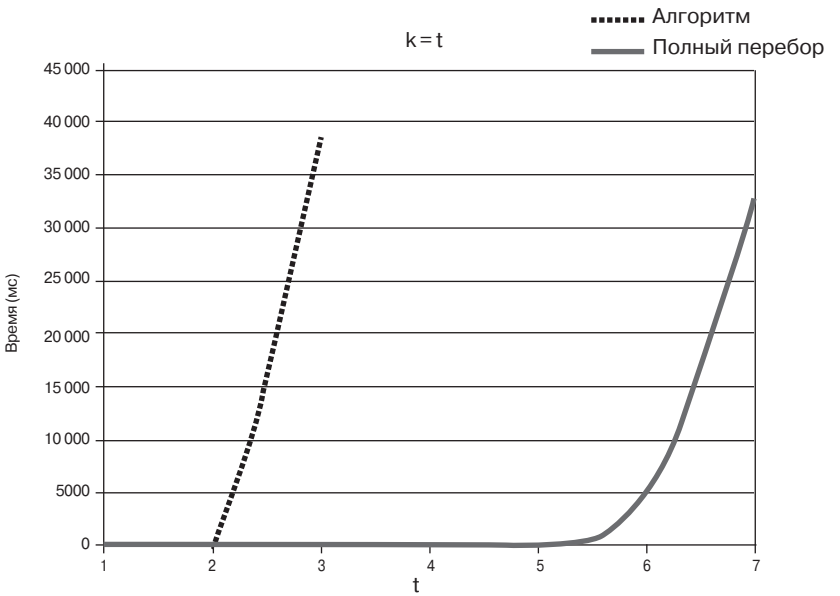


Рис. 3. Сравнение скорости работы двух алгоритмов при $k = 7$, число исправляемых ошибок $t \in [1,7]$

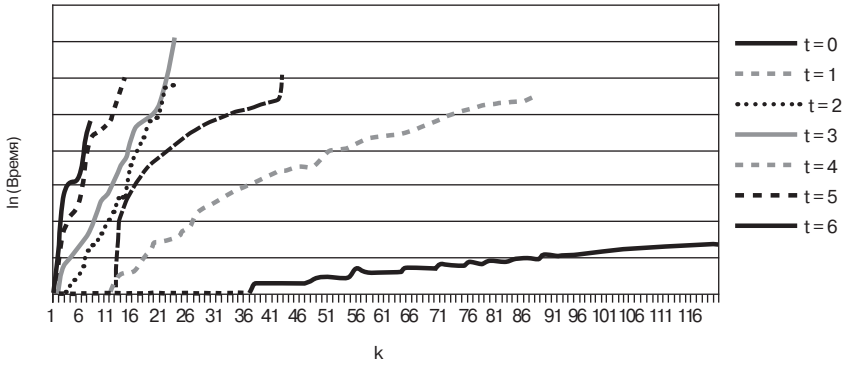


Рис. 4. Зависимость времени работы от параметров k, t

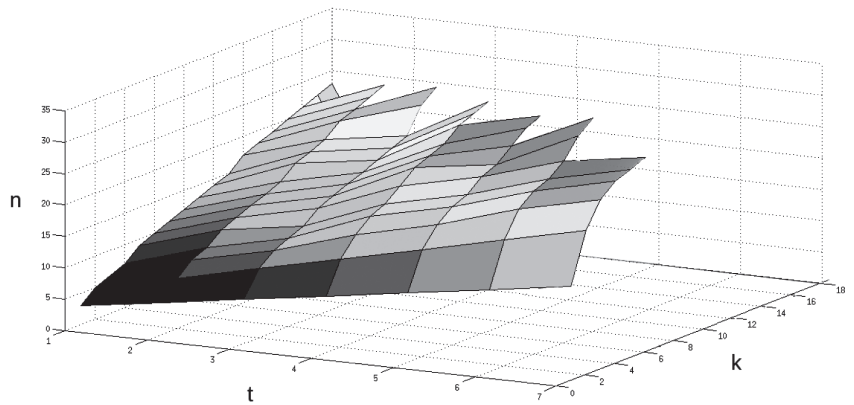


Рис. 5. Зависимость значения n от параметров k, t

графиков (рис. 6 и 7), этот параметр одинаков и у кодов, найденных с помощью полного перебора, и у кодов, построенных предложенным алгоритмом. Т. е. несмотря на то что предложенный алгоритм рассматривает гораздо меньше вариантов, эффективность кодов, построенных с его помощью, не уступает лучшим вариантам, найденным полным перебором.

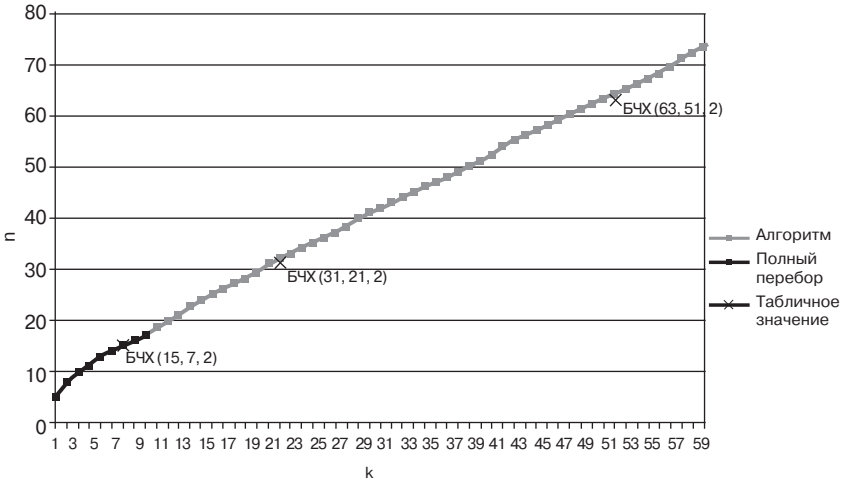


Рис. 6. Сравнение значения *n* у 2-х алгоритмов и табличных данных при $t = 2$

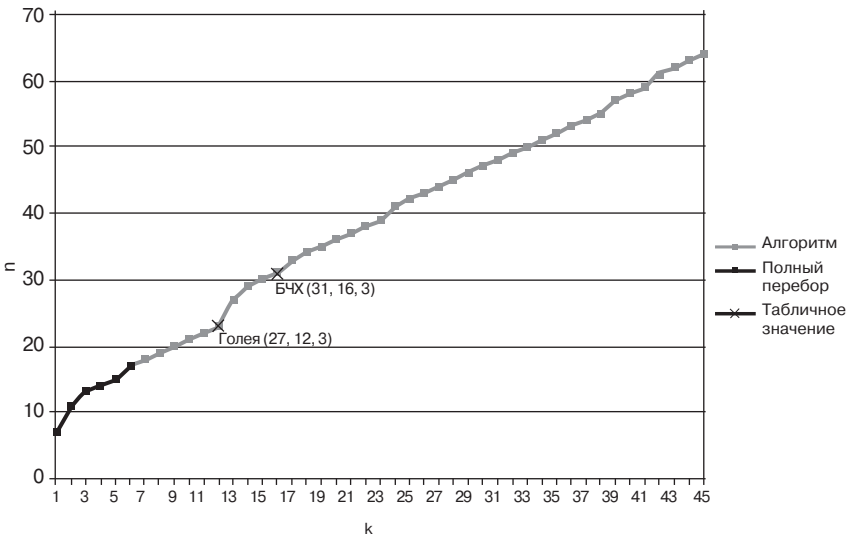


Рис. 7. Сравнение значения n у двух алгоритмов и табличных данных при t = 3

Вместе с тем алгоритм не всегда может найти самый лучший код из теоретически существующих. Это видно, если сравнить его результаты с известными на текущий момент кодами. В некоторых случаях параметр n у найденных решений несколько больше, чем у известных кодов. Например, известно о существовании БЧХ кодов с (n, k, t)-параметрами: (15,7,2), (31,21,2), (63,51,2), (31,16,3); совершенного кода Голея с параметрами (23,12,3)[5]. Предложенный в статье алгоритм находит соответственно коды со следующими параметрами: (15,7,2), (*32*,21,2), (*64*,51,2), (31,16,3), (23,12,3). Т. е. в некоторых случаях алгоритмом найден самый лучший вариант, в других значение $R = \frac{k}{n}$ незначительно хуже.

Рассмотренные алгоритмы были реализованы на языке C++. В качестве компилятора использовался gcc версии 4.8.2. Тесты проводились на ЭВМ с операционной системой LinuxMint 17 на процессоре IntelCore i7 2.2ГГц с 6 Гб ОЗУ.

В статье был предложен алгоритм построения линейных блоков двоичных кодов при заданных параметрах k — числе информационных символов и t — числе исправляемых ошибок. Теоретические и экспериментальные оценки показывают, что предложенный алгоритм обладает существенно меньшей вычислительной сложностью, чем алгоритм полного перебора. На основе анализа результатов работы предложенного алгоритма был сделан вывод о том, что параметры построенных кодов совпадают с параметрами кодов, найденных полным перебором. Было произведено сравнение параметров построенных кодов с параметрами некоторых известных в литературе кодов (БЧХ, Голея), которое показало, что в большинстве случаев параметры построенных кодов не уступают известным, а в остальных случаях незначительно хуже.

Примечания

[1] *Вернер М.* Основы кодирования: Учеб. для вузов. М.: Техносфера, 2004.

[2] *Духин А.А.* Теория информации: Учеб. пособие. М.: Гелиос АРВ, 2007.

[3] Там же.

[4] Там же.

[5] *Гаранин М.В. и др.* Системы и сети передачи информации: Учеб. пособие для вузов. М.: Радио и связь, 2001.

Abstracts

Ya. Bashuev, V. Grigorjev

Social nets deanonimization methods

The work is devoted to the study of the most important directions of the analysis of social networks – developing methods for deanonimization actors of those networks. The purpose of the paper is a comparative analysis of existing methods and models of users deanonimization and the development of a modified deanonimization algorithm based on proposed method of combining social graph vertices. It is shown that the use of graph vertices associations procedure enables the effective separation of tasks on equivalent subtasks, thus, achieving a drastic reduction in dimensionality of conducted calculations.

Key words: social network, deanonimization hidden users.

A. Bastron, E. Zheludeva

Media convergence in journalism. From classics to the universality

This article examines the use of information technologies in the work of the journalist. Challenges and opportunities of journalism in the context of media convergence are analyzed. It considers the problem of University education of the "universal" journalist in the process of integration of information and communication technologies into a single information resource.

Key words: media convergence, media, information technology, crowdsourcing, cloud technologies, processes of transformation, content.

N. Bobkova, A. Roganov, S. Stroganova, N. Teodorovich

Remote technology in teaching the technical subjects. Tendencies, prospects, chalanges

The article deals in issues of using the information communicational technologies and remote teaching technology in higher school professor's practice. Tendencies in the development of remote technology use in nowadays context are considered. There is a generalization of the best practices in the creating and usage of remote training in technical subjects. Through the example of such subject as "Electrical engineering" several difficulties specific to the implementation of the distant learning are identified and analyzed. A solution to their problem by applying the case technologies is presented.

Key words: remote teaching, information communicational technologies in education, educational environment, casetechnology, distant training in technical subjects.

D. Ivanov, A. Nikitin

Method of the textdependent voice authentication

In this work the authors propose method of user's biometric authentication by parameters of his voice. The principal parameters of the developed model are individual speed of the speech and pronouncing length of the speech elements.

In the cource of voice samples comparison algorithm development it was discovered that the analysis of the speech and pronouncing length of the speech elements in textdependent user's voice authentication procedure is reduced to finding the percentage of recording segments, overlapping in content and location, with due consideration for the variability of the uttered passphrase total length. For comparison the Mel-frequency cepstral coefficients method was used.

Key words: biometrics, voice authentication, Mel-frequency cepstral coefficients method.

O. Kazarin, M. Repin

Security state model of the payment system

The process of monitoring the state of information security of the payment system is the basis for the evaluation and analysis of information security risks.

An important aspect of the task of monitoring of information security state of the payment system is the need to evaluate the relations between initiating events and their influence on the vulnerability of the payment system.

These relations can be described with the help of logical and probabilistic models, the application of which is considered in this paper.

Key words: payment system, information security monitoring, logical and probabilistic models, risk of information security, initiating events.

V. Kiryukhin

Algorithm for constructing binary linear block codes according to the given number of information symbols and the number of correctable errors

The article presents an algorithm that constructs binary linear block codes according to the quantities of message and error correction bits. Theoretical complexity estimation and experimental time evaluation of the presented algorithm are proposed. It is shown that the algorithm provides codes with parameters equivalent to the results of algorithm exhaustive search. In most cases these parameters are the same as parameters of codes well-known from the literature (BCH, Golay), and in other cases they are inconsiderably worse.

Keywords: interference immune coding, linear codes.

V. Kuznetsov

Cloud service security model based OSE/RM open environment model

This paper proposes an algorithmic approach to building security model for cloud service was selected by the author OSE/RM open environment model as the basis of presentation for cloud system, which allows to organize and justify the choice of protection mechanisms. To demonstrate the application of the algorithm for constructing the security model an extension that allows to carry out the verification of the security model for cloud environment is built.

Key words: security model, cloud service, model of an open environment, verification of the security model.

M. Repin

Risk models of information security violations in the payment system

The process of providing information security risks early warning in the payment system is essential for defining the necessary control actions to minimize those risks.

An important aspect of the problem of preventing risks is to model the process of their occurrence.

Such models can be described in various ways, including those using logical and probabilistic models, the application of which is considered in this paper.

Key words: payment system, key risk indicators, logical-probabilistic models, risk of information security, initiating events.

A. Satunina, L. Sysoeva

The use of evaluation process modes in forming indicators panels of information analysis system of the organization

This article discusses the approaches to the use of ISO/IEC 15504 evaluation processes methodology for designing control panels of information analytical system. The analysis resulted in the technology for creation of components of evaluation the process: the measurement scheme, base process model, scope of business process model with a view to obtaining a set of indicators for their visualization on panels of information analytical system. The technology for forming business process model is a systematic approach to developing scales and indicators of processes.

Key words: information analytical system, process approach to management, process evaluation, scope of process model, process profile.

G. Shevtsova, A. Mozgov

Data security specifics in exhibition business

The article presents challenges in preparation the participation exhibition business for the organization handling confidential information in its operations. An inadequacy of research into the matter of information security in exhibition business entails the weak normative framework necessary to regulate information security issues there.

Key words: exhibition business, vulnerability of confidential information security, data security in exhibition business, safety of exhibition rendering.

Yu. Voronova

Time series mathematical modeling in volatility clustering context

The work considers an issue of volatility evaluation for prices of open-ended mutual investment funds through GARCH and EGARCH-processes. An evident advantage of EGARCH model use over results obtained with GARCH is the possibility to recognize volatility sign. Such effect is achieved by including the function $g_t(\varepsilon_{t-1})$ at the positive and negative interval ε_t allows the conditional dispersion process to respond asymmetrically to asset price increase and fall. Besides the study contains approaches with evaluation of time series fractal structure. Numerical results of time series predictions with the local approximation of 1st and 2nd orders are obtained. The output matrix of parameters *B* for the local approximation of 2nd order.

Key words: volatility, mutual fund, GARCH, kurtosis, EGARCH, approximation, prediction.

V. Zharov, T. Guseva, Yu. Taratukhina

Educational informatics as technical, philosophic notion and modern pedagogical concept

The article considers the developing branch of knowledge at the interface of the pedagogics, informatics and information flows control technologies in modern learning process. There is a substantiation for the preference given to the concept of educational informatics over the concept of information pedagogics. The authors provide examples of the significance of the new branch of knowledge studied by using educational informatics.

Key words: educational informatics, teacher's cultural relevant mentality, educational environment, constructive knowledge transfer, cross cultural didactics, information educational environment.

Сведения об авторах

Бастрон Алевтина Алексеевна – кандидат педагогических наук, доцент кафедры фундаментальной и прикладной математики, Институт информационных наук и технологий безопасности, РГГУ, bastron-aa@inbox.ru

Башуев Ярослав Павлович – студент, Московский технологический университет, ybashuev@gmail.com

Бобкова Наталья Юрьевна – начальник отдела формирования и реализации дистанционных технологий, Технологический университет, bobkova.ny@ut-mo.ru

Воронова Юлия Игоревна – студентка, Вятский государственный университет, vishny77@rambler.ru

Григорьев Виталий Робертович – кандидат технических наук, доцент, Московский технологический университет, grigorjev_vr@mail.ru

Гусева Татьяна Аркадьевна – специалист по учебно-методической работе, Институт информационных наук и технологий безопасности, РГГУ, guseva-ta@mail.ru

Жаров Валентин Константинович – доктор педагогических наук, профессор, заведующий кафедрой фундаментальной и прикладной математики, Институт информационных наук и технологий безопасности, РГГУ, valcon@mail.ru

Желудева Елена Вадимовна – кандидат философских наук, доцент кафедры русского языка, литературы и журналистики, Московский государственный гуманитарно-экономический университет, academia_mva@mail.ru

Иванов Дмитрий Александрович – аспирант, Московский технологический университет, fenix.104.2@mail.ru

Казарин Олег Викторович – доктор технических наук, ведущий научный сотрудник, Институт проблем информационной безопасности МГУ имени М.В. Ломоносова, профессор кафедры комплексной защиты информации, Институт информационных наук и технологий безопасности, РГГУ, okaz2005@yandex.ru

Кирюхин Виталий *Александрович* – студент, Московский технологический университет, v.a.kir@yandex.ru

Кузнецов Владимир Сергеевич – аспирант, Московский технологический университет, kuznecov.vladimir.00@mail.ru

Мозгов Алексей Александрович – специалист ЗАО «Конкордия – Эссет Менеджмент», antivandaller@mail.ru

Никитин Андрей Павлович – аспирант, Московский технологический университет, a.p.nikitin@bk.ru

Репин Максим Михайлович – ассистент кафедры ИУ-8, Московский государственный технический университет имени Н.Э. Баумана, bmstu.iu8@gmail.com

Роганов Андрей Арьевич – кандидат технических наук, доцент, заведующий кафедрой информационных систем и моделирования, Институт информационных наук и технологий безопасности, РГГУ, andrej.a@mail.ru

Сатунина Анна Евгеньевна – кандидат экономических наук, профессор кафедры информационных систем и моделирования, Институт информационных наук и технологий безопасности, РГГУ, aesat@mail.ru

Строганова Светлана Михайловна – старший преподаватель кафедры информационных технологий и управляющих систем, Технологический университет, stroganova.sm@ut-mo.ru

Сысоева Леда Аркадьевна – кандидат технических наук, доцент кафедры моделирования в экономике и управлении факультета управления, Институт экономики, управления и права РГГУ; директор Центра информационных систем и технологий в образовательной деятельности, leda@rggu.ru

Таратухина Юлия Валерьевна – кандидат филологических наук, доцент факультета бизнеса и менеджмента, Национальный исследовательский университет «Высшая школа экономики», jtaratuhina@hse.ru

Теодорович Наталия Николаевна – кандидат технических наук, доцент кафедры информационных технологий и управляющих систем, Технологический университет, teonat@rambler.ru

Шевцова Галина Александровна – кандидат исторических наук, доцент кафедры информационной безопасности, Институт информационных наук и технологий безопасности, РГГУ, shevtsova-g@rambler.ru

General data about the authors

Bashuev Yaroslav P. – student, Moscow Technological University, ybashuev@gmail.com

Bastron Alevtina A. – Ph.D. in Education, associate professor of the Department of Fundamental and Applied Mathematics, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, bastron-aa@inbox.ru

Bobkova Natal'ya Yu. – head of the Department of the Information Technology Generation and Implementation, University of Technology, bobkova.ny@ut-mo.ru

Grigorjev Vitaly R. – Ph.D. in Engineering, associate professor, Moscow Technological University, grigorjev_vr@mail.ru

Guseva Tat'yana A. – specialist in Instructions and Methodics, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, guseva-ta@mail.ru

Ivanov Dmitriy A. – postgraduate student, Moscow Technological University, fenix.104.2@mail.ru

Kazarin Oleg V. – Dr. in Engineering, leading researcher, Institute of Information Security Issues, Lomonosov Moscow State University; professor of the Department of Complex Information Security, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, okaz2005@yandex.ru

Kiryukhin Vitaly A. – student, Moscow Technologicalw University, v.a.kir@yandex.ru

Kuznetsov Vladimir S. – postgraduate student, Moscow Technological University, kuznecov.vladimir.00@mail.ru

Mozgov Aleksey A. – specialist, ZAO "Concordia – Asset Management", antivandaller@mail.ru

Nikitin Andrey P. – postgraduate student, Moscow Technological University, gouststalker@mail.ru

Repin Maxim M. – assistant at the Department IU-8, Bauman Moscow State Technological University, bmstu.iu8@gmail.com

Roganov Andrey A. – Ph.D. in Engineering, associate professor, head of the Department of Information Systems and Modelling, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, andrej.a@mail.ru

Satunina Anna E. – Ph.D. in Economics, professor of the Department of Information Systems and Modelling, Russian State University for the Humanities, aesat@mail.ru

Shevtsova Galina A. – Ph.D. in History, associate professor of the Information Technology Department, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, shevtsova-g@rambler.ru

Stroganova Svetlana M. – senior lecturer, Department of Information Technology and Controlling Systems, University of Technology, stroganova.sm@ut-mo.ru

Sysoeva Leda A. – Ph.D. in Engineering, associate professor of the Department of Modelling in the Economics and Management, Faculty of Management, Institute of Economics, Management and Law, director, Center of Information Systems and Technology in Education, Russian State University for the Humanities, leda@rggu.ru

Taratukhina Yulia V. – Ph.D. in Philology, associate professor of the Faculty of Business and Management, Scientific Research University–Higher School for Economics, jtaratuhina@hse.ru

Teodorovich Natalia N. – Ph.D. in Engineering, associated professor of the Department of Information Technology and Controlling Systems, University of Technology, teonat@rambler.ru

Voronova Yulia I. – student, Vyatka State University, vishny77@rambler.ru

Zharov Valentin K. – Dr. in Education, professor, head of the Department of Fundamental and Applied Mathematics, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, valcon@mail.ru

Zheludeva Elena V. – Ph.D. in Philosophy, associate professor of the Department of Russian Language, Literature and Journalism, Moscow State University for Economics and Humanities, academia_mva@mail.ru

Художник серии *В.В. Сурков*

Корректор *О.К. Юрьев*

Компьютерная верстка *М.Е. Заболотникова*

Подписано в печать 20.09.2016.
Формат $60\times90^{1}/_{16}$.
Усл. печ. л. 10,5. Уч.-изд. л. 11,0.
Тираж 1050 экз. Заказ № 82

Издательский центр
Российского государственного
гуманитарного университета
125993, Москва, Миусская пл., 6
www.rggu.ru
www.knigirggu.ru

Журнал «Вестник РГГУ»
Серия «Документоведение и архивоведение. Информатика.
Защита информации и информационная безопасность»
выходит 4 раза в год.
Подписка принимается всеми отделениями связи
без ограничений.
Подписной индекс в каталоге «Газеты. Журналы»
ОАО Агентства «Роспечать» – 71128
Не забудьте своевременно подписаться
на наш журнал!