

Зарегистрировано Федеральной службой по надзору
в сфере связи, информационных технологий и
массовых коммуникаций
Свидетельство № 015372 от 02.11.1996 г.

Журнал входит в систему Российского индекса
научного цитирования (РИНЦ) и международную
систему идентификации научных публикаций
CrossRef (DOI).

Председатель редакционного совета:

кандидат технических наук, доцент

Андрей Валерьевич Федичев

Главный редактор:

доктор технических наук, профессор

Дмитрий Анатольевич Ловцов

Шеф-редактор,

заместитель главного редактора:

Григорий Иванович Макаренко

Учредитель и издатель:

Федеральное бюджетное учреждение
«Научный центр правовой информации
при Министерстве юстиции
Российской Федерации»

Отпечатано в РИО НЦПИ при Минюсте России.

Печать цветная цифровая.

Подписано в печать 30.03.2018 г.

Общий тираж 100 экз. Цена свободная.

Адрес редакции:

125437, Москва, Михалковская ул.,
65, стр.1

Телефон: +7 (495) 539-25-29

E-mail: inform360@yandex.com

Требования, предъявляемые к рукописям,
размещены на сайте

<http://www.monitoringlaw.ru>

СОДЕРЖАНИЕ

ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

**ОБ ОКИНАВСКОЙ ХАРТИИ ГЛОБАЛЬНОГО
ИНФОРМАЦИОННОГО ОБЩЕСТВА И ЗАДАЧАХ РАЗВИТИЯ
РОССИЙСКИХ СИСТЕМ КОММУНИКАЦИИ**

Бочков С.И., Макаренко Г.И., Федичев А.В.4

ИНФОРМАЦИОННЫЕ И ЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ В ПРАВОВОЙ СФЕРЕ

**ЭФФЕКТИВНЫЙ АЛГОРИТМ УПРАВЛЕНИЯ ПЕРЕРАБОТКОЙ
СУДЕБНОЙ СТАТИСТИЧЕСКОЙ ИНФОРМАЦИИ**

Борисов Р.С.15

**ОБМЕН ИНФОРМАЦИЕЙ В ПРОФЕССИОНАЛЬНОЙ
ДЕЯТЕЛЬНОСТИ ЮРИСТА: ИССЛЕДОВАНИЕ
ОСОБЕННОСТЕЙ КОММУНИКАТИВНОЙ ДЕЯТЕЛЬНОСТИ**

Ващекин А.Н., Шевченко Д.И.23

**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ СТАТИСТИЧЕСКОГО
АНАЛИЗА МАРКЕТИНГОВЫХ ИССЛЕДОВАНИЙ**

Ловцов Д.А., Богданова М.В., Паршинцева Л.С.32

ИНФОРМАЦИОННАЯ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

**ИНФОРМАЦИОННАЯ НАДЕЖНОСТЬ ФУНКЦИОНИРОВАНИЯ
ТЕЛЕМАТИЧЕСКОЙ СЕТИ ГАС РФ «ПРАВОСУДИЕ»**

Ловцов Д.А.40

**КАЧЕСТВО СТАНДАРТИЗОВАННОЙ СИСТЕМЫ
АЛГОРИТМОВ ШИФРОВАНИЯ ДАННЫХ В ГАС РФ
«ПРАВОСУДИЕ»**

Королев В.Т., Ловцов Д.А.49

ТРИБУНА МОЛОДОГО УЧЁНОГО

**ГОСУДАРСТВЕННАЯ СИСТЕМА КООРДИНАЦИИ
ИНФОРМАТИЗАЦИИ КАК МЕХАНИЗМ ФОРМИРОВАНИЯ
ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА**

Троян (Фадеева) Н.А.60

Abstracts, Keywords and References68

РЕДАКЦИОННЫЙ СОВЕТ

ФЕДИЧЕВ Андрей Валерьевич
ЗАПОЛЬСКИЙ Сергей Васильевич
ЗУДОВ Юрий Валерьевич
ЕМЕЛИН Николай Михайлович
ИСАКОВ Владимир Борисович
МАКАРЕНКО Григорий Иванович
ТЮТЮННИК Вячеслав Михайлович

Иностранные члены

КУРБАНОВ Габил Сурхай оглы
ШАРШУН Виктор Александрович

председатель редакционного совета, кандидат технических наук, доцент, г. Москва
доктор юридических наук, профессор, г. Москва
кандидат исторических наук, г. Москва
доктор технических наук, профессор, г. Москва
доктор юридических наук, профессор, г. Москва
шеф-редактор, заместитель главного редактора, г. Москва
доктор технических наук, профессор, г. Москва

доктор юридических наук, профессор, г. Баку, Азербайджан
кандидат юридических наук, г. Минск, Белоруссия

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

АЛЕКСЕЕВ Владимир Витальевич
БЕТАНОВ Владимир Вадимович
ЗАЙЦЕВ Александр Владимирович
ЛОВЦОВ Дмитрий Анатольевич
МАРКОВ Алексей Сергеевич
НИЕСОВ Владимир Александрович
ФЕДОСЕЕВ Сергей Витальевич
ЦИМБАЛ Владимир Анатольевич
АТАГИМОВА Эльмира Исамудиновна
ЗАХАРЦЕВ Сергей Иванович
КАБАНОВ Павел Александрович
ПОЛЯКОВА Татьяна Анатольевна
РЫБАКОВ Олег Юрьевич
ТАНИМОВ Олег Владимирович
ТЕРЕНТЬЕВА Людмила Вячеславовна
ЧУБУКОВА Светлана Георгиевна

доктор технических наук, профессор, г. Тамбов
доктор технических наук, профессор, г. Москва
доктор технических наук, профессор, г. Москва
главный редактор, доктор технических наук, профессор, г. Москва
доктор технических наук, доцент, г. Москва
кандидат технических наук, профессор (МАААК), г. Москва
кандидат технических наук, доцент, г. Москва
доктор технических наук, профессор, г. Серпухов, Московская область
кандидат юридических наук, доцент, г. Москва
доктор юридических наук, профессор
доктор юридических наук, профессор
доктор юридических наук, доцент, г. Москва
доктор юридических наук, доктор философских наук, профессор, г. Москва
кандидат юридических наук, доцент, г. Москва
кандидат юридических наук, доцент, г. Москва
кандидат юридических наук, доцент, г. Москва

EDITORIAL COUNCIL

Andrei FEDICHEV
Sergei ZAPOL'SKII
Iurii ZUDOV
Nikolai EMELIN
Vladimir ISAKOV
Grigory MAKARENKO
Viacheslav TIUTIUNNIK

Foreign members

Gabil KURBANOV
Viktor SHARSHUN

Chairman of the Editorial Council, Ph.D. in Technology, Associate Professor, Moscow
Doctor of Science in Law, Professor, Moscow
Ph.D. in History, Moscow
Doctor of Science in Technology, Professor, Moscow
Doctor of Science in Law, Professor, Moscow
Managing Editor, Moscow
Doctor of Science in Technology, Professor, Tambov

Doctor of Science in Law, Professor, Baku, Azerbaijan
Ph.D. in Law, Minsk, Belarus

EDITORIAL BOARD

Vladimir ALEKSEEV
Vladimir BETANOV
Aleksandr ZAITSEV
Dmitrii LOVTSOV
Aleksei MARKOV
Vladimir NIESOV
Sergei FEDOSEEV
Vladimir TSIMBAL
El'mira ATAGIMOVA
Sergei ZAKHARTSEV
Pavel KABANOV
Tat'iana POLIAKOVA
Oleg RYBAKOV
Oleg TANIMOV
Liudmila TERENT'EVA
Svetlana CHUBUKOVA

Doctor of Science in Technology, Professor, Tambov
Doctor of Science in Technology, Professor, Moscow
Doctor of Science in Technology, Professor, Moscow
Editor-in-Chief, Doctor of Science in Technology, Professor, Moscow
Doctor of Science in Technology, Associate Professor, Moscow
Ph.D. in Technology, Professor (International Academic Accreditation & Certification Committee), Moscow
Ph.D. in Technology, Associate Professor, Moscow
Doctor of Science in Technology, Professor, Serpukhov, Moscow Oblast
Ph.D. in Law, Associate Professor, Moscow
Doctor of Science in Law, Professor
Doctor of Science in Law, Professor
Doctor of Science in Law, Associate Professor, Moscow
Doctor of Science in Law, Doctor of Science in Philosophy, Professor
Ph.D. in Law, Associate Professor, Moscow
Ph.D. in Law, Associate Professor, Moscow
Ph.D. in Law, Associate Professor, Moscow

Registered by the Federal Service for Supervision in the
Sphere of Telecom, Information Technologies and Mass
Communications

Registration Certificate No. 015372
of the 2nd of November 1996.

The journal is registered in the Russian Science Citation
Index (RINTs) and CrossRef, the official Registration
Agency of the International Digital Object Identifier
(DOI) Foundation

Chair of the Editorial Council:

Ph.D. in Technology, Associate Professor
Andrei Fedichev

Editor-in-Chief:

Doctor of Science in Technology, Professor
Dmitrii Lovtsov

Managing Editor,

Deputy Editor-in-Chief:
Grigoriy Makarenko

Founder and publisher:

Federal State-Funded Institution "Scientific
Centre for Legal Information under the
Ministry of Justice
of the Russian Federation"

Printed by the Printing and Publication Division
of the Scientific Centre for Legal Information
under the Ministry of Justice
of the Russian Federation.

Printed in digital colour. Approved for print
on the 30th of March, 2018.

Number of items printed: 100. Free price.

Postal address:

Mikhalkovskaya str., bld. 65/1, 125 438, Moscow,
Russia

Telephone: +7 (495) 539-23-14

E-mail: inform360@yandex.com

Guidelines for preparing manuscripts for
publication can be found on the website
<http://www.informatika360.ru>

CONTENTS

LEGAL REGULATION IN INFORMATION SOCIETY

ON THE OKINAWA CHARTER ON GLOBAL INFORMATION SOCIETY AND THE GOALS OF DEVELOPMENT OF RUSSIAN COMMUNICATION SYSTEMS

Sergei Bochkov, Grigoriy Makarenko4

INFORMATION AND ELECTRONICS TECHNOLOGIES IN THE LEGAL SPHERE

AN EFFICIENT CONTROL ALGORITHM FOR PROCESSING JUDICIAL STATISTICAL INFORMATION

Roman Borisov15

INFORMATION EXCHANGE IN THE LAWYER'S PROFESSIONAL ACTIVITIES: INVESTIGATION OF SPECIFIC FEATURES OF COMMUNICATIVE ACTIVITY

Andrei Vashchekin, Dar'ia Shevchenko23

INFORMATION TECHNOLOGIES IN THE STATISTICAL ANALYSIS OF MARKETING RESEARCH

Dmitrii Lovtsov, Marina Bogdanova, Lidiia Parshintseva32

INFORMATION AND COMPUTER SECURITY

INFORMATION RELIABILITY OF FUNCTIONING OF THE TELEMATIC NETWORK OF THE STATE AUTOMATED SYSTEM OF THE RUSSIAN FEDERATION "PRAVOSUDIIE" ["JUSTICE"]

Dmitrii Lovtsov40

QUALITY OF A STANDARDISED SYSTEM OF DATA ENCRYPTION ALGORITHMS IN THE STATE AUTOMATED SYSTEM OF THE RUSSIAN FEDERATION "PRAVOSUDIIE" ["JUSTICE"]

Vladimir Korolev, Dmitrii Lovtsov49

YOUNG RESEARCHERS FORUM

A STATE SYSTEM OF INFORMATISATION COORDINATION AS A MECHANISM FOR CREATING A SINGLE INFORMATION SPACE

Natal'ia Troian (Fadeeva)60

Abstracts, Keywords and References68

ОБ ОКИНАВСКОЙ ХАРТИИ ГЛОБАЛЬНОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА И ЗАДАЧАХ РАЗВИТИЯ РОССИЙСКИХ СИСТЕМ КОММУНИКАЦИИ

Бочков С.И., Макаренко Г.И., Федичев А.В.*

Ключевые слова: глобализм Интернета, информационная агрессия, информационные технологии, угрозы безопасности, угрозы информационной безопасности, стоимость информации, третья пригода Вселенной, закладки в оборудование.

Аннотация.

Окинавская хартия¹ глобального информационного общества служит основой в российском юридическом сообществе для обоснования государственной политики в области развития Интернет-технологий в стране. Однако опыт Китая показывает, что есть и другие — более безопасные с точки зрения государственности — стратегии развития информационных технологий. Авторами делается попытка ввести упорядоченную по видам классификацию информации различных видов, подвергаются сомнению декларируемые основные цели Окинавской хартии, показывается, что наличие «информационного общества» в ведущих экономически развитых западных странах не смогло способствовать устойчивому экономическому росту (скорее наоборот — поспособствовало кризису 1998 г.). В ряде случаев современные Интернет-сети привели к ряду государственных переворотов, принесли несчастье многим публичным людям, так как пользователи социальных сетей фактически не несут никакой ответственности за свои высказывания. Более того, стратегия развития технологии коммуникаций в надежде на международное разделение производства отдельных компонент оборудования сетей коммуникации для России опасна и может привести к катастрофе, так как выпускаемое западное оборудование нередко содержит вредоносные закладки.

DOI: 10.21681/1994-1404-2018-1-04-14

Начало 21 века характеризуется глобальным «наступлением» Интернета на человечество. Считается, что правовой основой такого наступления является «Окинавская хартия глобального информационного общества» (далее — Окинавская хартия), принятая 22 июля 2000 года на саммите лидеров стран G8. Именно на этот документ принято ссылаться в российском юридическом сообществе для обоснования государственной политики в области развития Интернет-технологий в стране. Однако следует обратить

внимание на два фактора среди множества других, оказавших влияние на процессы информатизации в России:

1. В Окинавской хартии отсутствует упоминание об Интернете. Документ посвящен общим представлениям лидеров стран о возможностях информационных технологий.

2. Саммиты G8 впоследствии были обозначены Президентом Российской Федерации как “клуб по интересам”, декларации которого не являются юридически значимым международными актами.

Тем не менее, если придерживаться основных положений Окинавской хартии, то необходимо

¹ “Окинавская хартия глобального информационного общества” от 21 июля 2000 года. Сайт: <http://base.garant.ru/2560931/>.

* **Бочков Сергей Иванович**, председатель Совета Некоммерческого партнерства «Неправительственный инновационный центр», Российская Федерация, г. Москва.

E-mail: vss-05@mail.ru

Макаренко Григорий Иванович, начальник отделения развития научной периодики ФБУ «Научный центр правовой информации при Министерстве юстиции Российской Федерации», Российская Федерация, г. Москва.

E-mail: monitorlaw@yandex.com

Федичев Андрей Валерьевич, кандидат технических наук, директор ФБУ «Научный центр правовой информации при Министерстве юстиции Российской Федерации», Российская Федерация, г. Москва.

E-mail: fedichev@scli.ru

рассмотреть ключевое понятие — информационно-коммуникационные технологии (ИТ).

Дословный перевод слова *informatio* с латинского языка на русский означает *разъяснение, изложение, осведомление* и как термин обыденного языка относится к познавательной-коммуникативной сфере человеческой деятельности. Информация означает совокупность новых (для получателя) сведений о каких-либо событиях или фактах [1], хотя считается, что в науку это понятие было введено в 1928 г. Р. Хартли (США) для обозначения меры количественного измерения снятой неопределённости при получении сведений, распространяемых по техническим каналам связи безотносительно к содержанию этих сведений¹. До настоящего времени современное общество не определилось с двойственным характером указанного понятия: является ли понятие информация характерным только для систем связи или для иконографической (книги, журналы, газеты, письма, документы и т. д.) продукции, применимо ли оно для устного общения?

В языкознании коммуникация — это «целенаправленная передача некоторого содержания с помощью языковых форм от одного участника ситуации общения другому»². Существуют и другие определения понятия коммуникация, в частности, это «взаимодействие людей и животных, предполагающее обмен информацией с помощью специализированных сигналов-посредников» и т. д. Учитывая эти аксиоматические утверждения, можно считать, что для коммуникации не всегда характерно наличие каких-либо материальных носителей (в том числе и сетей связи). Непосредственное общение людей с использованием звуковых сигналов, передача сообщения семафором, которая осуществляется сигнальщиками с помощью изменения положения флагов во флоте или включение водителем в автомобиле предупреждающего сигнала «поворот налево (направо)» и т. д. — всё это также примеры коммуникации. Аксиоматичный характер данного положения можно найти в Гражданском кодексе Российской Федерации. Так, в Статье 159, п.1. «Устные сделки» указывается: «Сделка, для которой законом или соглашением сторон не установлена письменная (простая или нотариальная) форма, может быть совершена

устно»³. Для того, чтобы двум субъектам договориться, необходимо совершить акт коммуникации — обменяться речевыми (или какими-либо другими) сообщениями, понять их, уяснить сведения, которые они получили друг от друга, и заключить устное соглашение. Здесь уместно заметить, что истоки указанной нормы лежат в российской истории, когда сделки между купцами совершались под «честное слово». Существовавший в до-революционной России⁴ купеческий кодекс чести был основан на православных традициях миропонимания и воспитания не одного поколения купцов. Честь всего рода у русских купцов ценилась превыше денег, а результат его деятельности оценивался не столько капиталом, сколько общественно полезными делами.

С правовой точки зрения понятие информации определено Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» как сведения (сообщения, данные) независимо от формы их представления. При этом в юридической научной литературе практически не встречается классификации понятия информации по форме представления. Предлагается данное правовое понятие классифицировать следующим образом:

1. Информация первого рода — совокупность производимых сообщений и воспринимаемых сведений в устной форме или с использованием каких-либо однозначно понимаемых звуко-визуальных сигналов (жестов) участниками непосредственного общения (коммуникаций).

2. Информация второго рода — совокупность производимых сообщений и воспринимаемых сведений участниками непосредственного общения (коммуникаций) в письменной форме собственноручно.

3. Информация третьего рода — совокупность производимых сообщений и воспринимаемых сведений участниками непосредственного общения (коммуникаций) с использованием систем связи без их сохранения на каких-либо материальных носителях.

4. Информация четвертого рода — совокупность производимых сообщений и воспринимаемых сведений участниками непосредственного общения (коммуникаций) с использованием си-

¹ Современный философский словарь (под редакцией д.ф.н. профессора В.Е. Кемерова). М.: ПАНПРИНТ, 1998.

² «Большая Российская Энциклопедия», электронная версия. Проект Министерства культуры Российской Федерации. Сайт: <https://bigenc.ru/section/linguistics>.

³ Гражданский кодекс Российской Федерации. Информационно-правовая система «Гарант». Сайт: <http://base.garant.ru/10164072/9/#ixzz53QBVD2XY>.

⁴ Великая октябрьская социалистическая революция, произошедшая в России в 1917 году.

стем связи с сохранением на каких-либо материальных носителях.

Исходя из такой классификации, можно сделать вывод, что основу коммуникаций должен составлять язык общения, т. е. алфавит и принципы его использования, образы и ассоциации, мировоззрение. Информационные технологии, как нам представляется, должны рассматриваться прежде всего с культурологической точки зрения.

Не претендуя на исключительность, схематично основу коммуникаций для человека можно представить в следующем виде (рис.1).



Рис. 1. Модель коммуникаций человека

В Окинавской хартии (п. 2) сформулированы основные цели, направленные на:

- устойчивый экономический рост;
- повышение общественного благосостояния;
- стимулирование социального согласия и полной реализации их потенциала в области укрепления демократии;
- транспарентное и ответственное управление, права человека,
- развитие культурного многообразия и укрепления международного мира и стабильности.

Итак, **устойчивый экономический рост**. Устойчивое развитие подразумевает обеспечение поступательного роста экономики без ущерба для основных отраслей промышленности, сбалансированность основных элементов национальной экономики. Экономический кризис в России 2008 году был спровоцирован ипотечным кризисом в США и, как следствие, кризисом ликвидности мировых банков. Анализ причин кризисной ситуации проведен различными экспертами достаточно детально⁵. Однако, хотелось бы обратить

внимание на два фактора: необходимость выплаты значительного долга российскими компаниями (более 500 млрд долларов США) при невозможности перекредитования и падение мировых цен на нефть. Следующий спад экономики России произошел в 2014 году. Среди наиболее значимых причин этого кризиса аналитики отмечают последствия кризиса 2008 года и дальнейшее падение цен на нефть, а также санкционная политика западных стран по отношению к России в связи с ситуацией на Украине.

Наличие «информационного общества»⁶ в ведущих экономически развитых западных странах не смогло способствовать устойчивому экономическому росту.

Базовый (как принято считать) закон ФЗ № 149 в области информационного права не содержит разделов, предусматривающих порядок разработки информационно-телекоммуникационных систем, а только условия эксплуатации. У каждой такой системы существует свой «жизненный цикл» (10—15 лет), который, кстати, может не совпадать с «жизненным циклом» информации [2]. Находящиеся в эксплуатации на территории Российской Федерации программно-технические средства, поставленные в начале текущего столетия, практически выработали свой физический ресурс, морально устарели и подлежат замене.

Основным недостатком ФЗ № 149, по мнению авторов, является его ориентация на попытку регулирования общественных отношений с использованием в качестве информационных технологий программно-технических средств глобальной сети Интернет. Уместно заметить, что наряду с использованием методов коммутации пакетов существуют и другие методы организации связи (англ. *telecommunications*), в частности, коммутации каналов и сообщений. Если мы рассматриваем случай с информацией третьего рода, то в этом случае речевой (акустический) сигнал преобразуется в аналоговый электрический сигнал, а не в цифровую форму с использованием аналогово-цифровых преобразований при передаче по каналу связи и цифро-аналогового преобразования на приеме этого речевого сообщения.

Закон ФЗ № 149 содержит и ряд других противоречий. В частности, в Статье 3. п.5 декларирует-

⁵ Сайт «Академик»: <https://dic.academic.ru/dic.nsf/ruwiki/1166175>.

⁶ «Информационное общество» — общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан (Указ Президента Российской Федерации «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы»).

ся: «недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами» при том, что данный закон посвящен практически только Интернет-технологиям без ссылок на конкретные рекомендации Международного союза электросвязи⁷ и не носит общего правового характера. Более того, в Статье 13 Модельного информационного кодекса для государств — участников СНГ (часть первая) информация определяется как «сведения, представленные в любой форме и любом виде, на любых носителях, о лицах, предметах, фактах, событиях, явлениях и процессах, которые имели, имеют или будут иметь место в обществе, государстве и окружающей среде»⁸ и, как видно, существенно отличается от базовых трактовок российского законодательства.

В настоящее время большинство чиновников, журналистов, т. н. «экспертов», да и представителей научного сообщества «ходят по кругу» в своих заблуждениях, смешивая материальный и нематериальный характер информации; отождествляя «базы данных» с «базами знаний», не различая объективный и субъективный характер информации; подменяя информационные коммуникации между людьми (т. е. общение) и информационные технологии сетями связи, основанные на принципах коммутации пакетов с использованием Интернет-интерфейсов (протоколов); путают формы с видами информации и т. д. Проблем с правовым регулированием коммуникаций с каждым годом становится все больше. Наиболее полно эти проблемы изложены в проекте «Концепции Информационного кодекса Российской Федерации»⁹.

Нельзя не согласиться с основными положениями Окинавской хартии, которые провозглашают благие цели. За период с момента ее принятия прошло значительное время. Поэтому можно подвести предварительные итоги. Главным достижением современной России является распространение программно-технических средств для обеспечения работы широких слоев населения в глобальной международной сети Интернет. На сегодня можно констатировать — Россия стала важнейшим участником процесса построения глобального информационного общества, а «интернетизация» охватывает уже более 70% населения страны. Получить сведения по основным показателям развития информационного общества в России можно из «Годового отчета о ходе реализации и оценке эффективности государственной программы Российской Федерации «Информационное общество (2011—2020 годы)», утвержденного Минкомсвязи 25 апреля 2017 года, в котором одним из важнейших показателей является количество пользователей сети Интернет. С одной стороны, можно приветствовать деятельность Минкомсвязи России, которое следует в фарватере Рекомендаций МСЭ по повышению Индекса развития «информационного общества» — ИКТ (IDI); данный индекс представляет собой интегрированное значение 11 показателей. С другой стороны, предложенная МСЭ система измерения «информационного общества» является несколько односторонней, так как не учитывает эффективность использования телекоммуникаций.

Необходимо обратить внимание на отсутствие до настоящего времени в России сколько-нибудь конкурентоспособного производства программно-технических средств связи и электронных компонентов. Таким образом, развитие «информационного общества» в России проводилось за счет закупок соответствующих программно-технических средств импортного производства за «нефтедоллары». Россия в начале 90-х гг. поддалась пению западных сирен о мире и дружбе и сама отказалась от производства высокотехнологичного оборудования, закрепив это положение на законодательном уровне — по умолчанию считалось, что развитие т. н. «Интернет-технологий» должно проводиться за счет закупок программно-технических средств зарубежных производителей. Таким образом, Россия стала самым большим рынком сбыта импортной вычислительной техники и средств связи, и это при том, что Окинавская хартия не предусматривала приобретения указанной техники.

⁷ Международный союз электросвязи является специализированным учреждением Организации Объединенных Наций в области информационно-коммуникационных технологий — ИКТ. Сайт: <https://www.itu.int/en/about/Pages/default.aspx>.

⁸ Модельный информационный кодекс для государств — участников СНГ (часть первая), Принят на тридцатом пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ (постановление № 30-6 от 3 апреля 2008 года). Сайт: <http://docs.cntd.ru/document/902124603>.

⁹ Концепция Информационного кодекса Российской Федерации / Под ред. И.Л. Бачило. М.: ИГП РАН, изд-во «Канон+» РООИ «Реабилитация», 2014. 192 с. ISBN 9 78-5-88373-409-9. С. 19.

Различные потенциальные угрозы для нормального функционирования российского сегмента сети Интернет за последние несколько лет преобразовались в реальные. Это связано с агрессивной политикой западных стран по отношению к России, причем начало этому процессу положено давно. Несмотря на осуществляемую гуманитарную агрессию по отношению к России со стороны западных транснациональных компаний, тенденции «недопонимания» последствий реализованных угроз информационному суверенитету российского государства усиливаются. Сложившееся положение отмечено в «Доктрине информационной безопасности Российской Федерации» 2016 года (п. 16—19)¹⁰, а ущерб от замены устаревшего импортного оборудования связи на современное может оказаться катастрофическим для Российской экономики. Кроме того, западное электронное оборудование напичкано закладками, назначение которых — вывести из строя оборудование при начале военных действий [3, 4].

Краткий анализ зависимости устойчивого экономического роста от развития Интернета показал, что развитие т.н. «информационного общества» в России не способствует развитию различных отраслей науки и промышленности, и прежде всего связанных с разработкой, созданием и эксплуатацией программно-технических средств связи.

С культурологической точки зрения было бы неплохо использовать исторический опыт создания систем связи и автоматизированных систем связи в СССР, касающийся обязательной оценки технико-экономической эффективности и целесообразности автоматизации тех или иных процессов. К сожалению, в последние десятилетия эта традиция была незаслуженно забыта. И если проводится технико-экономическое обоснование, то, как правило, осуществляется ориентировочная оценка затрат на создание системы с закупкой импортных программно-технических средств.

Повышение общественного благосостояния. Общественное благосостояние — категория достаточно сложная. Поэтому при оценке благосостояния населения в стране различными исследователями используются различные показатели. В формулировках различных авторов можно увидеть некоторые базовые противоречия, когда

оценка благосостояния касается только неимущих слоев населения, или отдельного гражданина, или различных социальных групп. Оценить уровень благосостояния в России исходя из официальных статистических данных не представляется возможным, так как однозначного и общепринятого определения нет. Считается, что благосостояние выражается системой показателей, характеризующих уровень жизни, таких как: распределение доходов, уровень бедности, качество жизни, уровень занятости, показатели образования и здоровья и др. При этом понятие общественного благосостояния в нормативных документах отсутствует, а государственная система статистики учитывает другие показатели¹¹. Возьмем для примера зависимость количества пользователей сети Интернет с уровнем бедности. Статистика показывает, что несмотря на постоянно повышающийся за последние годы уровень «интернетизации», количество бедного населения увеличилось до 20 млн человек и имеет тенденцию к его увеличению, а не снижению. Более того, методологические материалы Госкомстата России не учитывают в расчете своих показателей количество пользователей сети Интернет. Продолжая тему благосостояния, нельзя не отметить рост безработицы, которая, по мнению экспертов, в 2—2,5 раза превышает официальные статистические данные. Таким образом, вышеупомянутая сформулированная цель — это идеологема, которая аксиоматично предполагает тождество: благосостояние — это наличие у каждого человека планеты программно-технических средств для доступа к сети Интернет. По нашему мнению, истинность этого тождества сомнительна и, как показано в работах [5—7], такое состояние со статистикой не вызывает доверия населения и власти.

Стимулирование социального согласия и полной реализации их потенциала в области укрепления демократии. Основные положения указанного тезиса тесно переплетаются с такими понятиями, как свобода слова, осуществление права на поиск, получение, передачу, производство и распространение информации, вовлечение широких слоев граждан в управление государством и др.

Однако при использовании современного Интернета положительного результата достичь не удастся. На международном уровне роль глобаль-

¹⁰ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Собрание законодательства Российской Федерации, 12 декабря 2016 г., № 50, ст. 7074.

¹¹ Федеральная служба государственной статистики. Официальный сайт: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/population/level/#.

ной сети в совершении т. н. «цветных революций» с последующим свержением законных режимов нельзя недооценить. Подделка новостей и распространение их по «социальным сетям» из зон региональных конфликтов приводит к неадекватной реакции международного сообщества и постоянному возникновению конфликтов в ООН при попытке урегулировать эти конфликты демократическим путем. Подмена исторических фактов в Интернете вызывает деструктуризацию социокультурных отношений для тех или иных стран, основанных на традиционных нравственных ценностях. Так, например, украинский исследователь коммуникаций Г. Почепцов отмечает [8]: «В свое время гуманитарным изобретением был роман, сегодня его сменили телесериалы. Роман был столь силен, что после текстов Гете или Карамзина начиналась волна самоубийств. Сегодня «Синие киты» Интернета делают то же, но они индивидуально управляют будущей жертвой, а романы были массовым управлением, где самоубийство читателя было случайным, а не запрограммированным. Только украинская киберполиция, например, обнаружила почти тысячу таких групп в сети, из которых более 600 были заблокированы.»

Что касается России, то, по официальным статистическим данным Госкомнадзора, по состоянию на 2016 год на основании судебных решений в Единый реестр было внесено более 41,8 тысяч ссылок на Интернет-ресурсы, содержащие противоправную информацию (включая порядка 14,5 тысяч «веб-зеркал»). Вместо поиска и внедрения в практику механизмов достижения общественного согласия Интернет уже стал инструментом инициации конфликтов, изменения отношения и изменения поведения как отдельных социальных групп, так и множества отдельных граждан. Манипуляция сознанием, как технология управления большим массами населения, используется достаточно давно. По сути, информацию уже надо рассматривать как третью природу Вселенной, при манипулировании которой различные исследователи выделяют в основном следующие методы [9]:

- применение отдельных фактов для обобщения и последующего изменения системных представлений человека;
- толкование различных событий в интересах отдельных социальных групп;
- устрашение якобы надвигающимися катастрофами и запугивание;
- обращение внимания на одни факты при сокрытии других;
- создание слухов и мистификаций;

- подмена понятий и смыслов и т. д.

Информация и способы ее доведения до общества меняют само общество. Печатное дело с использованием бумаги изменило религиозное право на сакральные знания, газеты с освещением текущих событий существенным образом изменили скорость коммуникаций, изобретение электронных ламп, транзисторов, а затем и микросхем предопределило появление и развитие электро-связи, которая изменила возможности управления. Интернет и современное состояние вычислительной техники, несомненно, можно считать величайшим достижением конца XX века, но предугадать тренды развития социальных отношений в эпоху Интернета, пожалуй, не возьмется никто, кроме писателей-фантастов. Трансграничный обмен информацией, автоматизированные переводчики тестов с различных иностранных языков, хранение и обработка больших объемов данных, в том числе неформализованной информации на каком-либо национальном языке и другие инновации уже оказывают нивелирующее воздействие на культуру и традиции различных стран, трансформируют мировоззрение людей за счет искажения реальности в т. н. «виртуальном пространстве».

Интернет способствует манипуляции сознанием, при том, что субъекты воздействия считают свой выбор «свободным» в соответствии со «своими убеждениями», что с большой вероятностью приводит к желаемому «социальному согласию», а на государственном уровне влечет потерю суверенитета.

Для развенчивания этого псевдосоциального согласия государства уже сейчас должны тратить значительные средства, как на подготовку специалистов, так и на выполнение такой работы, а также материальные ресурсы.

Транспарентное и ответственное управление. Принято считать, что информационные технологии повышают эффективность управления. Такие понятия как «открытое информационное общество», «электронное государство», «открытое правительство» уже прочно вошли в нашу жизнь.

Произвольное изложение “Открытым правительством” Президентского указа № 601 от 7 мая 2012 г. «Об основных направлениях совершенствования системы государственного управления» сводится к решению задач по обеспечению:

- открытости системы госуправления;
- доступности и качества государственных услуг;
- вовлечения граждан в обсуждение, принятие и контроль исполнения государственных решений.

Имеет смысл обратить внимание на некоторые, мягко говоря, странности в реализации этого указа. В частности, на официальном сайте «Открытого правительства» (<http://open.gov.ru/event/5598187/>) провозглашается некая идеология: «Реализуя идеологию открытости на федеральном уровне, Правительство РФ в январе 2014 г. утвердило Концепцию открытости федеральных органов исполнительной власти (ФОИВ), ставшую основой Стандарта открытости ФОИВ». Данное положение носит не конституционный характер и нарушает Статью 13 (п.2) Российской Конституции: «Никакая идеология не может устанавливаться в качестве государственной или обязательной»¹². Действительно, 20 сентября 2011 года по инициативе США и при поддержке 7 стран (Великобритания, Бразилия, Норвегия, Индонезия, Мексика, Филиппины, ЮАР) была учреждена международная организация «Open Government Partnership» (OGP) с целью расширения гражданского участия в общественных делах и поиска путей сделать деятельность правительства более прозрачной, гибкой, подотчетной и эффективной. В настоящее время (по состоянию на 2017 год) в этой организации участвуют 65 стран, среди которых Россия не числится.

Некоторые критики Открытого правительства отмечают: «По мнению экспертов, приведенный алгоритм перестройки государственного управления под предлагаемую США модель с большой вероятностью приведет в итоге к утрате руководством России контроля над ситуацией в стране (ради чего, по-видимому, и создавалось это партнерство). А учитывая, что в проект вовлечено значительное количество государств, эксперты сходятся во мнении, что «Открытое правительство» является новым стратегическим проектом США по созданию системы глобального управления иностранными государствами по всему миру»¹³. Легитимность деятельности «Открытого правительства» вызывает некоторое недоумение, поскольку это правительство игнорирует те принципы «открытости», ради которых оно создавалось. Например, на сайте можно найти информацию о том, что «Методика мониторинга и оценки открытости федеральных органов исполнительной власти» утверждена «Протоколом заочного голо-

сования Правительственной комиссии по координации деятельности открытого правительства». Однако вышеуказанная методика никем не подписана и ее разработчик неизвестен, а утверждающий протокол не имеет элементарных реквизитов, присущих юридически значимому документу (номер и дата подписания, учетный номер в Правительстве РФ, а также должность, фамилия, имя, отчество и подпись уполномоченного лица). Подмена понятий не обошла стороной объявленные принципы «Открытого общества» — имеющийся на сайте «Стандарт открытости» фактически таковым не является, так как не отвечает требованиям российского законодательства по стандартизации¹⁴. Необходимо напомнить законодательное толкование понятия стандарт (статья 2, п.5, ФЗ № 162): «национальный стандарт — документ по стандартизации, который разработан участником или участниками работ по стандартизации, по результатам экспертизы в техническом комитете по стандартизации или проектом технического комитета по стандартизации утвержден федеральным органом исполнительной власти в сфере стандартизации и в котором для всеобщего применения устанавливаются общие характеристики объекта стандартизации, а также правила и общие принципы в отношении объекта стандартизации».

Анализ концепций, идеологией и проектами, связанных с **«транспарентным и ответственным управлением»** является задачей нетривиальной. Однако можно заметить, что качество управления в большей степени зависит от профессионализма управленцев, наличия у них соответствующих знаний и опыта, умения общаться со своими подчиненными на одном языке, брать на себя ответственность за принятые решения. О том, насколько «Открытое правительство» решает задачи, поставленные Президентом России в Указе № 601 от 7 мая 2012, достоверных оценок нет, так как нет меры ответственности «Открытого правительства» за предлагаемые решения. При отсутствии ответственности можно предлагать что угодно¹⁵, что мы и видели на примере дебатов претендентов на пост Президента Российской Федерации.

¹⁴ Федеральный закон от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Собрание законодательства Российской Федерации от 6 июля 2015 г., № 27, ст. 3953.

¹⁵ Как тут не вспомнить известного реформатора Красной Армии маршала Тухачевского М.Н., предлагавшего оснастить Красную Армию 100 тысячами танков. В то время у СССР даже металла и машиностроительного оборудования не хватило бы на их производство. Безответственность — родовое «проклятие» оппозиции.

¹² Конституция Российской Федерации. Официальный интернет портал правовой информации: <http://publication.pravo.gov.ru/Document/View/0001201408010002?index=0&rangeSize=1>.

¹³ Информационное агентство «Uraldaily.ru», <http://uraldaily.ru/biznes/april/16/otkrytoe-pravitelstvo-predatelstvo>.

Права человека. Истоки законодательного регулирования прав человека закреплены Главой 2 «Конституции Российской Федерации». Права человека в современном обществе рассмотрены достаточно детально различными исследователями. В данной статье представляется целесообразным остановиться только на двух аспектах прав человека, связанных с коммуникациями:

1. передача (прием) информации по техническим каналам связи между двумя субъектами:

статья 23. «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения».

Статья 24. «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются».

2. коммуникации между множеством субъектов посредством информации:

Статья 29 (п.4). «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом».

12 декабря 2018 года исполняется 25 лет с даты принятия Конституции Российской Федерации. Несмотря на грандиозные, по сравнению с предыдущим историческим опытом, изменения в области телекоммуникаций, Конституция не претерпела существенных изменений в части вышеуказанных статей. Естественно, Интернет «смешал все карты».

В Конституции статья 23 предусматривает общение (коммуникацию) субъектов непосредственно друг с другом посредством систем связи. Это было обусловлено уровнем развития систем связи на тот период времени, когда в основу были положены принципы коммутации каналов и установления соединений между двумя абонентами. Такие принципы были характерны и для передачи речи (телефонная связь), и передачи данных (телеграфная связь), а также неподвижных (факсимильная связь) и подвижных изображений (видео связь). Для каждого из этих видов связи существовали технические стандарты, регламентирующие не только достаточно жесткий порядок разработки, создания и эксплуатации программно-технических средств, но и конкретные требования к их характеристикам и методам оценки качества.

Методы коммутации каналов и сообщений при организации связи сами по себе существенно затрудняли неправомерный доступ злоумышленников к информации абонентов при осуществлении

коммуникаций, а для санкционированного съема информации, передаваемой по каналам связи, применялось громоздкое и дорогостоящее оборудование. Одновременно с этим развивалось другое направление в области связи — коммутация пакетов. Мало кто даже среди ученых и специалистов мог представить себе в 90-е годы, что через каких-то 10—15 лет методы цифровой обработки аналоговых сигналов станут доминирующими, а системы коммутации пакетов вытеснят оборудование для коммутации каналов и сообщений. Специфика принципов коммутации пакетов состоит в сохранении в узлах коммутации сигналов в двоичной системе счисления (битов, байтов и т. д.) и технической возможности сравнительно простыми методами несанкционированного удаленного доступа к информации. Не зря ФСТЭК России в качестве методического обоснования защиты информации одной из главных угроз считает вмешательство зарубежных спецслужб в работу российских информационных систем и систем связи. Необходимо учитывать также различия в европейских и американских принципах реализации систем коммутации пакетов. Если в европейских системах предусматривалась достаточно жесткая система нумерации и маршрутизации для идентификации пользователей сети и контроля трансграничного обмена информацией, то американские системы построены на протоколах открытой архитектуры, которые лишены этих свойств. Реализация систем связи изначально строилась с использованием т. н. Интернет-протоколов (англ. *Internet Protocol, IP*) для объединения отдельных вычислительных сетей в единую сеть. В развитии Интернета можно выделить две основные вехи: внедрение программного обеспечения «электронной почты» (отложенная доставка сообщений) и комплекса программного обеспечения для веб-интерфейса (англ. *web interface*). Общим для этих программных комплексов является размещение на компьютере пользователей некой «программной оболочки» — браузера (англ. *web browser*), позволяющего осуществлять удаленный доступ по каналам связи к программному обеспечению и базам данных, размещенных на вычислительных комплексах — веб-серверах. Эти сервера не всегда могут находиться в юрисдикции того или иного использующего их государства.

Вышеуказанные обстоятельства являются определяющими для правоотношений. Пользователь сети Интернет практически добровольно передает владельцам серверов свою информацию, к которой имеется возможность неконтро-

лируемого доступа со стороны пользователей. Существовавшие в прошлом веке сети связи общего пользования с разделением на телефонную, телеграфную и сети с интеграцией услуг ушли в небытие, а Интернет заменил собой эти сети (см. Федеральный закон «О связи» № 126-ФЗ). Таким образом, конституционное право на тайну телефонных переговоров, передачи данных и иных сообщений в настоящее время российским гражданам не гарантируется.

Еще одно конституционное положение из прошлого века о «праве свободно искать, получать, передавать, производить и распространять информацию любым законным способом» также требует переосмысления. Основным законом, регулирующее это положение, на тот период времени (1993 год) служил Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Сейчас данный закон практически не действует. В соответствии с законом под массовой информацией понимаются «предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы» и, естественно, все действия с информацией должны осуществляться неким юридическим лицом, являющимся средством массовой информации. По закону «под средством массовой информации понимается периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием)».

Современные программно-технические средства Интернета позволяют создавать различные системы для распространения информации неограниченному кругу пользователей, такие как, например, «веб-сайт», «социальные сети» и т. д. Но мы не «заметили» одного из самых главных условий: если информация распространяется среди миллионов граждан, то организационно-техническая система должна быть зарегистрированным установленным порядком как средство массовой информации. Такое утверждение может быть подвержено критике — обязательная регистрация Интернет-сайтов и т. д. в качестве СМИ, якобы, нарушает конституционные права о свободе слова. Однако, по нашему мнению, российские граждане должны иметь право знать: является ли тот или информационный ресурс средством массовой информации или это спецоперация иностранных спецслужб или, что еще хуже, результатом интеллектуальной деятельности отдельных граждан

с извращенным сознанием, которым всё равно, какую информацию размещать на своих сайтах, лишь бы получать рекламное финансирование? Если уж российское законодательство допускает существование в информационно-телекоммуникационной сети Интернет сайтов, не зарегистрированных в качестве средства массовой информации, то имеет смысл хотя бы лишение владельцев этих сайтов возможности заниматься рекламной деятельностью. Гражданин должен иметь право на достоверную информацию, а государство обязано ему в этом помочь [10, 11].

Развитие культурного многообразия и укрепления международного мира и стабильности. Реализация этого положения возможна разными методами и способами. В утвержденной Президентом России «Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы», отмечена необходимость «сохранения традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг», а также «приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий»¹⁶. Следует заметить, что совершенно разумные принципы, заложенные в указанной Стратегии, оказались основой дальнейшего развития телекоммуникаций (*электросвязь — рус.*), а не коммуникаций (*общение — рус.*). Театр, собрание, библиотеку, выставку, семинар, урок и т. д., наверное, в каком-то недалеком будущем возможно полностью заменить Интернетом. Но тогда сложно представить себе, насколько совокупность отдельных граждан будет представлять собой общество и государство в традиционном понимании. Истоки такой подмены понятий можно найти в той же Окинавской хартии, на которую сослались разработчики Стратегии.

Реальная практика жизни показала, что использование сети Интернет далеко не всегда несет благо. Так называемые «информационные войны», как основной двигатель цветных революций; сбои в оборудовании торговых сетях, приносящие многомиллионные убытки; замалчиваемый банкирами ради сохранения репутации финансовый ущерб; навязанные Интернет-услуги и мошенничество, кража интеллектуальной собственности,

¹⁶ Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы». Официальный сайт Президента Российской Федерации: <http://www.kremlin.ru/acts/bank/41919>.

компрометация, безнаказанное очернение репутации — это тоже все Интернет. Экономическая глобализация и либерализм, поддерживаемый Интернетом во всех его проявлениях, фрагментирует сознание людей во всем мире, негативно влияет на изменение отношения к традиционным для каждого народа духовно-нравственным ценностям и провоцирует большое количество людей на поступки, не свойственные их культурным традициям. Представляется, что оценка влияния информации на людей и автоматизация рутинных процессов с использованием электронно-вычислительной техники при массовом применении должны стать основой политики любого суверенного государства.

Выводы

1. «Информационное общество», как часть третьей природы Вселенной, должно научиться измерять как эффективность от различных телекоммуникационных технологий, так и потенциальные угрозы, и возможный ущерб.

2. Одной из основных технологий инфо-коммуникаций является язык общения — для России это русский язык. В соответствии с Федеральным законом от 1 июня 2005 г. № 53-ФЗ «О государственном языке Российской Федерации» русский язык принят в качестве государственного языка общения. Уместно обратить внимание на отсутствие в данном законе нормы права, закрепляющей свободное его распространение среди неограниченного круга, как это принято в других федеральных законах об информации. А пока с правовой точки зрения можно констатировать — русский язык является собственностью издательства «АСТ».

3. Современная наука рассматривает человека в неразрывном единстве трех составляющих — физическая, психофизиологическая и социальная. Как сказал советский писатель и поэт Вадим Шефнер: «Словом можно и убить, словом можно и

спасти, словом можно полки за собой повести...». К сожалению, современное общество сконцентрировало свое внимание при рассмотрении феномена «информации» прежде всего на проблемах Интернета, а не на содержательной сущности коммуникаций. Представляется, что правовое регулирование в информационной сфере является сложной задачей, сложность решения которой пока не вполне осознается юридической наукой — гораздо более сложной и важной задачей, чем автоматизированное генерирование законов и нормативных актов.

При решении задачи правового регулирования в информационной сфере необходимо учитывать научные достижения в информологии, социологии, психологии, медицине, экономике, политологии, культурологии, лингвистике, причем окончательного решения мы можем ожидать нескоро.

4. Как мы указывали выше, вся современная российская информационно-коммуникационная техника построена из импортных компонентов. Если в ближайшие годы Россия не начнет производство таких компонентов (что вполне возможно — еще не все специалисты «рассеялись», не все заводы и институты электронной промышленности «разрушились»), то будущее российской цифровой экономики может и не состояться. Опыт войны с Ираком показал, что западными производителями предусмотрено отключение любого электронного оборудования путем разного рода закладками, обнаружить которые проблематично. Еще одна санкция на поставки России такого оборудования, и в России возможен системный кризис.

Уже на протяжении нескольких лет Институт государства и права Российской Академии наук (ИГП РАН) инициирует рассмотрение Информационного Кодекса Российской Академии наук. Но широкого общественного отклика он так и не получил.

*Рецензент: **Запольский Сергей Васильевич**, доктор юридических наук, профессор, заведующий сектором административного и бюджетного права Института государства и права Российской академии наук, Российская Федерация, г. Москва
E-mail: zpmoscow@mail.ru*

Литература

1. Бочков С.И. Информационное общество: поиск социальных детерминант формирования массового, группового и индивидуального сознания. URL: <http://np-nic.ru/publikatsii/filosofiya/5>.

2. С.И.Бочков, А.И.Федичев. О ценности информации на различных этапах жизненного цикла // Правовая информатика. 2016. № 3. С.35—40.
3. Клянчин А.И. Каталог закладок АНБ (SPIGEL). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. № 2(3). С. 60—65.
4. Клянчин А.И. Каталог закладок АНБ (SPIGEL). Часть 2. Рабочее место оператора // Вопросы кибербезопасности. 2014. № 4(7). С. 60—68.
5. Макаренко Д.Г. Общественное доверие как ресурс власти и управления // Бюллетень науки и практики. 2016. № 8 (9). С. 129—132.
6. Макаренко Д.Г. Принцип доверия как детерминанта эффективного правового регулирования общественных отношений: правовое обеспечение // Мониторинг правоприменения. 2017. № 4 (25). С. 15—22. DOI: 10.21681/2226-0692-2017-4-15-22.
7. Макаренко Д.Г. Система социально-правового регулирования как общая среда взаимодействия права и доверия // Вестник Владимирского юридического института. 2017. № 2 (43). С. 158—161.
8. Почепцов Г.Г. Коммуникации и гуманитарные изменения. Электронное СМИ «Media Sapiens». URL: http://www.osvita.mediasapiens.ua/trends/1411978127/kommunikatsii_i_gumanitar-nye_izobreteniya/.
9. Леонтьев Б.Б., Макаренко Г.И. Третья природа вселенной // Правовая информатика. 2016. № 4. С. 4—9.
10. Плигин В.Н., Макаренко Г.И. Страна нуждается в обновлении общественных договоров в современном российском обществе // Мониторинг правоприменения. 2015. № 1 (14). С. 4—11.
11. Dmitrii Lovtsov, Dmitrii Makarenko, Andrei Fedichev, Architecture of the National Classification of Legal Regimes of Restricted Access Information // Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies (BIT 2017), Moscow, Russia, December 6-7, 2017, pp. 70-73.

ЭФФЕКТИВНЫЙ АЛГОРИТМ УПРАВЛЕНИЯ ПЕРЕРАБОТКОЙ СУДЕБНОЙ СТАТИСТИЧЕСКОЙ ИНФОРМАЦИИ

Борисов Р.С.*

Ключевые слова: судебная статистическая информация, алгоритм управления, эффективность, ресурсоёмкая задача, методы распределения нагрузки, система планирования распределения нагрузки, управление параллельными вычислениями, неструктурированный массив данных.

Аннотация.

Цель работы: совершенствование методов предварительной переработки судебной статистической информации.

Метод: разработка и экспериментальный анализ алгоритма управления параллельными вычислениями для эффективной переработки судебной статистической информации.

Результаты: показана важность проблемы поиска эффективных методов предварительной переработки судебной статистической информации и необходимость оптимизации использования имеющихся вычислительных ресурсов. Проведен обзор существующих методов планирования вычислений. Показано, что универсальные методы распределения нагрузки малоэффективны для конкретных наборов задач, это связано с индивидуальными возможностями распараллеливания задач и особенностями конкретного вычислительного комплекса. Предложен подход к организации системы планирования распределения нагрузки между вычислительными узлами при переработке судебной статистической информации посредством облачных технологий. Показано, что для создания эффективного подхода необходимо обладать информацией о возможностях решения каждой задачи на конкретном наборе аппаратно-программных средств вычислительного комплекса. Для этого в системе планирования реализован алгоритм обучения, который собирает информацию о параметрах вычислительной задачи, имеющихся средствах и требуемых параметрах результатов вычислений. Эта информация формализуется в виде базы моделей переработки и уточняется в процессе решения прикладных задач. Чем больше решенных задач, тем обширнее база моделей и больше вероятность получения решения близкого к оптимальному. Для системы планирования в качестве критерия оптимизации выбрано минимальное время решения задач на выделенном наборе ресурсов. Предполагается, что каждая задача обладает приоритетом и директивным сроком решения, по окончании которого результаты становятся не актуальными.

Показано, что для переработки судебной статистической информации одной из наиболее популярных ресурсоёмких вычислительных задач этого класса является задача поиска заданных сообщений в неструктурированном массиве данных. Планирование заключается в распределении задач наивысшего приоритета по имеющимся ресурсам таким образом, чтобы число решаемых задач было максимальным. Причем для задач не должны быть превышены значения директивного срока решения. Оставшиеся задания распределяются в соответствии с приоритетами по ресурсам по мере их высвобождения. Подход работоспособен в случае изменения конфигурации вычислительных средств как при выходе некоторых из них из строя, так и при подключении отдельных узлов к вычислительному комплексу.

Приведены математические основы формирования моделей планов решения типовых задач. Приведены результаты экспериментальных исследований. Проведена сравнительная оценка разработанного алгоритма с наиболее популярными алгоритмами диспетчеризации и управления вычислениями.

DOI: 10.21681/1994-1404-2018-1-15-22

* **Борисов Роман Сергеевич**, кандидат технических наук, доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.

E-mail: bestseller@bk.ru

Введение

Судебная статистика позволяет решать важнейшие задачи динамического моделирования социально-правовых процессов в обществе и выявлять устойчивые тенденции и закономерности их развития [11]. Важным шагом в сторону решения этих статистических задач является развитие прикладных программных продуктов в рамках Государственной автоматизированной системы (ГАС) РФ «Правосудие», в состав которой входят программные изделия «Судебная статистика» и «Судимость» функциональной подсистемы «Судебное делопроизводство и статистика».

Процесс создания единого информационного пространства судов общей юрисдикции и системы Судебного департамента при Верховном Суде Российской Федерации еще далёк от завершения [12, 14], между тем, объёмы циркулирующей в системе информации постоянно требуют модернизации аппаратной инфраструктуры. На сегодняшний день аппаратная платформа ГАС РФ «Правосудие» представляет собой облачную инфраструктуру с более чем 1,5 тысяч процессорных ядер, совокупной ёмкостью оперативной памяти 31 Тбайт и с возможностью хранения до 1,5 Пбайт информации. Эти вычислительные мощности достаточны для решения текущих задач, однако, необходимо учитывать актуальные задачи создания единого информационного пространства и перспективы формирования более качественной и многоаспектной системы судебной статистики, обеспечивающей динамический анализ автоматически собираемых данных с учетом географической привязки их параметров [10, 13].

Открывающиеся в этой связи перспективы качественного решения важнейших задач судебной статистики сталкиваются с необходимостью переработки огромного количества неструктурированных данных, циркулирующих в судебных информационных системах [6, 7, 9, 10].

Эффективная и своевременная переработка таких массивов возможна исключительно при использовании систем распределенной и параллельной переработки, которые могут быть развернуты на аппаратной платформе ГАС РФ «Правосудие». Эффективность существующей облачной инфраструктуры можно значительно повысить, используя специализированные алгоритмы управления вычислениями без использования бесконечного наращивания вычислитель-

ных мощностей посредством увеличения числа вычислительных ядер и объёма оперативной памяти. Известно, что эффективность использования облачных технологий прямо зависит от того, каким образом распределяется нагрузка между отдельными вычислительными элементами в облаке [9]. Следовательно, задачу эффективного распределения нагрузки вычислительной среды по всем вычислительным задачам, поступающим на переработку, с учетом специфики переработки судебной статистической информации следует считать актуальной и важной.

Задаче распределения вычислительных ресурсов посвящено большое число работ. Существуют работы, связанные с оптимизацией вычислительных ресурсов, которые базируются на:

- знании времени решения задачи до ее выполнения [2];
- оценивании времени выполнения;
- прогнозировании использования ресурсов на основе статистических моделей [1].

Известны подходы к динамическому планированию задач с зависимостями, схемы планирования с использованием предпочтений пользователей и другие [4]. Исследования результативности существующих подходов к планированию [3, 4] показывают, что проблема построения эффективной системы управления вычислительного комплекса далека от решения.

Часто применяемые в планировщиках подходы не учитывают присущих современным высокопроизводительным вычислительным комплексам при решении типовых ресурсоемких задач ряда особенностей, включая:

- различные ресурсные требования для данных задач;
- гетерогенную природу вычислительных сред, являющуюся естественным источником разбалансировки нагрузки;
- отсутствие, как правило, полной информации о ресурсных потребностях конкретных задач;
- возможное изменение конфигурации вычислительных средств в процессе решения задач.

Учет данных факторов приводит к усложнению задач выбора стратегии управления вычислительным комплексом и делает весьма актуальными вопросы поиска новых методов планирования распределения вычислительных ресурсов по задачам [8]. Очевидно, что точное распределение ресурсных возможностей по задачам уменьшит время переработки информации и повысит эффективность электронной переработки в целом [4].

Требуется разработать механизмы планирования, учитывающие данную особенность перераспределения ресурсов. Предлагаемый подход основан на динамическом перераспределении вычислительных ресурсов на основе прогнозной оценки времени выполнения задач с учетом директивного срока решения и приоритетов отдельных заданий.

Общая схема организации вычислений

На вход вычислительного комплекса поступает пакет из n однотипных статистических задач, каждая из которых представлена комплектом идентичных элементарных заданий, различающихся набором исходных данных. Общая структура схемы переработки статистической информации в вычислительном комплексе представлена на рис. 1.

Для каждой i -й задачи существует набор заранее рассчитанных планов распределения ресурсов, упорядоченный по времени решения. В качестве ресурсов комплекса выступают вычислительные элементы, представляющие однозначно адресуемые структурные единицы, входящие в

состав вычислительного устройства и предназначенные для выполнения вычислений независимо от других элементов. В качестве вычислительных элементов в инфраструктуре ГАС РФ «Правосудие» выступают отдельные виртуальные процессорные ядра. Система управления вычислениями формирует общий план распределения вычислительных элементов, минимизирующий время решения пакета из n задач, и отправляет задания на переработку.

В процессе вычислений поступает запрос на исполнение новой задачи. Система управления вычислениями посредством динамической реконфигурации вычислительного комплекса высвобождает часть вычислительных ресурсов для решения новой задачи с учетом приоритета и директивного срока решения каждой из задач. Под *динамической реконфигурацией* в данном случае понимается выделение части ресурсов вычислительного комплекса для решения новой задачи без остановки выполнения предыдущих. *Директивный срок решения* — максимально допустимое время решения задачи, назначенное при ее формировании.

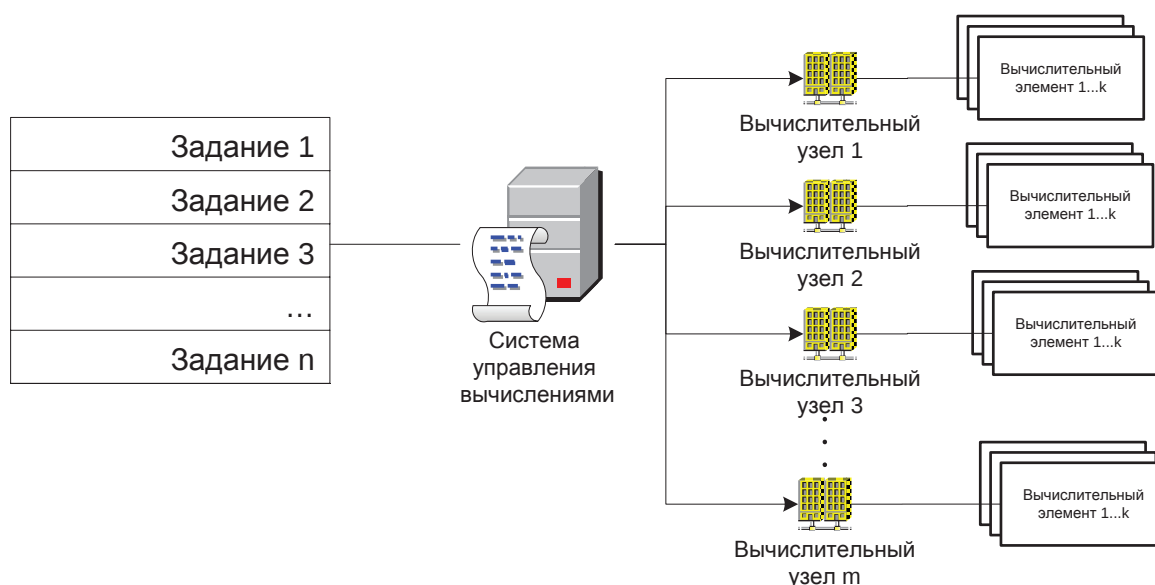


Рис. 1. Схема выполнения заданий в вычислительном комплексе

Планирование распределения вычислительных задач

При планировании распределения загрузки вычислительного комплекса введем следующие допущения:

распределение нагрузки осуществляется на прикладном уровне;

издержки на коммуникацию между вычислительными узлами значительно ниже времени решения элементарных задач;

для каждой поступающей задачи известен директивный срок ее решения, после которого исполнение задачи теряет смысл.

Предположим, что на вход вычислительного комплекса поступили прикладные ресурсоемкие

задачи $\hat{a}_1, \hat{a}_2, \dots, \hat{a}_n$. Каждая из задач декомпозируется на ряд элементарных заданий $H_{\hat{a}_i}$ (i — номер задачи). Задача $\hat{a}_i$ имеет директивный срок решения $D_{\hat{a}_i}$, задаваемый при поступлении, и известный расчетный срок их исполнения на имеющемся множестве вычислительных ресурсов $\tau_{\hat{a}_i}^r$ (r — вектор множества ресурсов).

Величина $\Delta = D_{\hat{a}_i} - \tau_{\hat{a}_i}^r$ показывает имеющийся запас по времени решения задачи, который может использоваться для оптимизации применения вычислительных ресурсов. Задача считается выполнимой, если максимальное значение времени выполнения задачи на множестве вычислительных ресурсов $\tau_{\hat{a}_i}^r$ не превысит директивный срок решения $D_{\hat{a}_i}$. В процессе выполнения задач выявляется необходимость решения новой задачи $\hat{a}_{n+1}$ с аналогичным или более высоким приоритетом и ожидаемым временем завершения $\tau_{\hat{a}_{n+1}}$.

Существующие подходы к разрешению подобных ситуаций включают два сценария [6]. *Первый* предполагает игнорирование новой задачи до завершения вычислений; *второй* основан на выполнении комплекса мероприятий прерывания вычислений, включающего операции сохранения результатов промежуточных вычислений по задаче $\hat{a}_i$, создания точки восстановления и др. В дальнейшем производится реконфигурация вычислительного комплекса под решение задачи $\hat{a}_{n+1}$, загрузка данных задачи $\hat{a}_{n+1}$ и проведение вычислений. По завершению вычислений по задаче $\hat{a}_{n+1}$ проводятся операции, необходимые для завершения выполнения задачи $\hat{a}_i$, аналогичные представленным выше.

Очевидно, что при значительных сроках выполнения задачи $\hat{a}_i$ *второй* подход — наиболее предпочтительный, однако возникающие накладные расходы по затратам времени на прекращение и возобновление вычислений могут составлять до 50 % и более от времени решения задачи [4].

В подобных ситуациях предлагается использовать подход, основанный на динамическом сокращении ресурсов вычислительного комплекса, используемых для текущей вычислительной задачи без останова ее выполнения и перераспределения высвобождающихся ресурсов на новую возникшую задачу в реальном времени. Перераспределение вычислительных ресурсов происходит на основе прогнозной оценки времени выполнения задач с учетом директивного срока решения и приоритетов отдельных заданий. Фактически, вычислитель-

ная среда динамически разделяется на два и более кластера, каждый из которых оптимизирован в части состава аппаратных средств на решение своей прикладной задачи.

Предлагаемый подход основан на уменьшении объема ресурсов вычислительного комплекса, используемых для текущей вычислительной задачи в пределах директивного срока её решения. Полученный резерв ресурсов перераспределяется на новые задачи в реальном времени с учетом заданных приоритетов задач. Для проведения оптимизации необходимо сформировать базу данных значений времени выполнения типовых задач на множестве вычислительных ресурсов $\tau_{\hat{a}_i}^r$.

Формирование базы моделей

Основная трудность при планировании работ — выбор оптимизированного состава вычислительных средств, достаточного для обеспечения выполнимости конкретной прикладной задачи в заданные сроки.

База данных, содержащая комплекс типовых эффективных моделей решения задачи, формируется в процессе решения задач вычислительным комплексом следующим образом. Необходимо оценить время, затрачиваемое на решение одной задачи с учетом производительности вычислительных средств. Каждую из задач $\hat{a}_i$ можно охарактеризовать набором параметров

$$\hat{a}_i = (c_{\hat{a}_i}, m_{\hat{a}_i}, t_{\hat{a}_i}, H_{\hat{a}_i}, w_{\hat{a}_i}, \rho_{\hat{a}_i}),$$

где $c_{\hat{a}_i} \in N$ — число вычислительных средств из общего множества доступных N , выделенных для решения задачи $C_1, \dots, C_N$ [5]; $m_{\hat{a}_i} \in K$ — объем оперативной памяти, запрашиваемый для исполнения каждой подзадачи, K — общий объем доступной памяти; $\tilde{t}_{\hat{a}_i} \in N$ — оценка времени решения задачи на вычислительных средствах с единичной относительной производительностью; $H_{\hat{a}_i}$ — набор параллельных элементарных заданий в рамках задачи; $w_{\hat{a}_i}, \rho_{\hat{a}_i}$ — тип и приоритет задачи, соответственно.

Элементарные задания $H_{\hat{a}_i}$ запускаются локальным планировщиком на всех выделенных вычислительных средствах одновременно. Те ресурсы, которые выделяются для текущей задачи, будут освобождены при завершении всех ее процессов. Для вычисления оценки времени $\tau_{\hat{a}_i}^r$ решения задачи при условии учета производительности вычислительных средств, которые выделены планировщиком, используется формула:

$$\tau_{\hat{a}_i}^r = \frac{\tilde{t}_{\hat{a}_i}}{\min_{(k,r) \in A_{\hat{a}_i}} S_{kr}^n}, \quad (1)$$

где $A_{\hat{a}_i}$ — множество вычислительных средств, назначенных системой управления вычислениями задаче $\hat{a}_i$; S_{kr}^n — относительная производительность комплекса вычислительных средств, показывающая, во сколько раз быстрее работает набор вычислительных средств по сравнению с наименее производительным вычислительным элементом.

Используя выражение (1), можно оценить время выполнения прикладной задачи для любой комбинации вычислительных средств вычислительного комплекса.

Сформированный таким образом кортеж

$$L_{\hat{a}_i} = \langle S_{kr}^n, \tau_{\hat{a}_i}, w_{\hat{a}_i}, \rho_{\hat{a}_i} \rangle \quad (2)$$

содержит данные о наборе вычислительных средств S_{kr}^n , необходимом для ее решения в пределах директивного срока выполнения, расчетном времени выполнения задачи $\tau_{\hat{a}_i}$, типе задачи $w_{\hat{a}_i}$ и ее приоритете $\rho_{\hat{a}_i}$.

При планировании используется частично вытесняющая стратегия, которая основана на прерывании задачи при появлении более приоритетной. Перепланирование возможно в строго определенные интервалы времени, которые соответствуют этапам вычислений ресурсоемкой задачи.

Общая продолжительность выполнения задач с учетом сформулированного подхода, включающего остановку хода их решения для реконфигурации вычислительного комплекса и обслуживания более приоритетных задач, может быть определена выражением

$$\tau_{\hat{a}_i}^r = \tau_{\hat{a}_i} + J^r + \sum_{j=hp(i)} F^r, \quad (3)$$

где J^r — время, необходимое для реконфигурации; $\sum_{j=hp(i)} F^r$ — сумма длин интервалов ожидания выполнения более приоритетных задач, $j = hp(i)$ — множество задач с приоритетом не ниже, чем у задачи $\hat{a}_i$.

Таким образом, общая продолжительность складывается из времени выполнения самой задачи $\tau_{\hat{a}_i}$, суммы длин интервалов, когда задача ожидает выполнения более приоритетных $\sum_{j=hp(i)} F^r$, а также времени J^r , необходимого для реконфигурации, включая время ожидания планового момента проведения реконфигурации, время прерывания вычислений и время для нового запуска задач.

Описание процесса планирования

Приведем общий алгоритм планирования заданий на основе сформированных моделей вычислений (1) — (3). На входе системы планирования формируется очередь заданий для перспек-

тивного решения. Из очереди выбираются задачи с наивысшим приоритетом. Компаратор проверяет наличие набора готовых типовых решений для данных заданий с известным временем решения, и в случае его отсутствия, передает задание в моделирующий комплекс, который запускает процесс формирования моделей с учетом директивного срока решения. По готовым наборам задач формируется модель реконфигурации вычислительного комплекса, включающая плановые моменты времени проведения реконфигурации и оптимизированные планы распределения вычислительных ресурсов с учетом приоритетов задач.

При формировании модели перераспределения задач по имеющимся ресурсам система руководствуется следующими правилами:

1) выбирается максимальное число задач с наивысшими приоритетами, которое может быть решено на данном наборе вычислительных средств с гарантией соблюдения директивных сроков их исполнения;

2) если после данного выбора очередь задач пуста, проводится распределение задач по вычислительным ресурсам, начиная с наименее приоритетных, оставляя, таким образом, приоритетным задачам максимальный набор ресурсов.

Основным критерием эффективности решения задач планирования распределения ресурсов следует считать минимизацию времени выполнения задач на выделенном наборе ресурсов [4]. Предложенный подход к распределению нагрузки вычислительного комплекса — основа для функционального наполнения некоторых программных средств диспетчеризации и управления.

Оценка эффективности алгоритма планирования с динамической балансировкой

Для проведения экспериментальных исследований предложенного подхода реализована программа формирования моделей переработки, позволяющая накапливать общую статистику по комплексам типовых моделей решения прикладных задач в соответствии с формулой (2) на различных комбинациях вычислительных средств [5]. В дальнейшем, сформированная база типовых решений использована для планирования выполнения потока заданий на вычислительном комплексе.

В качестве типовой выступает задача поиска заданных сообщений в неструктурированном массиве данных. Задача содержит комплект, включающий от 2^{18} до 2^{24} элементарных заданий, которые отличаются друг от друга только исходными

данными. Общее число типовых задач для перспективного решения — 100. Из типовых задач было скомпоновано 30 псевдослучайных наборов. Для каждого из наборов оценивалось время решения при использовании различных алгоритмов планирования. Для наглядности в таблице приведены пять первых наборов.

Сравнение разработанного алгоритма проводилось с двумя наиболее популярными мето-

дами балансировки нагрузки вычислительного комплекса — алгоритмом *RR* (*Round Robin*) и алгоритмом *TLB* (*Throttled Load Balancing*). В таблице и последующих рисунках, данные, относящиеся к разработанному алгоритму динамической балансировки обозначены синим цветом, к алгоритму *Round Robin* — серым, а алгоритму *Throttled Load Balancing* — желтым.

Таблица

Время решения пакета задач при использовании различных алгоритмов планирования

Номер набора	Алгоритм планирования		
	с динамической балансировкой, с	RR, с	TLB, с
1	32183,18	42348,16	36463,23
2	34226,17	40538,65	38435,98
3	25677,34	39523,46	34279,17
4	36273,38	41384,25	37328,33
5	29163,45	40372,31	35172,14

Результаты оценки времени вычислений для всех 30 наборов приведены на рис. 2.

В результаты анализа не включён вариант проведения вычислений без использования механизмов балансировки нагрузки, который значительно увеличивает время проведения вычислений на всех наборах задач.

Анализ приведенных на рис. 2 зависимостей показывает значительное повышение скорости вычислений алгоритма динамической балансировки по сравнению с алгоритмом *RR*. Между тем

на двух комбинациях, 8 и 12, алгоритм *RR* показал лучшие результаты, хотя в этом случае сокращение времени вычислений было незначительным. Последующий анализ результатов показал, что на данных наборах состав задач для решения на конкретных вычислительных средствах был близок к оптимальному для алгоритма *RR*. Использование алгоритма *TLB* также показывает прирост скорости вычислений по сравнению с *RR*, однако это увеличение несколько ниже, чем при использовании алгоритма с динамической балансировкой.

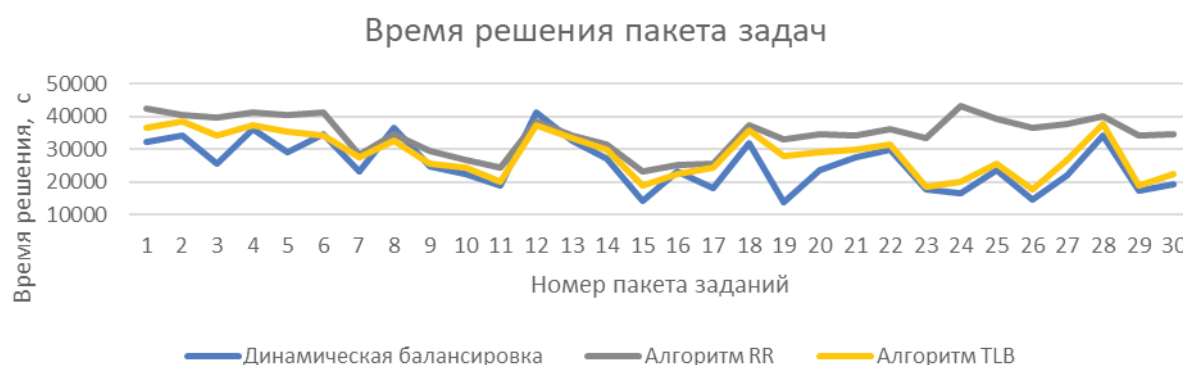


Рис. 2. Оценка времени решения задач для различных наборов

Поскольку в зависимости от конкретного набора задач изменение производительности отклоняется довольно значительно, более объективной

будет оценка среднего значения времени проведения вычислений. Для 30 представленных наборов задач среднее время решения представлено

на рис. 2. Из рисунка видно, что сокращение среднего времени вычислений при использовании метода динамической балансировки составляет до 36% по сравнению с алгоритмом *RR* и более 11% по сравнению с алгоритмом *TLB*, что говорит

о достаточно неплохих перспективах применения разработанного алгоритма. Сокращение времени вычислений достигается за счет более рационального распределения задач по имеющимся ресурсам.

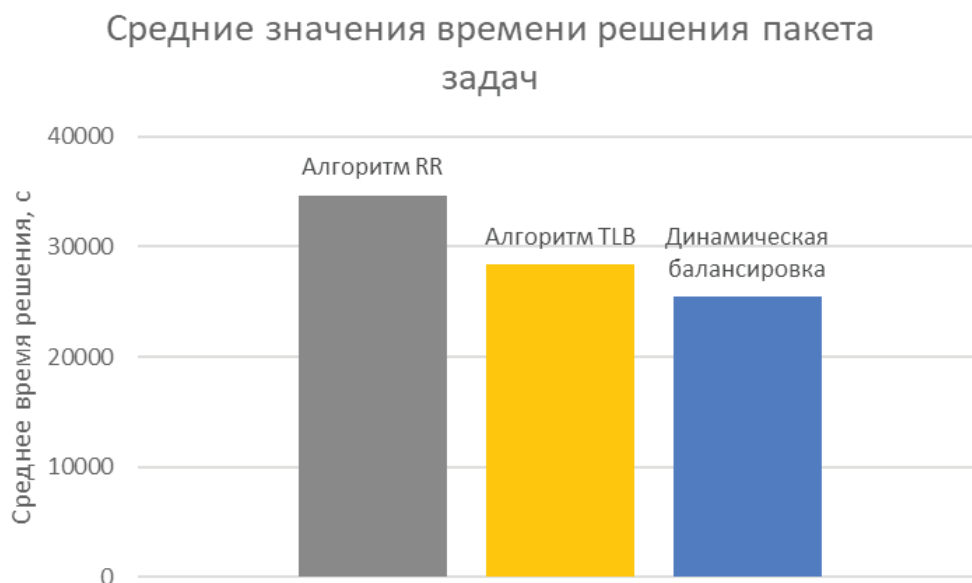


Рис. 3. Среднее значение времени вычислений для 30 наборов задач

Заключение

Одна из важнейших задач реализации параллельных вычислений в системах переработки судебной статистической информации — оптимизация распределения нагрузки между вычислительными узлами. Универсальные методы распределения малоэффективны для конкретных наборов задач, что приводит к необходимости разработки частных подходов, учитывающих специфику заданий, выполняемых вычислительным комплексом.

Разработанный алгоритм организации системы динамического распределения нагрузки между узлами вычислительного комплекса на основе приоритетов и директивных сроков решения задач обеспечивает эффективную переработку статистической информации в предположении, что параметры задачи, вычислительных средств и результатов вычислений априорно известны. При этом первоначально задачи распределяются по принципу минимизации времени их решения

на имеющихся наборах вычислительных средств; с приходом новой задачи происходит динамическая реконфигурация вычислительного комплекса, уменьшающая число вычислительных средств, задействованных для выполнения задач таким образом, чтобы директивное время их выполнения не превышало заданное.

Экспериментальные исследования разработанного алгоритма планирования с динамической балансировкой подтвердили его существенное быстроедействие по сравнению с известными алгоритмами *RR* и *TLB*, что обусловлено рациональным оперативным распределением заданий переработки между вычислительными ресурсами.

В дальнейшем представляется целесообразным исследовать устойчивость предложенного подхода к различным вариантам реконфигурации вычислительного комплекса в процессе выполнения задач и определить вероятностные меры их успешного завершения.

Рецензент: **Федосеев Сергей Витальевич**, кандидат технических наук, доцент, доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва
E-mail: fedsergvit@mail.ru

Литература

1. Neural Network and Regression Based Processor Load Prediction for Efficient Scaling of Grid and Cloud Resources, M. T. Imam et al., 14th Intern. Conf. on Computer and Information Technology (ICCIT), IEEE, 2011, pp. 333-338.
2. Performance Evaluation and Optimization of an Adaptive Scheduling Approach for Dependent Grid Jobs with Unknown Execution Time, M. Chtepen et al., 18th World IMACS / MODSIM'09 Congress. Cairns, Australia 13-17 July 2009, pp. 1003-1009. URL: <http://www.mssanz.org.au/modsim09/C5/ghtepen.pdf> (дата обращения: 12.02.2018).
3. Астриков Д. Ю., Кузьмин Д. А. Исследование методов оценки эффективности вычислительных систем на основе функциональных моделей // Вестник Сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнева. 2016. Т. 17. № 2. С. 295—301.
4. Борисов Р. С. Черных А. М. Динамическая балансировка нагрузки гетерогенной вычислительной системы // Вестник компьютерных и информационных технологий. 2017. № 10. С. 28—34.
5. Борисов Р. С. Аппаратно-ориентированная модель взаимодействия открытых систем // Электротехнические и информационные комплексы и системы. 2011. Т. 7. № 1. С. 21—25.
6. Ващекин А. Н., Ващекина И. В. Информационное право: прикладные задачи и математические методы // Информационное право. 2017. № 3. С. 17—21.
7. Ващекин А. Н., Ващекина И. В. Информационно-программное обеспечение рационального распределения судебных дел // Правовая информатика. 2017. № 4. С. 24—30.
8. Ефименко А. А. Интегрированная интеллектуальная технология оптимизации параллельных алгоритмов в высокопроизводительных вычислительных системах // Труды Междунар. науч.-практ. конф. «Современные тенденции в науке, технике, образовании» (31 января 2016 г.). Смоленск: «Новаленсо», 2016. С. 59—61.
9. Королев В. Т., Ловцов Д. А., Радионов В. В. Системный анализ. Часть. 2. Логические методы / Под ред. Д. А. Ловцова. М.: РГУП, 2017. 160 с.
10. Ловцов Д. А., Богданова М. В., Паршинцева Л. С. Пакеты прикладных программ для многоаспектного анализа судебной статистической информации // Правовая информатика. 2017. № 1. С. 28—36.
11. Ловцов Д. А., Богданова М. В., Паршинцева Л. С. Правовая статистика преступности в современных условиях // Правовая информатика. 2017. № 4. С. 40—48.
12. Ловцов Д. А., Нисов В. А. Актуальные проблемы создания и развития единого информационного пространства судебной системы России // Информационное право. 2013. № 5. С. 13—18.
13. Ловцов Д. А., Черных А. М. Модернизация системы судебной статистики на основе новой геоинформационной технологии // Правовая информатика. 2016. № 1. С. 7—14.
14. Чубукова С. Г. Стратегии развития информационного общества и направления развития законодательства // Правовая информатика. 2017. № 2. С. 67—72.

ОБМЕН ИНФОРМАЦИЕЙ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ЮРИСТА: ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ КОММУНИКАТИВНОЙ ДЕЯТЕЛЬНОСТИ

Ващекин А.Н., Шевченко Д.И.*

Ключевые слова: юрист, респондент, коммуникативная деятельность, информационное взаимодействие, наблюдение, опрос, экспертные оценки, показатель, параметр, информационная модель, диаграмма.

Аннотация.

Цель работы: исследование коммуникативных качеств, которыми следует обладать юристу, включающих способность устанавливать и поддерживать контакт с респондентом, умение преодолевать психологические барьеры в процессе общения, способность адекватно оценивать личность собеседника и собственное поведение, реагировать на складывающиеся обстоятельства в процессе обмена информацией, владеть вербальными и невербальными средствами общения.

Методы: наблюдение, социологический опрос; экспертные оценки, сглаживаемые вычислениями, проводимыми на основе анализа иерархий.

Результаты: обосновано введение понятия коммуникативной деятельности (профессионального общения) юриста в широком смысле слова, под которым понимается процесс установления и развития взаимодействия между юристом и любым респондентом, содержанием которого являются: обмен информацией, достижение взаимопонимания, оказание мотивообразующего воздействия на респондента с целью вовлечения последнего в совместную деятельность.

Исследование показало, что глобальная информатизация и широкое внедрение информационно-компьютерных средств, ресурсов, технологий, порождающие изменения общественно-производственных отношений, не снижают актуальности для практикующего юриста традиционных форм информационного обмена, и прежде всего речевой коммуникативной деятельности. Поэтому при целенаправленном повышении общего уровня информационной подготовки практикующих юристов следует дополнять имеющиеся методики комплексным освоением правил информационного взаимодействия.

DOI: 10.21681/1994-1404-2018-1-23-31

Владение навыками коммуникации и умение успешно применять их в организации труда, обеспечения взаимодействия с коллегами и получения достоверной информации значительно улучшают результаты работы деятельности специалиста практически любой профессии. Развитие современного общества выдвигает высокие требования к психологической организации, интеллекту, личностным качествам лица, занятого юридической деятельностью. **Для юриста коммуникативная деятельность является «краеугольным**

камнем» успешного владения профессией, обеспечивая его эффективным инструментом воздействия на информационную среду.

Коммуникативные качества, которыми следует обладать юристу, включают способность устанавливать и поддерживать контакт с респондентом, умение преодолевать психологические барьеры в процессе общения, способность адекватно оценивать личность собеседника и собственное поведение, реагировать на складывающиеся обстоятельства в процессе обмена информацией, владеть вербальными и невербальными средствами общения.

* **Ващекин Андрей Николаевич**, кандидат экономических наук, доцент, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.

Email: vaschekin@mail.ru

Шевченко Дарья Ивановна, юрист, ООО «Нефтемашсервис-С», Российская Федерация, г. Москва.

Email: dasha1212sheva@mail.ru

При изучении особенностей профессионального общения юриста обычно отмечают, что это общение, как правило, носит официальный характер, а иногда ведется в строго регламентированных рамках, установленных законом. Юристу приходится взаимодействовать с гражданами, принадлежащими к разным социальным, возрастным, национальным группам. Среднестатистический юрист в основном контактирует с респондентами особого рода — правонарушителями, подозреваемыми, свидетелями и др. В этих обстоятельствах он обладает некоторыми властными полномочиями по отношению к собеседнику, и может оказывать на него психологическое воздействие, что в свою очередь легко может привести к конфликту, поскольку цели, преследуемые сторонами общения, могут кардинально отличаться. Психическое, эмоциональное состояние участников постоянно меняется, часто им присуще нервное напряжение, агрессия [12].

Однако профессиональное общение юристов отнюдь не сводится к контактам лишь с участниками правонарушения. Им приходится вступать в контакт с различными должностными лицами, руководителями, сослуживцами, оперативными сотрудниками. Такое информационное взаимодействие называют *не процессуальным* общением, происходящим в рамках профессиональной деятельности. Итак, мы приходим к осознанию понятия коммуникативной деятельности (профессионального общения) юриста в широком смысле слова. Под ним следует понимать процесс установления и развития взаимодействия между юристом и любым респондентом, содержанием которого являются: обмен информацией, достижение взаимопонимания, оказание мотивообразующего воздействия на респондента, с целью вовлечения последнего в совместную деятельность.

Профессиональное общение юриста имеет свои функции, включающие информационно-коммуникативную, регулятивно-коммуникативную и аффективно-коммуникативную. Основной профессиональной задачей коммуникативной деятельности юриста следует считать достижение уровня интерактивного общения, который можно охарактеризовать как совместную деятельность, направленную на достижение общих целей [2].

Базовым предприятием для экспериментального изучения особенностей и выявления закономерностей коммуникативной деятельности юриста было выбрано московское ООО «Нефтемашсервис-С» — одна из типичных достаточно крупных московских компаний. Юридиче-

ский отдел компании, сотрудники которого приняли активное участие в эксперименте, занимается консультированием и сопровождением сделок, заключением договоров, решением судебных и арбитражных споров.

«Нефтемашсервис-С» — это независимая и успешная энергосбытовая компания, которая является субъектом розничного рынка электроэнергетики и осуществляет деятельность по энергоснабжению и поставке электрической энергии потребителям на основании Федерального закона от 26 марта 2003 г. №35-ФЗ «Об электроэнергетике», предусматривающего *принцип свободы выбора* покупателем электрической энергии поставщика (по договору энергоснабжения, договору купли-продажи либо договору поставки электрической энергии), и Правил функционирования розничных рынков электрической энергии, утвержденных Постановлением Правительства Российской Федерации от 31 августа 2006 г. № 530, устанавливающих *принцип альтернативного (конкурентного) обслуживания* покупателей энергосбытовыми организациями. К клиентам компании относятся объекты Министерства обороны Российской Федерации, другие потребители бюджетной сферы, коммерческие предприятия и население.

Современные системные методики экспериментального исследования предполагают обязательное сравнение, сопоставление получаемых данных, продуктивное сочетание *неформализованных* (к которым относятся наблюдение, опросы, беседы) и *формализованных* методов (включающих логическую обработку тестов, анкет, интервью, проективных и психофизиологических обследований).

В зависимости от способов предъявления материала и вспомогательных средств выделяют различные типы тестов: выполняемые индивидуально или группой; *вербальные* (осуществляемые в словесно-логической форме) или *невербальные* (представленные чертежами, графиками, пиктограммами и диаграммами). По типам выделяют тесты интеллекта, способностей, достижений, личностные, а также тесты познавательных процессов.

В качестве основных методов проведения экспериментального исследования в компании «Нефтемашсервис-С» использовались, главным образом, наблюдение, опрос и экспертные оценки.

Наблюдение играет важную роль в любом исследовании, поскольку только этим способом

можно достичь целенаправленного и организованного восприятия поведения изучаемого объекта. Важное обстоятельство: при ведении наблюдения следует минимизировать вмешательство наблюдателя в процесс взаимодействия наблюдаемого юриста с респондентом. Метод наблюдения обеспечивает полноценную оценку происходящего, понимание мотивов поведения взаимодействующих субъектов, однако сам по себе также субъективен. Наблюдение происходит в ходе разнообразных опросов, анкетирования, обсуждения документов. Результаты наблюдения отражаются в специальных протоколах.

Метод *опроса* заключается в сборе информации, получаемой в виде ответов на серию упорядоченных вопросов. Это один из самых распространенных методов в психологических, социологических и экономических исследованиях [1]. Ответы опрашиваемого позволяют исследователю получить сведения, являющиеся важными в соответствии с целями и задачами исследования [11]. Поэтому при создании опроса, как правило, сначала формулируются эти цели и задачи, выделяются вопросы, соответствующие их решению, а также вопросы, маскирующие цели и задачи исследователя для опрашиваемого лица, чтобы устранить попытки угадать и помочь «правильными» ответами [9].

Эффективность метода опроса зависит от того, насколько исследователю удастся избежать таких проблем, как неполучение ответа на поставленные вопросы, ошибок в ответах, сознательных искажений. Ответы, которые не отражают истинных убеждений опрашиваемых, могут значительно изменить результаты опроса. Такие обстоятельства могут возникнуть ненамеренно, будучи спровоцированными неправильными формулировками вопросов, но могут оказаться и сознательным действием со стороны испытуемого, который пытается ввести в заблуждение наблюдателя с целью изменить ход исследования [6]. Важной ошибкой исследователя может стать неправильный охват зоны наблюдения. Выбирать людей для наблюдения нужно в определенном количестве, также необходимо учитывать и качественные признаки (например, пол и возраст), поэтому массовость опроса не всегда гарантирует успех [4].

То же касается и метода *экспертных оценок*, поскольку при отсутствии средств однозначного измерения эксперт всегда оперирует нечеткой информацией [10]. Доверять мнению одного эксперта можно только с поправкой на субъективный

характер оценки, часто искажающий реальную картину вплоть до обратного значения. Поэтому в исследовании следует задействовать нескольких экспертов, а для выработки согласованного решения применять метод анализа иерархий [3].

С формальной стороны усреднение мнения нескольких экспертов выглядит следующим образом. Пусть $X = \{\tilde{o}_1 \dots \tilde{o}_n\}$ — множество результатов, полученных попарными сравнениями результатов коммуникативной деятельности юристов, занятых в исследовании. Группе экспертов необходимо найти вектор приоритетов $\omega = (\omega_1, \dots, \omega_n)^{\tilde{O}}$, где $\tilde{O}$ — операция транспонирования, который определит степень их «важности».

Обозначив как a_j число, соответствующее значимости i -го элемента по сравнению с j -ым по мнению эксперта, мы получаем квадратную обратносимметричную матрицу A размера $n \times n$.

Если суждение эксперта совершенно при всех сравнениях, то $a_k = a_j a_k$ для всех i, j, k , и матрица A является согласованной.

В случае точных измерений для согласованной матрицы

$$a_j = \frac{\omega_i}{\omega_j}, \quad i, j = 1, \dots, n, \quad \text{и} \quad \text{поэтому} \\ a_j a_k = \frac{\omega_i}{\omega_j} \frac{\omega_j}{\omega_k} = \frac{\omega_i}{\omega_k} = a_k.$$

В случае нечетких (полученных экспертным путем) измерений ω является собственным вектором матрицы A с собственным значением n :

$$\begin{pmatrix} \omega_1/\omega_1 & \omega_1/\omega_2 & \dots & \omega_1/\omega_n \\ \omega_2/\omega_1 & \omega_2/\omega_2 & \dots & \omega_2/\omega_n \\ \vdots & \vdots & \dots & \vdots \\ \omega_n/\omega_1 & \omega_n/\omega_2 & \dots & \omega_n/\omega_n \end{pmatrix} \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = n \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}$$

В этом случае величины a_j будут в некоторой степени отклоняться от «идеальных» отношений $\frac{\omega_i}{\omega_j}$.

В случае согласованности n — есть наибольшее собственное значение матрицы A (из теории матриц известно, что все собственные значения такой матрицы равны нулю, за исключением одного, равного n).

Если элементы a_j положительной обратносимметричной матрицы A незначительно изменить, то собственные значения также изменятся незначительно [13].

Поэтому, если диагональ матрицы A состоит из единиц ($a_j = 1$) и A - согласованная матрица, то при малых изменениях в a_j наибольшее собственное значение λ_{max} остаётся близким к n , а остальные собственные значения - близкими к нулю.

В связи с этим приемлемое значение вектора приоритетов ω можно искать как решение следующей задачи: если A — матрица значений парных сравнений, то для нахождения вектора приоритетов нужно найти такой ω , который удовлетворяет условию:

$$A\omega = \lambda_{max}\omega,$$

т.е. вектор ω , представляет собой собственный вектор матрицы A , соответствующий собственному значению λ_{max} .

Для нормализации решения слегка изменим ω , полагая $\alpha = \sum_{i=1}^n \omega_i$ и заменяя ω на $\frac{1}{\alpha}\omega$. Это обеспечивает *единственность* решения, а также то, что $\sum_{i=1}^n \omega_i = 1$.

Так как малые изменения в a_j вызывают малое изменение λ_{max} , отклонение последнего от n является мерой согласованности. Поэтому индекс $\delta = \frac{\lambda_{max} - n}{n - 1}$ можно рассматривать как

показатель «близости к согласованности». Если этот индекс достаточно мал, например $\delta \leq 0,1$, мы можем быть удовлетворены суждениями эксперта. Подобные методики нахождения согласованного решения активно используются при решении разнообразных задач моделирования [14].

Использование рассмотренных методических основ в проведенном экспериментальном исследовании позволило получить обоснованные результаты в виде совокупности диаграмм, отражающих пропорции (в %) наблюдаемых показателей и параметров. На первом этапе исследования было проведено наблюдение за участниками, далее — выявление субъективного мнения по тем же параметрам в форме опроса.

Результаты собственно наблюдения за участниками экспериментального исследования, возраст которых составил 30 — 40 лет (половина из них — женщины), фиксировались в персональной реляционной (табличной) информационной модели коммуникативной деятельности специалиста. Пример заполнения такой модели приведен в таблице.

Рассмотрим подробнее полученные результаты (см. таблицу).

Таблица
Информационная модель коммуникативной деятельности юриста

Вопросы	Результат наблюдения	Представление сотрудника о себе
Частота речевого устного общения во время выполнения служебных обязанностей - часто/средне/мало	часто	часто
Частота устного речевого общения по телефону во время выполнения служебных обязанностей - часто/средне/мало	часто	средне
Частота письменного речевого общения (электронная почта, смс и т.д.) - часто/средне/мало	мало	средне
Как проще общаться по телефону или вживую - по телефону/и так и так не сложно/вживую	«вживую»	и так, и так не сложно
Как проще общаться - с помощью устной или письменной речи? - с помощью устной речи/ и так и так не сложно/ с помощью письменной речи	устной	устной
Быстрота произношения - быстро/средне/медленно	средне	быстро
Громкость голоса - громко/средне/тихо	средне	средне
Использование пауз в речи - часто/иногда/почти не использую	иногда	часто
Использование слов-паразитов - часто/иногда/почти не использую	почти не использует	иногда; часто
Сколько требуется времени, чтобы подобрать нужное слово - много времени (часто забываю нужные слова)/ не очень много времени/ почти не нужно время	много времени	быстро

Юристы довольно часто используют устную речь в профессиональной деятельности, что еще раз подчеркивает важность нашего исследования. Частота устного общения работников юридического отдела по телефону по результатам наблюдения чуть ниже — 17% участников общаются часто, а 83% участников — со средней частотой. Письменной речью работники пользуются реже, чем устной.

Было проведено наблюдение за тем, каким образом юристам компании легче достигать взаимопонимания с участниками общения — по телефону или «вживую». Оказалось, что 50% участников проще общаться, когда они видят собеседника, а 50% — удобно общаться как по телефону, так и лично.

Следующий измеряемый показатель касался удобства общения с помощью устной или письменной речи: 67%-м участников проще общаться с помощью устной речи (по телефону или «вживую»), 17% испытуемых проще общаться с помощью письменной речи, а 16% — просто общаться и с помощью устной речи, и с помощью письменной речи.

Далее была проведена оценка быстроты произношения при вербальном общении сотрудников юридического отдела: 50% испытуемых говорят со средней быстротой, 33% — быстро, 17% — медленно. Параметр громкости голоса имеет следующие показатели: 67% испытуемых говорят со средней громкостью, 17% — громко, 16% — тихо.

Участники наблюдения в основном говорили по телефону или при личном контакте со средней громкостью голоса, один участник говорил очень

громко; создавалось впечатление, что он раньше работал там, где было необходимо сильно повышать голос. Один человек разговаривал очень тихо.

Следующий этап наблюдений позволил оценить наличие пауз в речи юристов: 50% испытуемых используют паузы иногда, 17% — часто, 33% практически не используют паузы в речи.

Проверка на использование слов-паразитов в речи дала следующий результат: 67% испытуемых почти не используют подобных слов при общении с клиентами, 17% — используют их часто и 16% — иногда.

Почти 83% испытуемых нужно много времени, чтобы подобрать нужное слово, а 17% - на это времени практически не затрачивает.

Далее, в соответствии с планом исследования, результаты наблюдения были сопоставлены с результатами опроса самих сотрудников по тем же показателям и параметрам.

Первые три показателя, оценивающие частоту устного и письменного общения сотрудников юридического отдела с клиентами, в целом совпадают по результатам наблюдения и самоотчета. Однако по четвертому показателю самоотчет испытуемых юристов отличается от результатов наблюдения.

Как видно из построенной по результатам экспериментального анализа диаграммы (рис. 1), большинство участников эксперимента считают, что им просто общаться и по телефону и лично, однако результаты наблюдения это не подтверждают.

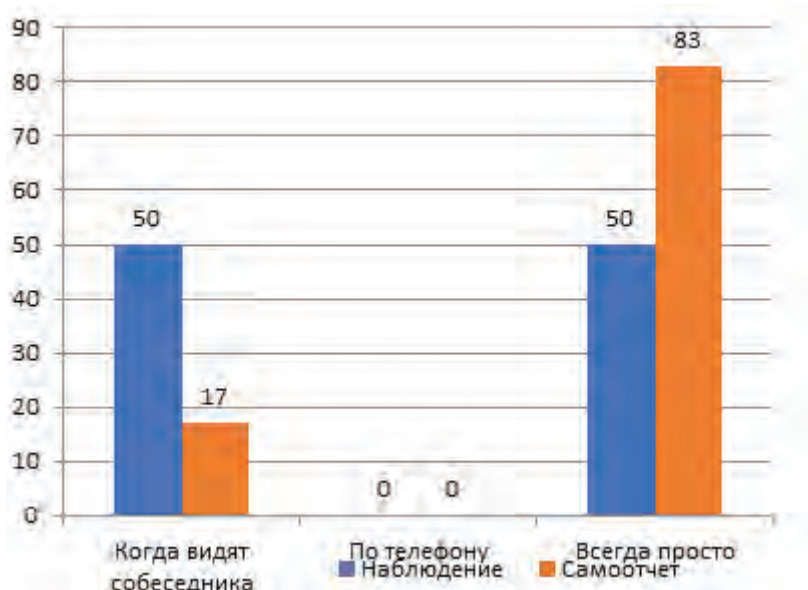


Рис. 1. Общение с клиентами по телефону или лично

Информационные и электронные технологии в правовой сфере

Практически такой же результат можно увидеть при анализе показателя простоты общения с помощью письменной и устной речи (рис. 2). Однако в современном мире большинство клиентов сначала обращаются за консультацией по телефо-

ну, а по результатам данной консультации принимают решение о выборе помогающей организации. Именно поэтому для увеличения количества клиентов необходимо развивать навыки общения сотрудников по телефону.



Рис. 2. Письменное или устное общение с клиентами

Следующий анализируемый параметр — быстрота речевого общения. По диаграмме, изобра-

женной на рис. 3, видно, что сотрудники неадекватно оценивают собственную речь.

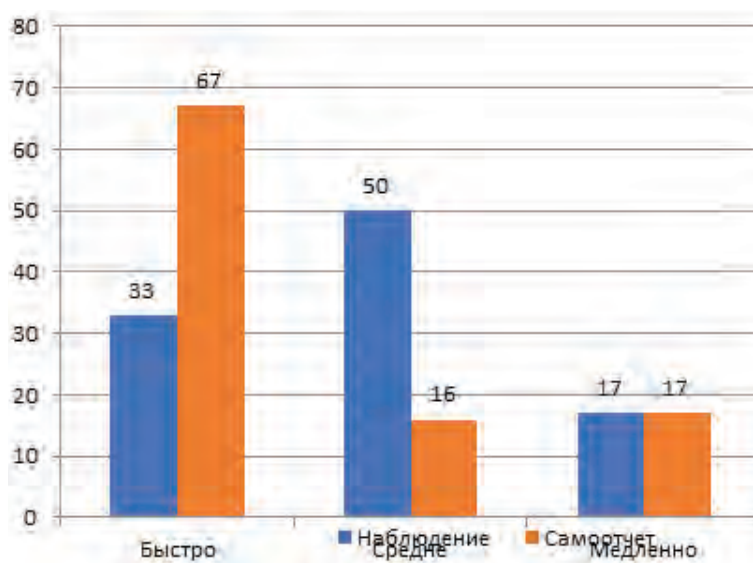


Рис. 3. Быстрота речи

При оценивании громкости речи испытуемые фактически не искажают данные — два графика на рис. 4 практически совпадают. Это свидетельствует о том, что данный параметр речи чаще всего находится в зоне сознания человека. Окружающие создают обратную связь, обеспечивая адекватную громкость своей речи, что позволяет

ведущему консультацию (говорящему) более уверенно оценивать эту характеристику.

Использование слов-паразитов в речи, пауз и времени для подбора нужного слова фактически не осознается специалистом, если только он не следит за этими параметрами своей речи специально. Экспериментальные результаты показаны на рис. 5 и 6.

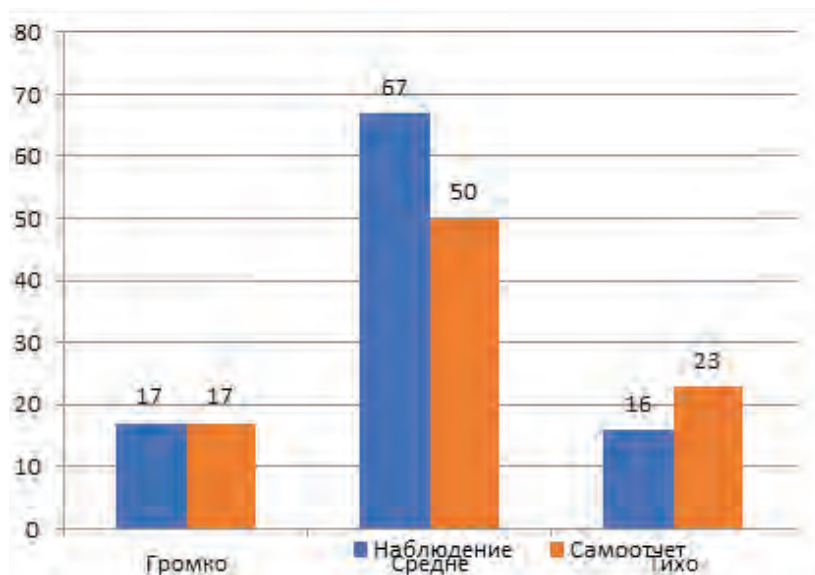


Рис. 4. Громкость речи

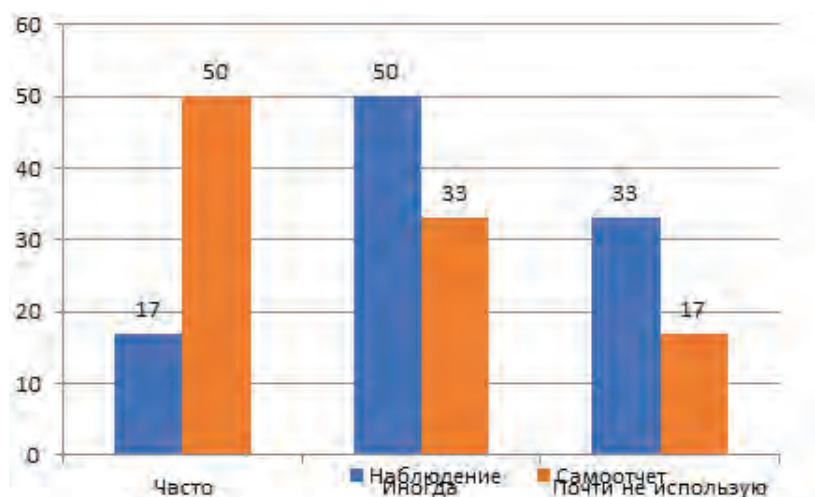


Рис. 5. Использование пауз в речи

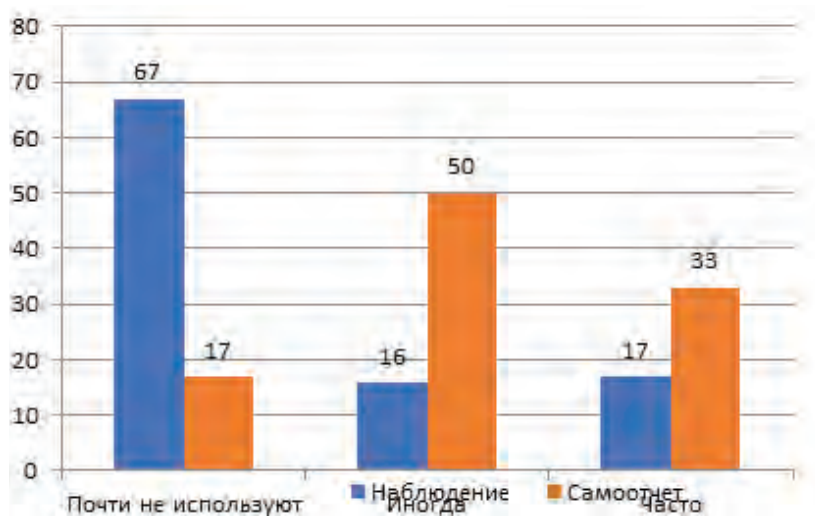


Рис. 6. Использование слов-паразитов

Сотрудники юридического отдела компании весьма критично оценивают последние два параметра, считая, что они делают больше пауз в словах, используют больше слов-паразитов в своей речи, чем по результатам наблюдения. Это можно объяснить тем, что данные параметры речи могут сильнее всего испортить впечатление от разговора со специалистом, поэтому они переживают, не

используют ли слова-паразиты и паузы в речи с неоправданной частотой.

С другой стороны, испытуемые явно недооценивают количество времени, которое им необходимо на подбор нужного слова: 83% испытуемых тратят на это достаточно много времени, что может приводить к плохому впечатлению клиентов об общении с таким юристом (см. рис. 7).

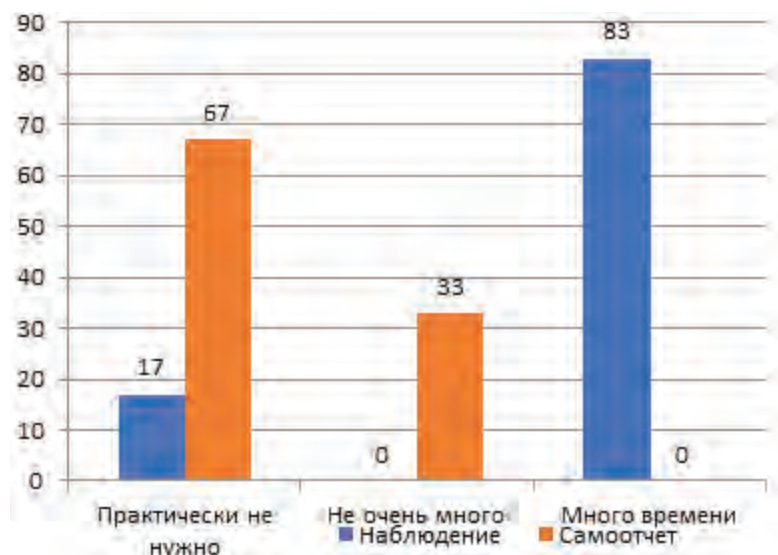


Рис. 7. Количество времени на подбор нужного слова

В целом по результатам проведенного эксперимента можно сделать следующие обобщающие выводы:

1. Юристы часто используют устную речь в своей профессиональной деятельности, причем письменную речь используют реже, чем устную.

2. Юристам проще работать с клиентами при личном контакте, чем по телефону или обмениваться информацией в письменной форме.

3. При оценивании таких параметров речи, как быстрота и количество времени на подбор нужного слова, юристы, как правило, *переоценивают* свои способности.

4. При оценивании таких параметров речи, как использование пауз и слов-паразитов, юристы часто *недооценивают* свои способности.

5. При оценивании такого параметра, как громкость голоса, юристы *адекватно* оценивают свои способности.

Подводя итоги, заметим, что глобальная информатизация и широкое внедрение информационно-компьютерных средств, ресурсов, технологий, порождающие изменения общественно-производственных отношений, не снижают актуальности для практикующего юриста традиционных

форм информационного обмена, и прежде всего, речевой коммуникативной деятельности. Поэтому при целенаправленном повышении общего уровня подготовки практикующих юристов в наступающем глобальном информационном обществе следует дополнять имеющиеся методики комплексным освоением правил информационного взаимодействия, обеспечивающих успешное ведение коммуникативной деятельности (профессионального общения) юриста в широком смысле слова. Это возможно обеспечить в результате непрерывной информационной подготовки юриста [5] в ходе изучения педагогически рационального комплекса учебных дисциплин «информационного» цикла, соответствующих мировому научно-образовательному уровню. Причём учебная дисциплина «информационное право» должна занимать центральное место, объединяя необходимые информационные и юридические знания в «единое целое», что в итоге позволит обеспечить современный уровень требований к квалификации юриста наступающего глобального информационного общества.

Таким образом, проведение подобных экспериментальных исследований и получаемые

обобщенные реальные результаты позволят обосновать и совершенствовать современную информационную модель специалиста (юриста), что, в свою очередь, может помочь юридическим вузам своевременно модернизировать [7, 8] известные

концепции непрерывной информационной подготовки юриста с учетом возникающих новых условий информатизации и, в частности, «цифровизации» современной экономики и общественно-производственной деятельности.

Рецензент: **Атагимова Эльмира Исамудиновна**, кандидат юридических наук, Аппарат Государственной Думы Федерального Собрания Российской Федерации, Российская Федерация, г. Москва

E-mail: atagimova75@mail.ru

Литература

1. Быканова О.А., Ахмадеев Р.Г. Диверсификация портфельных инвестиций суверенных фондов // Азимут научных исследований: экономика и управление. 2016. Т. 5. № 4 (17). С. 59—63.
2. Ващекин А.Н., Ващекина И.В. Информационное право: прикладные задачи и математические методы // Информационное право. 2017. № 3. С. 17—21.
3. Ващекина И.В., Ващекин А.Н. Информационный обмен между уровнями иерархий в банковских, промышленных и торговых системах // Научное обозрение. Экономические науки. 2017. № 3. С. 51-59.
4. Ващекина И.В. Перспективы реформирования организационной структуры платежной системы в России // Наука и практика. № 4 (16). 2014. С. 5—14.
5. Ершов В.В., Ловцов Д.А. Концепция непрерывной информационной подготовки юриста // Информационное право. 2007. № 3. С. 29—34.
6. Косов М.Е. Идеологический подход в исследовании нелегальной экономики // Вестник Московского университета МВД России. 2011. № 7. С. 40.
7. Ловцов Д. А. Современная концепция непрерывной информационной подготовки юриста // Российское правосудие. 2013. № 5. С. 57—66.
8. Ловцов Д. А. Модернизация информационно-правового образования в условиях формирования информационного общества // Правовая информатика. 2017. № 4. С. 4—13.
9. Пичуренко Е.А. Тестовые задания «Интеллектуальная лабильность» // Экономика. Право. Печать. Вестник КСЭИ. 2011. № 4-6 (50-52). С. 214—218.
10. Полевая М.В. Обобщенный подход к оценке эффективности персонала на основе нечетких отношений // Транспортное дело России. 2015. № 4. С. 107—109.
11. Славянов А.С. Поддержка принятия управленческих решений в период проведения инновационной модернизации производства на основе модели жизненного цикла предприятия // Контроллинг. 2017. № 1 (63). С. 26—31.
12. Тонтеева Т.В. К вопросу о коммуникативной деятельности юриста // Современные научные исследования и инновации. 2016. № 3 [Электронный ресурс]. URL: <http://web.snauka.ru/issues/2016/03/65327>.
13. Akhmadeev R.G., Kosov M.E., Bykanova O.A., Korotkova E.V., Mamrukova, O.V. Assessment of the tax base of the consolidated group of taxpayers in Russia using the method of polynomial interpolation, Indian Journal of Science and Technology, 2016, № 9 (12), p. 89533.
14. Vashchekin A.N., Khrustalev M.M. Studying stability of the econometric model of nonantagonistic game of the wholesale market subjects, Automation and Remote Control, 2005, T. 66, № 10, pp. 1677-1689.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ СТАТИСТИЧЕСКОГО АНАЛИЗА МАРКЕТИНГОВЫХ ИССЛЕДОВАНИЙ

Ловцов Д.А., Богданова М.В., Паршинцева Л.С.*

Ключевые слова: информационные технологии, пакеты прикладных программ, маркетинг, маркетинговые исследования, основные макроэкономические показатели, законодательство, статистические методы, объем рынка маркетинговых исследований, основные этапы исследования, методологическая диаграмма.

Аннотация.

Цель работы: повышение эффективности многоаспектного статистического анализа состояния маркетинговых исследований на основе применения современных информационно-программных средств.

Методы: сравнительный анализ динамики объема рынка маркетинговых исследований, сравнительный технико-экономический анализ существующих статистических методов и информационно-программных средств.

Результаты: на основе применения программных средств среды R и табличного процессора MS Excel проведена оценка объема и динамики маркетинговых исследований в России за последние десять лет как одного из наиболее интересных и востребованных инструментов маркетинга; выполнен сравнительный анализ динамики объема рынка маркетинговых исследований в сопоставимых ценах с динамикой основных макроэкономических показателей; показана роль статистических методов и информационно-программных средств в проведении маркетинговых исследований, дана их краткая характеристика. Обоснована методологическая диаграмма продуктивного маркетингового исследования.

Приведены рекомендации по использованию информационных технологий для решения прикладных аналитических задач и по выбору соответствующих статистических информационно-программных средств, а также результаты экспериментального анализа.

DOI: 10.21681/1994-1404-2018-1-32-39

Становление в России рыночной экономики и её переориентация с производства на потребление создало условия для перехода маркетинга на качественно новый уровень развития. Если в советское время, в условиях неофициального запрета маркетинга, использовались лишь некоторые его элементы, такие, например, как создание популярных торговых марок, то сегодня маркетинг является важнейшей составляющей успешной деятельности любой фирмы. Глав-

ным источником правового регулирования маркетинговой деятельностью является Гражданский кодекс¹ РФ, дополнительными — множество федеральных законов, регулирующих, в частности,

¹ Гражданский кодекс РФ, часть первая от 30 ноября 1994 г. с изменениями, внесёнными Федеральным законом от 10 января 2003 г. № 15-ФЗ // Собрание законодательства Российской Федерации. 1994. № 32. Ст. 3301; 2003. № 2. Ст. 167; часть четвёртая от 18 декабря 2006 г. № 230-ФЗ, с изменениями, внесёнными Федеральным законом от 4 октября 2010 г. № 259-ФЗ // Собрание законодательства Российской Федерации. 2006. № 52 (1 ч.). Ст. 5496; РГ. 2010. 8 окт.

* **Ловцов Дмитрий Анатольевич**, доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, заместитель по научной работе директора Института точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.

E-mail: dal-1206@mail.ru

Марина Валерьевна Богданова, доктор экономических наук, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.

E-mail: bogdanovamv2009@yandex.ru

Паршинцева Лидия Сергеевна, кандидат экономических наук, доцент кафедры статистики Государственного университета управления, Российская Федерация, г. Москва.

E-mail: lspantelina@yandex.ru

отношения субъектов маркетинговой деятельности², продвижение продукции³; маркетинговые исследования, распространение и использование маркетинговой информации⁴ и др.

Одним из наиболее интересных и востребованных инструментов маркетинга являются маркетинговые исследования — форма бизнес-исследования и направление прикладной социологии, которое, изучает предпочтения и поведение потребителей, конкурентов и рынков в рыночной экономике с учётом действующего законодательства. Результаты маркетинговых исследований входят в состав единого информационного поля и влияют на принятие компаниями управленческих

В настоящее время проведение продуктивных маркетинговых исследований на основе многоаспектной переработки больших объёмов разнородной (правовой, экономической, финансовой, патентной, конъюнктурной и др.) содержательной информации представляется возможным на основе проблемно-ориентированных информационных [3, 4, 10, 11] и геоинформационных [12] технологий статистического анализа с применением современных информационно-программных средств с учётом, прежде всего, информационного законодательства.

За последнее десятилетие, по оценкам Объединения исследователей рынка и общественного

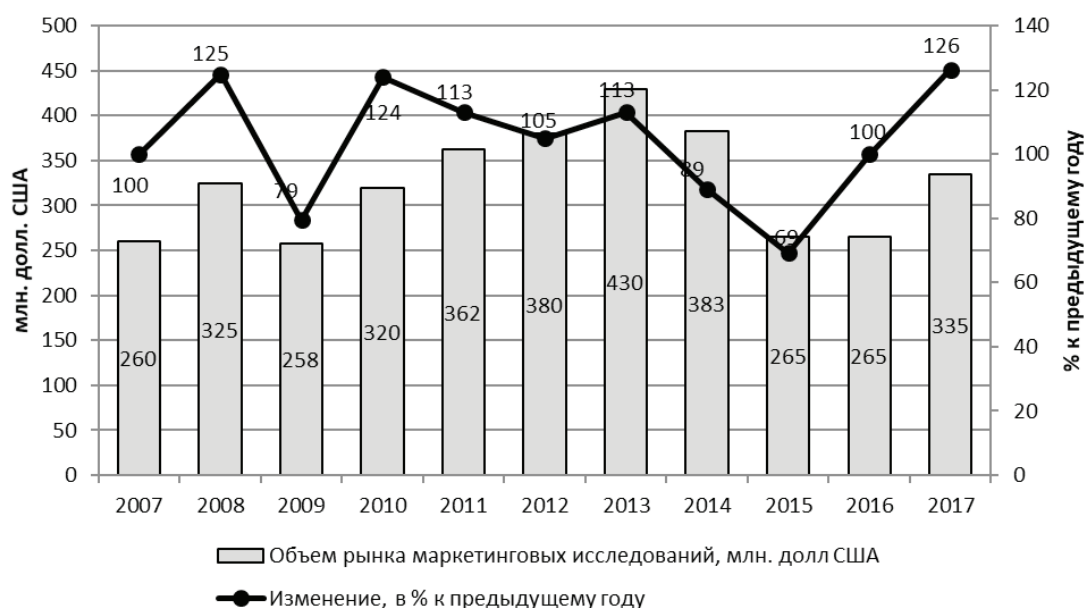


Рис. 1. Динамика объема рынка маркетинговых исследований в период 2007 — 2017 гг. в России

решений, что, в свою очередь, отражается и на рынке в целом.

² Закон РФ от 7 февраля 1992 г. № 2300-1 «О защите прав потребителей» // РГ. 1992. 7 апр.

³ Федеральный закон от 18 июля 1995 г. № 108-ФЗ «О рекламе» // Собрание законодательства Российской Федерации. 1995. № 30. Ст. 2864.

⁴ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. 29 июля; Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» с изменениями, внесенными Федеральным законом от 9 февраля 2009 № 10-ФЗ // Ведомости СНД и ВС РФ. 1992. № 7. Ст. 300; Собрание законодательства Российской Федерации. 2009. № 7. Ст. 778; Закон РФ от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных» // Ведомости СНД и ВС РФ. 1992. № 42. Ст. 2325 и др.

мнения (ОИРОМ), наибольший объем рынка маркетинговых исследований в России имел место в 2013 году и составил 430 млн. долл. США.

При этом на объеме рынка маркетинговых исследований в России отрицательно сказались кризисы 2008 г. и 2014 г. (рис. 15). Так, в 2009 году рассматриваемый показатель, рассчитанный в долларах США, снизился на 21%, а в 2015г. — на 31% по сравнению с предыдущим годом. В 2017 году отмечался прирост объема рынка маркетинговых исследований, рассчитанный в долларах США, на 26% по сравнению с 2016 годом.

⁵ Рассчитано авторами по данным ОИРОМ [13].

Если рассматривать динамику объема рынка маркетинговых исследований в национальной валюте в текущих ценах и с учетом уровня инфляции, то ситуация будет несколько иная (рис. 2⁶).

значительное опережение темпа прироста рассматриваемого показателя за период с 2007 по 2016 гг. над темпом прироста ВВП (внутреннего валового продукта) в сопоставимых ценах (в 4,2



Рис. 2. Объем рынка маркетинговых исследований в России за период с 2007 по 2017 гг. в текущих и сопоставимых ценах, млн. руб.

В результате сравнительного анализа динамики объема маркетинговых исследований за период с 2007 по 2017 гг. в России в долларах США с динамикой показателя в национальной валюте, видно, что во втором случае кризисы 2008 и 2014 гг. на графике менее заметны. Так, за рассматриваемый период наблюдался непрерывный рост объема рынка маркетинговых исследований в текущих ценах (+193,8%).

Однако на покупательную способность денег влияет не только валютный курс, но и уровень инфляции, который за последние десять лет составил 119,2%. Так, объем рынка маркетинговых исследований в сопоставимых ценах в 2017 году по сравнению с 2007 годом увеличился всего лишь на 34,0%. Из графика объема рынка с учетом инфляции видно и влияние кризисов: в 2009 году — снижение показателя на 6,9% по сравнению с предыдущим годом, а в 2015 году — снижение на 2,8%. Начиная с 2015 года, рассматриваемый показатель в сопоставимых ценах увеличился на 12,0% или на 952,8 млн. руб.

При сравнении динамики объема рынка маркетинговых исследований с динамикой основных макроэкономических показателей отмечается

раз), темпом прироста оборота розничной торговли в сопоставимых ценах (в 1,7 раза) и темпом прироста реальной среднемесячной заработной платы (в 1,5 раза) (см. таблицу⁷).

Так, ВВП в сопоставимых ценах за период 2007—2016 гг. увеличился на 8,1%, физический объем оборота розничной торговли вырос на 19,9%, а реальная среднемесячная заработная плата увеличилась на 22,7% при росте объема рынка маркетинговых исследований в сопоставимых ценах на 34,0%.

В связи с этим и учитывая приведенные численные расчеты, можно сделать вывод, что в последнее время маркетинговые исследования приобретают всё больший интерес среди отечественных компаний. Важнейшими требованиями, предъявляемыми к результатам маркетинговых исследований, являются точность, достоверность, легитимность (правовая значимость) и актуальность полученной информации. Все эти требования должны учитываться на каждом этапе маркетингового исследования.

В основе проведения маркетинговых исследований лежат статистические методы и информационно-программные средства многоаспект-

⁶Рассчитано авторами по данным ОИРОМ [13], сайта audit-it.ru, сайта уровень-инфляции.рф

⁷Рассчитано авторами по данным ОИРОМ [13], сайта www.gks.ru [15].

Таблица

Динамика основных макроэкономических показателей и объема рынка маркетинговых исследований в России за 2007—2016 гг.

Показатель	Значение показателя		Изменение в 2016 г. по сравнению с 2016 годом		Коэффициент опережения темпа прироста объема рынка маркетинговых исследований над темпом прироста основных макроэкономических показателей, раз
	2007 год	2016 год	%	в абсолютном выражении	
ВВП в сопоставимых ценах, млрд. руб.	33247,5	35924,6	+8,1	2677,1	4,2
Оборот розничной торговли в сопоставимых ценах, млрд. руб.	10869,0	13032,1	+19,9	2163,1	1,7
Реальная среднемесячная заработная плата, руб.	13593,0	16680,1	+22,7	3087,1	1,5
Валютный курс, руб./долл. США, средневзвешенный за год	25,6	67,0	+161,7	41,4	-
Объем рынка маркетинговых исследований в сопоставимых ценах, млн. руб.	6650,0	8913,4	+34,0	2263,4	-

ного анализа больших объемов статистических данных, позволяющие освещать количественную сторону изучаемого явления или процесса в качественной определенности. То есть, точность, достоверность и актуальность результатов маркетингового исследования напрямую зависит от выбранных статистических методов и информационно-программных средств (пакетов прикладных программ), в частности, зависят от того, как формировалась выборочная совокупность, репрезентативна ли она, какие статистические методы и средства выбраны для анализа собранных статистических данных, отвечают ли эти методы и средства требованию актуальности, корректно ли применены статистические методы и средства к имеющимся данным и др.?

В любом маркетинговом исследовании [6, 8, 9] можно выделить несколько важных этапов:

1. Постановка цели, задач исследования и определение его плана.
2. Формирование первичной информационной базы.
3. Обобщение и группировка полученных данных.
4. Анализ статистических данных.
5. Интерпретация и оформление полученных результатов.

На первом этапе исследования определяется суть проблемы, формулируются его цель и задачи, уточняются действующие нормативные правовые акты, создается проект исследования. Этот этап является одним из важнейших, так как он создает основу для дальнейших исследований. Именно на первом этапе определяется потребность в различных статистических данных, решается вопрос о применении тех или иных методов и информационно-программных средств сбора, переработки и анализа данных.

На втором этапе маркетингового исследования выполняется сбор данных посредством статистического наблюдения, при этом среди способов получения статистической информации важное место отводится опросу, необходимая информация при котором получается непосредственно от респондентов. Из всех видов опроса, а именно: экспедиционный, способ саморегистрации, корреспондентский, явочный и анкетный — особый интерес для маркетинга с точки зрения анализа покупательского спроса представляет последний. А с учетом того, что анкетирование при сплошном наблюдении — достаточно трудозатратный и дорогостоящий процесс, в маркетинге наиболее часто используется несплошное наблюдение. При этом предпочтение отдается выборочному наблю-

дению как единственному несплошному наблюдению, позволяющему с определенной точностью и с заданной вероятностью оценить параметры генеральной совокупности [2, 7].

После получения первичных статистических данных в целях выделения основных типов явления, изучения состава совокупности по ряду признаков, а также выявления взаимосвязей используется группировка статистических данных, которая составляет третий этап маркетингового исследования.

Четвертый этап маркетингового исследования самый объемный. На этом этапе, как правило, применяется обоснованный комплекс статистических методов для переработки и анализа данных, среди которых наиболее часто комплексированы следующие частные методы: табличный и графический методы анализа, расчет относительных и средних величин [7], расчёт показателей вариации и дифференциации, проверка гипотез, индексный метод анализа, анализ временных рядов и прогнозирование, корреляционный и регрессионный анализ, кластерный, факторный, дискриминантный анализ и др.

Завершающим этапом выполнения маркетингового исследования является подведение итогов исследования: интерпретация и оформление полученных обобщенных результатов. Оформляется маркетинговое исследование в виде отчета, который впоследствии представляется руководству компании.

На каждом этапе маркетингового исследования должен выполняться непрерывный организационно-технический, правовой и содержательный контроль качества исследования, так как ошибка или просчет, сделанные на любом из его этапов, могут привести к получению некорректных результатов всего исследования, что, в свою очередь, может спровоцировать руководство компании к принятию неверных (нерентабельных, неправовых, неэффективных и др.) управленческих решений.

В целом логическую последовательность методологических этапов продуктивного маркетингового исследования и основных информационно-статистических методов, применяемых на каждом этапе маркетингового исследования, можно представить в виде методологической диаграммы (рис. 3).

В качестве примера приведем исследование «Отношение рекламодателей к рынку маркетинговых услуг», проводимое ежегодно Российской ассоциацией маркетинговых услуг (РАМУ), начи-

ная с 2010 года, целью которого является выявление актуального состояния, направления и потенциала развития рынка маркетинговых услуг (МУ), с точки зрения экспертов-потребителей. Опираясь на методологию исследования, представленную на официальном сайте РАМУ, оно охватывает г. Москву и г. Санкт-Петербург [14]. Экспертами выступают сотрудники компаний-рекламодателей, которые имеют опыт работы с МУ-агентствами не менее 2 лет. При этом размер выборки составляет не менее 220 интервью. То есть для получения первичных данных используется несплошное наблюдение в виде опроса.

Анализ презентаций, сформированных по результатам исследования и размещенных в открытом доступе на официальном сайте Ассоциации, показал, что в процессе изучения отношения рекламодателей к рынку маркетинговых услуг были использованы такие статистические методы, как табличный и графический методы анализа, статистическая группировка и сводка данных, расчет относительных величин, построение рейтингов и кластерный анализ. Вследствие применения этих методов результаты исследования представляют значительный интерес для пользователей, являются научно обоснованными и взаимодополняющими.

Маркетинговые исследования охватывают большое количество единиц совокупности, что подтверждает приведенный пример. Ручная оперативная и качественная переработка больших объемов соответствующих статистических данных практически невозможна, вместе с тем в условиях высокой конкуренции и быстро меняющегося рынка необходимо обладать актуальной информацией для принятия своевременных обоснованных управленческих решений. Поэтому в настоящее время существенно возросла роль информационных и электронных («цифровых») технологий статистического анализа при проведении маркетинговых исследований. Для электронной переработки статистических данных существует множество пакетов прикладных программ, которые условно можно разделить на платные и бесплатные, с открытым и закрытым исходным кодом.

По назначению все статистические программные продукты можно разделить на 3 основные группы: профессиональные, универсальные и специализированные [2].

К профессиональным программам для статистического анализа, особенностью которых является возможность работы со сверхбольшими объемами данных, относятся SAS и BMDP [4, 10].

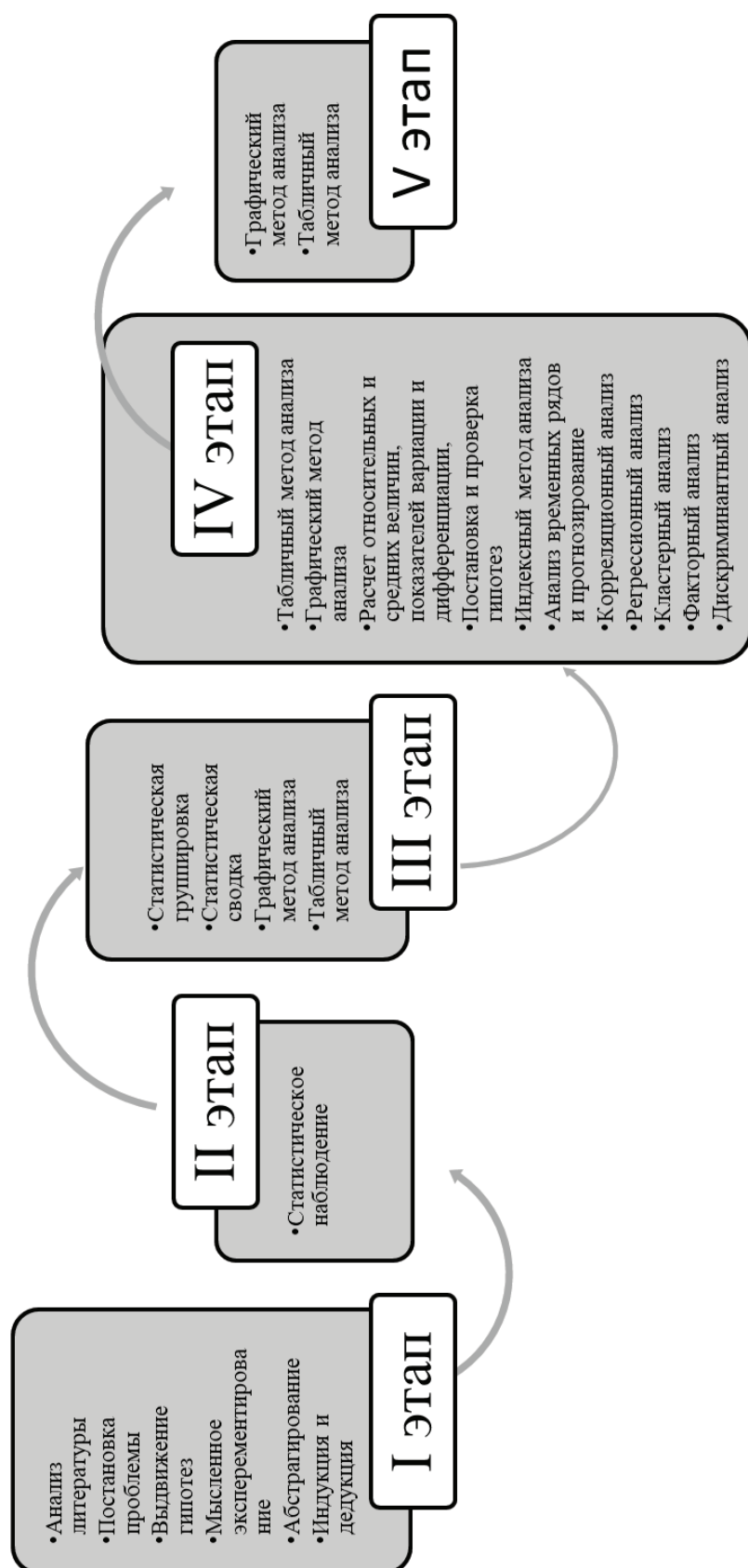


Рис. 3. Логическая последовательность методологических этапов маркетингового исследования и информационно-статистические методы

Универсальные программы предназначены для выполнения анализа данных по широкому кругу статистических методов в различных сферах человеческой деятельности.

Среди большого разнообразия универсальных программ отдельно следует выделить такие бесплатные программы, как среда R, Macanova, Vista, MyStat, InStat+, AtteStat, Microsirir, PSPP и PAST.

В специализированных пакетах реализовано ограниченное число статистических методов для детального анализа по изучаемой проблеме. К специализированным бесплатным статистическим программам относятся Gretl, Jmulti, SALTSTAT (BETA), G7, FACTOR и др.; среди коммерческих — наибольший интерес представляют такие пакеты, как Мезозавр, Эвриста и САНИ [4, 10].

При выборе того или иного информационно-программного пакета для детального статистического анализа представляется целесообразным опираться на следующие рекомендации:

Современные бесплатные статистические программы не уступают коммерческим по своим возможностям и интерфейсу.

Выбор того или иного пакета должен отвечать целям и требованиям конкретного исследования.

В настоящее время большой научный интерес представляет среда R, являющая собой язык программирования для обработки статистических данных. В отличие от целого ряда других статистических программ среда R имеет ряд преимуществ, среди которых: широкое представление статистических методов, кросс-платформенность, бесплатность, качественная графика, возможность работы с разными форматами данных, открытый

исходный код, большое множество проверенных пакетов (более 7 тыс.), возможность создания скриптов и новых пакетов и др. [4, 10].

Анализ рынка вакансий в сфере маркетинга по крупным городам России показал, что наиболее популярной и востребованной программой для выполнения маркетинговых исследований является коммерческая универсальная программа SPSS (Statistical Package for the Social Science — «Статистический пакет для социальных наук») [1], знание которой дает конкурентное преимущество соискателю вакансии в области маркетинга.

Для анализа временных рядов и прогнозирования целесообразно остановиться на одном из специализированных информационно-программных пакетов, которые включают исчерпывающий спектр статистических методов в этой области [4, 10].

Таким образом, подводя итог выполненному теоретико-экспериментальному анализу, можно утверждать, что проблемно-ориентированные информационные технологии статистического анализа с применением современных информационно-программных средств с учётом, прежде всего, информационного законодательства имеют важнейшее значение на каждом этапе маркетинговых исследований, обеспечивая научно обоснованную информационную базу для принятия легитимных маркетинговых и управленческих решений. Дальнейшее развитие соответствующих информационных технологий связано с использованием системы пространственных данных Российской Федерации [12] и с внедрением имитационно-игрового моделирования развития бизнес-структур в условиях рыночных отношений [5].

Рецензент: Марков Алексей Сергеевич, доктор технических наук, старший научный сотрудник, профессор МГТУ им. Н. Э. Баумана, Российская Федерация, г. Москва

E-mail: a.markov@bmstu.ru

Литература

1. Алексеева А. Ю., Ечевская О. Г., Ковалева П. С. Анализ социологических данных с применением пакета SPSS. Новосибирск: РИЦ НГУ, 2003. 112 с.
2. Берестнева О.Г., Марухина О.В., Шевелев Г.Е. Прикладная математическая статистика. Томск: Изд-во Томского политех. ун-та, 2012. 188 с.
3. Бернс Э. С., Буш Р. Ф. Основы маркетинговых исследований с использованием MS Excel. М.: Вильямс, 2005. 704 с.
4. Богданова М. В., Паршинцева Л. С. Современные средства электронной обработки социально-экономической информации // Вестник университета. 2017. № 5. С. 10—15.
5. Ловцов Д. А. Имитационно-игровое моделирование функционирования и развития совокупности крупномасштабных эргосистем // Труды XVI Междунар. науч.-метод. конф. «Информатика: проблемы, методология, технологии» (11—12 февраля 2016 г.) / ВГУ. Воронеж: Изд-во «Науч.-исслед. публикации», 2016. С. 78—86.
6. Ловцов Д. А., Богданова М. В. Проблема управления инвестициями оборонных проектов России // Обзореватель-Observer. 2000. № 8. С. 53—57.
7. Ловцов Д. А., Богданова М. В., Паршинцева Л. С. Основы статистики / Под ред. Д. А. Ловцова. М.: РГУП, 2017. 160 с.

8. Ловцов Д. А., Богданова М. В. Информационно-статистические показатели качества проектных инвестиций // НТИ РАН. Сер. 2. Информ. процессы и системы. 2000. № 12. С. 28—36.
9. Ловцов Д. А., Богданова М. В. Экономико-правовое регулирование оборота результатов интеллектуальной деятельности предприятий промышленности России // Экономика, статистика и информатика. Вестник УМО. 2013. № 1. С. 53—56.
10. Ловцов Д. А., Богданова М. В., Паршинцева Л. С. Пакеты прикладных программ для многоаспектного анализа судебной статистической информации // Правовая информатика. 2017. №1. С. 28—36.
11. Ловцов Д. А., Богданова М. В., Паршинцева Л. С. Правовая статистика преступности в современных условиях // Правовая информатика. 2017. № 4. С. 40—48.
12. Ловцов Д. А., Черных А. М. Модернизация системы судебной статистики на основе новой геоинформационной технологии // Правовая информатика. 2016. № 1. С. 7—14.
13. Объединение исследователей рынка и общественного мнения ОИРОМ [Электронный ресурс]. Режим доступа: <http://oirom.ru/> (дата обращения: 20.03.2018 г.)
14. РАМУ — Российская ассоциация маркетинговых услуг [Электронный ресурс]. Режим доступа: <https://www.ramu.ru/> (дата обращения: 20.03.2018г.)
15. Федеральная служба государственной статистики Росстат [Электронный ресурс]. Режим доступа: www.gks.ru (дата обращения: 21.03.2018).

ИНФОРМАЦИОННАЯ НАДЁЖНОСТЬ ФУНКЦИОНИРОВАНИЯ ТЕЛЕМАТИЧЕСКОЙ СЕТИ ГАС РФ «ПРАВОСУДИЕ»

Ловцов Д.А.*

Ключевые слова: информационная надёжность, телематическая сеть (ТМС), ГАС РФ «Правосудие», привилегированная информация, ГОСТ, система доменных имён, протокол пограничного шлюза, международные технико-правовые стандарты, инфраструктура открытых ключей, криптографические алгоритмы, нетрадиционный информационный канал (НИК).

Аннотация.

Цель работы: формирование продуктивной теоретической и правовой базы разработки и развития телематической сети Государственной автоматизированной системы Российской Федерации (ГАС РФ) «Правосудие», обладающей повышенной информационной надёжностью.

Метод: комплексный теоретико-прикладной анализ и разработка информационно-математического обеспечения информационной надёжности функционирования телематической сети ГАС РФ «Правосудие».

Результаты: обоснована и декомпозирована математическая постановка задачи ситуационного управления защищённым обменом привилегированной информацией в условиях воздействия значительных случайных и преднамеренных дестабилизирующих факторов в телематической сети с произвольной топологической структурой; предложен способ решения поставленной сложной задачи, а также определены организационно-правовые и технологические мероприятия в рамках международно-правовой стандартизации основных сетевых протоколов глобальной сети Интернет как одного из эффективных путей решения проблемы обеспечения информационной надёжности телематической сети ГАС РФ «Правосудие».

Предложен ряд мероприятий на государственном уровне по обеспечению требуемого уровня информационной надёжности функционирования телематической сети ГАС РФ «Правосудие» и её абонентов-пользователей.

DOI: 10.21681/1994-1404-2018-1-40-48

Телематическая сеть (ТМС) Государственной автоматизированной системы Российской Федерации (ГАС РФ) «Правосудие», в которой осуществляется защищённый обмен привилегированной информацией, иерархически объединяет множество территориально распределённых информационно-вычислительных сегментов объектов автоматизации: Верховного Суда РФ, судов общей юрисдикции, органов Судебного департамента, центров подготовки и обучения, центров поддержки и др.

Каждый сегмент S_i , $i = 0, 1, 2, \dots, N$ (рис. 1) практически представляет собой локальную информационно-вычислительную сеть с единой точкой

подключения (через узлы защиты — УЗ) к глобальной вычислительной сети Интернет. В логико-физической модели ТМС такими точками являются маршрутизаторы $PC(0,1)$, $PC(1,1)$, $PC(2,1)$, $PC(3,1)$. Каждый из перечисленных маршрутизаторов соединен каналом связи с соответствующим маршрутизатором $PC(0,2)$, $PC(1,2)$, $PC(2,2)$, $PC(3,2)$ провайдера услуг сети Интернет.

Поскольку оборудование и каналы связи общедоступной сети Интернет не контролируются средствами защиты корпоративной сети ГАС РФ «Правосудие», в целях обеспечения информационной безопасности следует предполагать наличие внешнего нарушителя, способного перехватывать, модифицировать, подделывать или

* Ловцов Дмитрий Анатольевич, доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, заместитель по научной работе директора Института точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.

E-mail: dal-1206@mail.ru

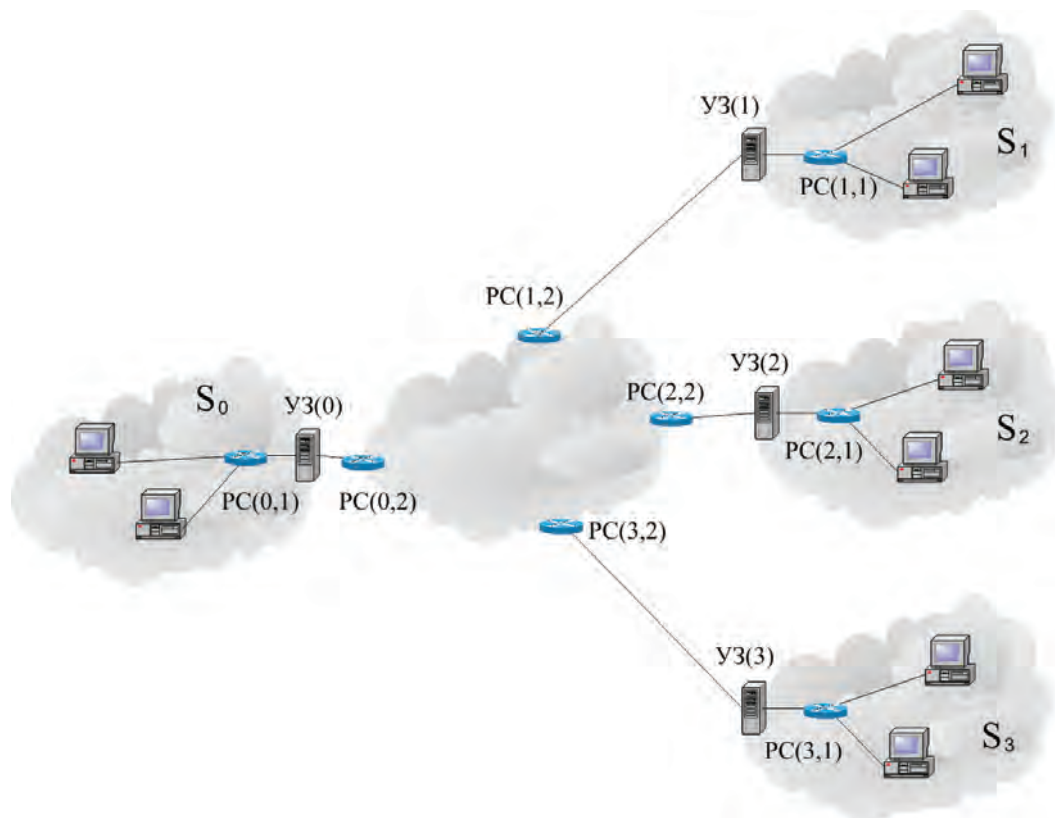


Рис. 1. Фрагмент логико-физической структуры телематической сети

уничтожать информационные массивы (ИМ), передаваемые по общедоступной сети. В связи с этим при построении и развитии корпоративной сети ГАС РФ «Правосудие» необходимо применение средств защиты, препятствующих взаимодействию внешнего нарушителя с узлами корпоративной сети, а также обеспечивающих *конфиденциальность, аутентичность и целостность* [8] информации, передаваемой между сегментами. Кроме того, следует учитывать также возможность различных возмущающих воздействий случайного характера на информационные ресурсы корпоративной сети.

Таким образом, телематическая сеть ГАС РФ «Правосудие» функционирует в условиях ситуационной неопределённости среды, определяемой всевозможными дестабилизирующими (возмущающими) факторами $\omega_i \in \Omega, i = 1, 2, \dots$, двух типов:

случайными, т. е. технической ненадёжностью средств ТМС, различными видами погрешностей криптопреобразования и др.;

преднамеренными — воздействиями нарушителя политики безопасности (противника) на аппаратно-программные средства ТМС, осуществляемыми как по традиционным, так и по *нетрадиционным* (скрытым) информационным каналам (НИК) [2, 5].

Алгебраическую модель процесса защищённого обмена привилегированной информацией (включая криптопреобразования и маршрутизацию) в ТМС можно представить в виде (рис. 2) [3]:

$$\begin{cases} \langle M_0, M_1, \Phi, \Omega, f(M_0, M_1, \Omega), \tau \rangle \\ a_M(Q) : M_0 \times \Omega \longrightarrow M_1 \times \Omega, \end{cases} \quad (1)$$

где M_0 — множество исходных информационных массивов (ИМ) — оригиналов, предназначенных для защищённой передачи посредством ТМС потребителю; M_1 — множество ИМ, преобразованных с использованием некоторого алгоритма $a_M(Q) \in A_M$ криптопреобразования и маршрутизации и переданных потребителю; Φ — структура алгебраической модели ТМС (определяет количество *структурной* — преобразующей информации [4]); $\Omega = \{\omega_i\}, i=1, 2, \dots$ — множество факторов неопределённости; f — конкретный вид ситуационного (характеризуется Ω) распределения сложных событий, состоящих в том, что на входе ТМС действует ИМ $m_{0i} \in M_0$, а на выходе через определённый промежуток времени τ появляется ИМ $m_{1j} \in M_1$.

Согласно модели (1) алгоритмического процесса криптопреобразования и маршрутизации ИМ в ТМС меру (оценку) технологического эффекта, получаемого от данной ТМС как совокупности взаимосвязанных информационных узлов в результате выполнения процесса криптопреобразования и маршрутизации ИМ, можно определить в виде функции

$$E\{f(M_0, M_1, \Omega)\}. \quad (2)$$

Кроме традиционного требования аддитивности к функции (2) можно предъявить следующие требования:

$$E(f) = \begin{cases} 0, & \text{если } p(m_{0i}, m_{1j}) = p(m_{0i}) p(m_{1j}), \\ \max, & \text{если } p(m_{1j} | m_{0i}) = p(m_{0i}, m_{1j}) / p(m_{0i}) = 1. \end{cases} \quad (3)$$

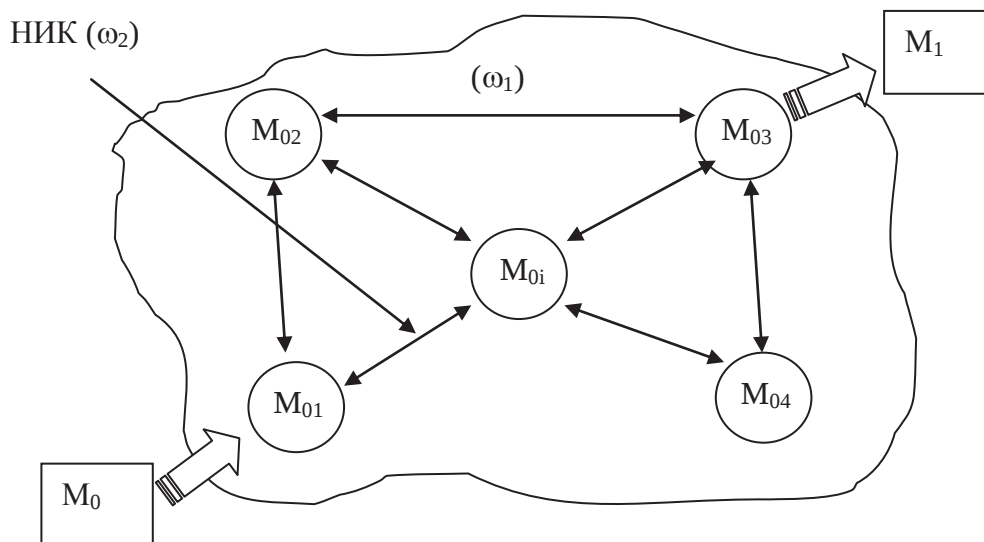


Рис. 2. Концептуально-логическая модель процесса защищенной передачи информации по телематической сети

Первое равенство в требовании (3) соответствует случаю полной статистической независимости событий, состоящих в поступлении на вход ТМС $m_{0i} \in M_0$ и событий, состоящих в образовании на выходе $m_{1j} \in M_1$. Второе равенство соответствует идеальному случаю, когда m_{1j} является результатом применения алгоритма $a_m(Q) \in A_m$ к ИМ m_{0i} . Всем перечисленным требованиям удовлетворяет функция

$$E(f) = \ln\{p(m_{0i}, m_{1j}) / (p(m_{0i}) p(m_{1j}))\}. \quad (4)$$

Усреднение по всем парам $\langle m_{0i}, m_{1j} \rangle$ даёт меру технологического эффекта функционирования ТМС:

$$E = \sum_i \sum_j p(m_{0i}, m_{1j}) \ln\{p(m_{0i}, m_{1j}) / (p(m_{0i}) p(m_{1j}))\}. \quad (5)$$

Выражение (5) преобразуется к виду [4, 11]:

$$E = H(M_1) - \sum_i p(m_{0i}) H(M_1 | m_{0i}), \quad (6)$$

где $H(M_1) = \sum_j p(m_{1j}) \ln\{p(m_{1j})\}$; $H(M_1 | m_{0i}) = \sum_j p(m_{1j} | m_{0i}) \ln\{p(m_{1j} | m_{0i})\}$.

С учётом (6) определим выражение для имеющего практическое значение показателя информационной надёжности функционирования ТМС:

$$Q = E / H(M_1), \quad (7)$$

где $Q \in (0, 1]$ — информационная надёжность равна 1 в случае отсутствия дестабилизирующих факторов.

При этом под информационной надёжностью [3, 6, 10] функционирования ТМС понимается свойство подсистемы контроля и защиты информации выполнять требуемые функции криптопреобразования, маршрутизации и доставки информационных массивов, циркулирующих в ТМС в условиях информационного соперничества, характеризующее степень защищённости обмена привилегированной информацией и заключающееся в способности не допускать случайного или целенаправленного искажения, разрушения, раскрытия, модификации или переадресации информационных массивов.

Числовой пример. Посредством ТМС в VPN-подсети осуществляется защищённая передача (преобразование, маршрутизация и доставка) ИМ (сообщений, пакетов) m_{0i} , $i = 1, \dots, 3$ в условиях воздействия значительных случайных и преднамеренных дестабилизирующих факторов Ω . Преднамеренные помехи, осуществляемые, главным образом, по НИК, направлены на переадресацию (ложную маршрутизацию через внешние для VPN-подсети информационные узлы) отдельных авторизованных ИМ m_{0i} , $i = 1, \dots, 3$, а также на инфиль-

трацию ложных ИМ m_{0i} , $i = 4, \dots, 5$. Результатами работы алгоритма a_M криптопреобразования, маршрутизации и доставки ИМ m_{0i} , $i = 1, \dots, 3$ потребителю являются ИМ m_{1j} , $j = 1, \dots, 3$. Распределение $f(M_0, M_1, \Omega)$ описывается матрицей совместных вероятностей ИМ m_{0i} и m_{1j} (которую можно составить непосредственно перед реализацией защищённого обмена привилегированной информацией на основе проведения сеансов маскирующего обмена):

$$f = \begin{vmatrix} 0,12 & 0,02 & 0,04 & 0,04 & 0,02 \\ 0,05 & 0,08 & 0,12 & 0,10 & 0,03 \\ 0,10 & 0,05 & 0,03 & 0,12 & 0,08 \end{vmatrix}$$

Отсюда с учётом (6) получим:

$$E = 0,14 \text{ бит};$$

$P(M_1) = < 0,24 \ 0,38 \ 0,38 >$, что даёт $H(M_1) = 1,55 \text{ бит}$.

$$\text{Тогда: } Q = E / H(M_1) = 0,1.$$

Выражения (5) — (7) получены на основе общепринятых методов, основанных на том, что само понятие технологической эффективности имеет статистический характер [11].

В отношении показателя (7) доказана [6] справедливость следующего утверждения-теоремы: уровень Q информационной надёжности ТМС с произвольной топологической структурой определяется соответствующим локальным показателем выходного информационного узла L ($L = 1, \dots, L$) при любых условиях, т. е. $Q \leq Q_L$.

Таким образом, математическую постановку задачи ситуационного управления защищённым обменом привилегированной информацией в условиях воздействия значительных случайных и преднамеренных дестабилизирующих факторов [9] в ТМС с произвольной топологической структурой сети можно представить в виде:

$$K: Q(w^*, \tau) = \max_{\{w_j\}} (8)$$

$$Q(w) = E / H(M_1) = 1 - \{\sum_i p(m_{0i}) H(M_1 | m_{0i})\} / H(M_1),$$

$$i = 1, \dots, J;$$

$$Q \in (0, 1];$$

$$W = \{w_j, j = 1, \dots, J\};$$

$$t_p < \tau < T,$$

где $w_j = < R, C, t_p >$ — набор ключевых параметров; $R \geq R^0$ — результативность (стойкость к взлому, случайному сбою, воздействию НИК и др.); $C \leq C^0$ — ресурсоемкость алгоритмов криптопреобразования и маршрутизации; t_p — временные затраты на криптопреобразование и маршрутизацию, τ — время доставки ИМ; $T \leq T^0$ — время актуальности ИМ.

Задача в данной постановке (8) является сложной многопараметрической многоэтапной оптимизационной задачей оперативного стохастиче-

ского программирования, методов решения которой в настоящее время не существует. Особенностью данного типа задач является, в частности, то, что её надо решать каждый раз заново, учитывая сложившуюся ситуацию (ситуационное описание ТМС). Логическая декомпозиция сформулированной задачи выявила следующие частные (относительно простые) прикладные подзадачи:

- формализации ситуации (настройки расчётных алгоритмов);

- распределения наборов w_j , $j = 1, \dots, J$ ключевых параметров [1];

- модификации криптопреобразования ИМ (по отечественным ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-94)¹;

- выработки усиленной электронной подписи² (возведения в степень по модулю, умножения чисел по модулю, сложения чисел по модулю);

- проверки усиленной электронной подписи (вычисления обратного элемента по модулю (может быть вычислен путём возведения в степень $Q-2$ по модулю Q), двух возведений в степень по модулю P , двух умножений по модулю Q);

- хэширования (вычисления Ψ^k — k -й степени преобразования Ψ применяемой в составе шифрующего преобразования алгоритма вычисления шаговой функции хэширования);

- модификации сетеобразующих протоколов: разрешения доменных имён DNS (Domain Name System — система доменных имён) — защищённой трансляции символьных доменных имён в IP-адреса узлов сети Интернет; хранения и передачи подписей служебной информации, хранения и передачи открытых ключей, защиты отрицательных ответов;

- глобальной динамической маршрутизации BGP (Border Gateway Protocol — протокол пограничного шлюза) — «проверки источника» информации о блоках сетевых адресов, опирающейся на существующую систему региональных интернет-реги-

¹ ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. М.: Госстандарт России, 1994; ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Госстандарт России, 1994; ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Гос. комитет СССР по стандартам, 1989.

² Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // РГ. 2011. 8 апр.

стратур³, основанной на использовании усиленной электронной подписи и требующей использования расширения инфраструктуры публичных ключей *PKI* (*Public Key Infrastructure* — инфраструктура открытых ключей) для аутентификации; разделения принятия решений о маршрутизации и реализации собственно транзита трафика между двумя различными элементами — платформой управления маршрутами и собственно маршрутизатором) [7].

Для обеспечения (повышения) информационной надежности функционирования ТМС представляется целесообразным разработать соответствующую методику, реализующую алгоритмы и протоколы выполнения перечисленных частных *прикладных подзадач* и обеспечивающую численную оценку соответствующих показателей следующих трёх групп, имеющих практическое значение: *результативности* (стойкости к взлому, к случайному сбою, к воздействию НИК), *оперативности* (времени реализации алгоритмов криптопреобразования и маршрутизации) и *ресурсёмкости* (расходования оперативной памяти сетевых процессоров).

В настоящее время известно множество *относительно* надёжных (безопасных, достоверных, устойчивых) вариантов сетевых протоколов, принятых интернет-сообществом в форме *RFC* (*"Requests for Comments"* — «требования к обсуждению»), играющих роль международных технико-правовых стандартов.

В частности, стандартизирующей международной организацией (СМО) *IETF* (*Internet Engineering Task Force* — Инженерный совет Интернета) принят стандарт (*RFC*) защищённого протокола разрешения доменных имен *DNSSec* (*DNS Security*), предлагающий весьма надёжную криптографическую защиту протокола *DNS* и сохраняющий полную обратную совместимость с ним, т.е. обеспечивающий возможность в защищённом от искажений виде выполнять трансляцию символьных доменных имен в *IP*-адреса узлов ТМС. При этом основными вспомогательными протоколами являются: *RRSIG* — протокол хранения и передачи подписей служебной информации протокола *DNS*, *DNSKEY* — протокол хранения и передачи открытых ключей, *NSSEC* — протокол защиты отрицательных ответов.

³ В выделенном регионе регистрирует домены, выдаёт *IP*-адреса, выделяет адреса автономных систем и др.

Существуют принятые СМО *IETF* международные стандарты модифицированного протокола глобальной маршрутизации *BGP*:

- *SIDR-RPKI* (*Resource PKI*) — предусматривает построение системы «проверки источника» (*origin validation*) информации о блоках сетевых адресов, опирающейся на существующую систему региональных интернет-регистратур⁴, основан на использовании электронной цифровой подписи (обеспечивая невозможность подделки информации по пути её следования к потребителю) и требует использования расширения инфраструктуры публичных ключей);

- *RCP* (*Route Control Platform* — платформа управления маршрутами) — предусматривает концептуальное разделение принятия решений о маршрутизации и реализации транзита трафика между двумя различными элементами: платформой (процессором) управления маршрутами и собственно маршрутизатором.

Вместе с тем проблема информационной надежности телематической сети ГАС РФ «Правосудие» и ее абонентов-пользователей остаётся актуальной, что обусловлено как несовершенством традиционных и предлагаемых СМО *IETF* модифицированных сетевых протоколов, так и возможностью несанкционированного доступа к циркулирующей привилегированной информации с использованием популярных с конца 90-х гг. нетрадиционных информационных каналов (НИК)⁵.

Например, в результате несанкционированного воздействия на протокол *BGP* возможно изменение маршрутов передачи привилегированной информации с выходом из контролируемой зоны для её сбора и содержательного анализа (криптоанализа), что может остаться незамеченным для взаимодействующих абонентов используемого

⁴ При европейской региональной интернет-регистратуре *RIPE* (*Reseaux IP Europeens* — Европейские *IP*-сети) создана наиболее развитая база информации об актуальных связях автономных систем между собой.

⁵ В России разработан ряд соответствующих технико-правовых норм для защиты от НИК. См., например, ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. М.: Стандартинформ, 2008. Исполн. Д. Б. Кабелев, А. А. Грушо, А. В. Гусев, Д. А. Ловцов и др.; ГОСТ Р 53113.2-2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, ИТ и АС от атак с использованием скрытых каналов. М.: Стандартинформ, 2009. Исполн. Д. Б. Кабелев, А. А. Грушо, А. В. Гусев, Д. А. Ловцов и др.

сегмента телематической сети. При несанкционированном воздействии на протокол DNS и искажении таблиц IP-адресов (необходимых для трансляции символьных доменных имён) ряда серверов возможна задержка и даже потеря передаваемых сообщений, а также их замена и инфильтрация нелегитимных данных.

Всё это обуславливает возможность отдельным государствам управлять работоспособностью крупномасштабных ТМС в других государствах того же региона. Поскольку угроза попыток влияния на региональную интернет-регистратуру со стороны властей страны, в которой она расположена, представляется вполне реальной, так как соответствующая организация является, как правило, юридическим лицом, подчиняющимся законам страны пребывания, в том числе и её силовым органам и спецслужбам, и отказ, в частности, выполнения требования спецслужб об изъятии какой-либо записи из базы данных (что приведёт к прекращению маршрутизации для соответствующего блока сетевых адресов) представляется маловероятным.

Более того, существует риск «политических» деструктивных атак как на *DNSSEC*, так и на *SIDR*. Причём, если в первом случае атаки возможны только как прямое недружественное действие по отношению к соответствующему государству или владельцу зоны *DNS*, а значит, последствия и резонанс такой атаки будут максимальны, то во втором случае местом проведения атаки является база данных региональной интернет-регистратуры, а объектом может быть отдельный блок сетевых адресов, содержащий конкретные сетевые ресурсы в конкретной стране, т.е. такая атака может направляться на конкретный ресурс, организацию и др. и не позиционироваться как недружественный акт на международном уровне. Однако и в первом случае для атак такого рода все возможности имеются, поскольку управление корневой (*root*) зоной *DNS* осуществляет американская организация *ICANN* (*Internet Corporation for Assigned Names and Numbers* — Международная корпорация по присвоению имён и номеров), а техническое сопровождение работ по созданию и наполнению зоны осуществляет американская компания *Verisign, Inc.*⁶.

Вообще говоря, все атаки, типичные для *SIDR*, имеют смысл и для *DNSSEC*, в частности, это уничто-

жение валидной записи искажением одного бита при её передаче (электронная цифровая подпись будет неверна), имитация отказа держателя зоны от использования *DNSSEC* (*“downgrade attack”*), атаки на «центр» инфраструктуры и на каналы, по которым он распространяет информацию и др.

Кроме того, применение криптографических средств в данных сетевых протоколах вносит в них множество новых возможных «уязвимостей», связанных со стойкостью используемых криптографических алгоритмов, с используемыми процедурами генерации, распределения, хранения и смены ключей [10]; процедурами выпуска и отзыва сертификатов электронной цифровой подписи и др. В этой связи необходимо заметить, что если в протоколе *DNSSEC* предусмотрена возможность выбора и использования различных криптографических алгоритмов, то проект *SIDR* предусматривает использование только одного криптографического алгоритма и даже необходимость (в случае его компрометации) наличия механизма его смены (*algorithm rollover*) не осознавалась до недавнего времени разработчиками этого проекта.

Наиболее тревожным представляется то, что последовательное внедрение валидации информации с помощью криптографических средств приведёт к выделению в ТМС определённых «центров», которые будут выполнять роль и функции «центров доверия». Такие «центры» станут, очевидно, привлекательной целью для различного рода атак, как технологических, так и организационно-политических. Также важным представляется то, что надёжность сетевых протоколов после их модернизации становится зависимой от надёжности использованных в них криптографических алгоритмов, а также уверенности в их высоком качестве и отсутствии недеklarированных возможностей.

Наконец, процесс внедрения разрабатываемых модернизаций займёт, скорее всего, значительный период времени (возможно, несколько лет), и всё это время телематические сети будут должны обеспечивать функционирование протоколов одновременно и в «модернизированном» и в «немодернизированном» режимах, что открывает различные возможности проведения *“downgrade attacks”*, а также сохраняет возможности для различных форм киберпреступности (включая крэкинг, спаминг, фишинг, киберсквоттинг и др.).

В связи с наличием принципиально неустраняемых уязвимостей современных сетевых протоколов, снижение вероятности отказов сети

⁶ Компания, поддерживающая разнообразные сетевые структуры, включая два из тринадцати существующих корневых серверов *DNS*, и др. (г. Рестон, штат Вирджиния).

Интернет на территории России можно обеспечить только комплексом организационно-правовых и технологических мероприятий, направленных либо на снижение вероятности реализации уязвимостей за счёт ограничений, накладываемых на информацию, циркулирующую в сетевом протоколе, либо на уменьшение негативного эффекта при её реализации (уменьшение времени обнаружения причин уязвимости, локализацию области распространения неверной информации, уменьшение времени восстановления сетевой связности и др.).

В такой комплекс мероприятий входят, в частности:

- разработка регламентов для основных операторов национального сегмента сети Интернет по конфигурированию протокола глобальной маршрутизации *BGP*, учитывающих мировую практику и имеющих целью уменьшить вероятность реализации уязвимостей протокола *BGP*;
- разработка регламентов для операторов национального сегмента сети Интернет, обеспечивающих использование операторами локальных баз данных и локальной системы корневых серверов;
- разработка регламентов⁷ по использованию в системах защиты сетевых протоколов сети Интернет и обеспечивающих служб сертифицированных криптографических средств защиты информации, опирающихся на отечественные криптографические алгоритмы;
- разработка регламентов по внесению информации о критически важных ресурсах сети Интернет в сетевые протоколы и мерах по обеспечению её неискаженного состояния для операторов сети Интернет, предоставляющих соединение с сетью Интернет для подобных ресурсов;
- создание распределённой системы мониторинга и предупреждения о фактах распро-

странении недостоверной информации по сетевым протоколам;

- создание распределённой системы мониторинга актуальной сетевой информации о критически важных ресурсах сети Интернет, а также о ресурсах, поддержание непрерывной работоспособности которых считается важным с экономической, политической или социальной точек зрения;
- создание локальной системы корневых серверов протокола *DNS*, синхронизированной по содержанию с глобальными корневыми серверами, но находящейся под национальным контролем и управлением;
- внедрение средств обеспечения целостности и непротиворечивости информации в базах данных регистратур *DNS*, защиты этих баз данных от возможных атак, а также средств и методик контроля целостности информации в этих базах;
- внедрение средств контроля целостности и непротиворечивости информации в базах данных региональных интернет-регистратур;
- организация локальной базы данных о существующих блоках сетевых адресов, синхронизированной по содержанию с базами данных региональных интернет-регистратур, но находящейся под национальным контролем и управлением.

Целесообразным представляется также активное участие в процессе модернизации существующих сетевых протоколов российских специалистов и экспертов, с целью обеспечения учёта требований, необходимых для обеспечения безотказной работы национального сегмента сети Интернет в Российской Федерации, противодействия внедрению технологий, ведущих к концентрации возможностей глобального управления сетью Интернет, в том числе на территории и за пределами Российской Федерации. При этом следует поддерживать модернизацию существующих сетевых протоколов и обеспечивающих их служб, направленные на усиление защиты и повышение достоверности информации, циркулирующей в протоколах и обеспечивающих службах.

Как правило, такие модернизации в настоящее время существенно опираются на использование криптографических алгоритмов, в связи с чем представляется целесообразным продвижение отечественных криптографических алгоритмов как стандартных элементов соответствующих протоколов, с целью обеспечения возможности их использования в модернизированных сетевых

⁷ См., например: RFC 5830. GOST 28147-89. Encryption, Decryption, and Message Authentication Code (MAC) Algorithms. March 2010. Executers: D. Kabelev, I. Ustinov, I. Emelianova, V. Dolmatov; RFC 5831. GOST R 34.11-94. Hash Function Algorithm. March 2010. Executers: D. Kabelev, I. Ustinov, V. Dolmatov, S. Vyshensky; RFC 5832. GOST R 34.10-2001. Digital Signature Algorithm. March 2010. Executers: D. Kabelev, I. Ustinov, V. Dolmatov, S. Vyshensky; RFC 5933. GOST R 34.10-2001. Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC. July 2010. Executers: D. Kabelev, I. Ustinov, V. Dolmatov, A. Chuprina.

бразующих протоколах как минимум в пределах национального сегмента сети Интернет.

Соответствующий комплекс эффективных алгоритмов и протоколов, отвечающих требованиям отечественных ГОСТ и предлагаемых RFC, в составе специализированной (проблемно-ориентированной) функциональной базы данных и знаний подсистемы контроля и защиты информации в ГАС РФ «Правосудие» позволит снизить деструктивное влияние возможных дестабилизирующих (возмущающих) факторов, и, прежде всего, преднамеренных, что позволит повысить (на 20 — 25%) общий уровень информационной надёжности телематической сети ГАС РФ «Правосудие».

Вместе с тем, поскольку в настоящее время среди вновь разрабатываемых и исследуемых протоколов нет чётко выраженных «преемников» для существующих сетевых протоколов *BGP* и *DNS*, следует активно принимать участие в правовых и технологических исследованиях и разработках по данной тематике, чтобы формировать направления развития новых протоколов, их свойства и характеристики так, чтобы они по принципам их построения и реализации обеспечивали более высокую защищённость, надёжность и устойчивость функционирования национального сегмента сети Интернет по сравнению с настоящим временем.

Таким образом, для обеспечения требуемого уровня информационной надёжности функционирования телематической сети ГАС РФ «Правосудие» и её абонентов-пользователей представляется необходимым следующее:

принимать активное участие в разработке новых сетевых протоколов и модернизации существующих;

модификацию сетевых протоколов с целью повышения их эффективности тесно связать с модификацией криптографической части этих протоколов, в связи с чем Российской Федерации следует принять все предлагаемые СМО *IETF* модификации сетевых протоколов при условии замены используемых криптографических алгоритмов на отечественные алгоритмы ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001⁸;

определить порядок использования криптоалгоритмов в сетевых протоколах национального сегмента сети Интернет, а также порядок работы с криптографическими ключами и обеспечить выполнение этих требований операторами связи;

вести целенаправленную работу по международно-правовой стандартизации используемых криптографических алгоритмов.

Рецензент: **Бетанов Владимир Вадимович**, доктор технических наук, профессор, начальник центра АО «Российские космические системы», Российская Федерация, г. Москва
E-mail: vlavab@mail.ru

Литература

1. Кабелев Д. Б. О решении задачи распространения и хранения открытых ключей в АСБР Московского региона // Обозрение прикладной и промышленной математики (в Российской Федерации). 2002. Т. 9. Вып. 1. С. 18—25.
2. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74.
3. Ловцов Д. А. Информационные показатели эффективности функционирования АСУ сложными динамическими объектами // Автоматика и Телемеханика. 1994. № 12. С. 143—150.
4. Ловцов Д. А. Модели измерения информационного ресурса АСУ // Автоматика и Телемеханика. 1996. № 9. С. 3—17.
5. Ловцов Д. А., Ермаков И. В. Классификация и модели нетрадиционных информационных каналов в эргосистеме // НТИ РАН. Сер. 2. Информ. процессы и системы. 2005. № 2. С. 1—7.
6. Ловцов Д. А. Информационные оценки технологической эффективности переработки информации // НТИ РАН. Сер. 2. Информ. процессы и системы. 1997. № 11. С. 22—26.
7. Ловцов Д. А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3—7.
8. Ловцов Д. А. Информационная теория эргосистем: Тезаурус. М.: Наука, 2005. 248 с.

⁸ В настоящее время, например, в СМО *IETF* и др. имеется значительное противодействие признанию отечественных криптоалгоритмов ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 в качестве допустимых к использованию в сетевых протоколах со стороны представителей в основном американских компаний.

9. Ловцов Д. А., Кабелев Д. Б. Ситуационное управление защищённым обменом привилегированной информацией в АСУ специального назначения // Труды XXX Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (30 июня — 1 июля 2011 г.) в 5-и т. Т. 4 / РАН, РАО. Серпухов: Серп. воен. ин-т, 2011. С. 166—169.
10. Ловцов Д. А., Кабелев Д. Б. Технология и проблемы рационального управления ключевой информацией в АСУ специального назначения / // Труды XXIX Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (24—25 июня 2010 г.) в 5-и т. Т. 4 / РАН, РАО. Серпухов: Серп. воен. ин-т, 2010. С. 144—148.
11. Шилейко А. В., Кочнев В. Ф., Химушин Ф. Ф. Введение в информационную теорию систем. М.: Радио и связь, 1985.

КАЧЕСТВО СТАНДАРТИЗОВАННОЙ СИСТЕМЫ АЛГОРИТМОВ ШИФРОВАНИЯ ДАННЫХ В ГАС РФ «ПРАВОСУДИЕ»

Королев В.Т., Ловцов Д.А.*

Ключевые слова: основной шаг криптопреобразования, простая замена, гаммирование, имитовставка, привилегированная информация, ГАС РФ «Правосудие», ГОСТ, нетрадиционный информационный канал (НИК), качество.

Аннотация.

Цель работы: совершенствование научно-методической базы теории правовых режимов ограниченного доступа информационных ресурсов.

Метод: комплексный теоретико-сравнительный анализ криптографических средств обеспечения защищённости привилегированной информации от раскрытия.

Результаты: определены численные параметры и математические операции стандартизованных процедур криптопреобразования данных, в целом позволяющие оценить современное состояние проблемы обеспечения защищённости привилегированной информации в Государственной автоматизированной системе Российской Федерации (ГАС РФ) «Правосудие»; дана теоретическая сравнительная оценка качества алгоритмов шифрования по ГОСТ 28147-89 и DES-75; предложено для обеспечения требуемого уровня защищённости привилегированной информации в ГАС РФ «Правосудие», учитывая значительные возможности осуществления несанкционированного доступа по нетрадиционным информационным каналам, использовать криптографические алгоритмы ГОСТ 28147-89 как во внутреннем — закрытом контуре, так и во внешнем — публичном контуре информационного взаимодействия.

DOI: 10.21681/1994-1404-2018-1-49-59

В Государственной автоматизированной системе Российской Федерации (ГАС РФ) «Правосудие» осуществляется защищённый обмен привилегированной информацией на основе применения криптографических алгоритмов в корпоративной телематической и локальных вычислительных сетях объектов автоматизации в условиях непрекращающихся попыток несанкционированного доступа, главным образом, по нетрадиционным (скрытым) информационным каналам [4]. Наиболее уязвимой при этом является информация, циркулирующая в телематической сети, в которой реализуются сетевые интернет-протоколы, использующие несовершенные криптографические алгоритмы [2, 5].

В Российской Федерации действует единый стандарт шифрования данных в сетях ЭВМ, в отдельных

вычислительных комплексах и компьютерах — ГОСТ 28147-89. Стандарт допускает как аппаратную, так и программную реализацию алгоритма, удовлетворяет требованиям криптографической стойкости и не накладывает ограничений на степень секретности защищаемой информации. Стандарт задает блочный симметричный алгоритм криптографического преобразования данных. Шифруемый массив данных разбивается на блоки, а секретный ключ используется и для зашифрования открытых информационных массивов (ИМ), и для расшифрования криптограмм — зашифрованных ИМ (ЗИМ).

Логика построения шифра и структура ключевой информации. В стандарте содержится описание алгоритмов двух уровней:

- на верхнем уровне иерархии находятся алгоритмы криптографических преобразований в следующих режимах: простой замены, гаммирова-

* **Королев Владимир Тимофеевич**, кандидат технических наук, профессор, почетный работник высшего профессионального образования Российской Федерации, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.

E-mail: timofeyich@mail.ru

Ловцов Дмитрий Анатольевич, доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, заместитель по научной работе директора Института точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.

E-mail: dal-1206@mail.ru

ния, гаммирования с обратной связью, выработки имитовставки;

- на нижнем уровне находятся два алгоритма, называемых базовыми циклами: цикл шифрования, цикл расшифрования (каждый из базовых циклов представляет собой многократное повторение одной и той же процедуры, называемой основным шагом криптографического преобразования).

Ключевая информация, используемая в алгоритмах стандарта, состоит из двух структур данных: собственно ключа шифрования и таблицы замен.

Ключ шифрования — двоичный код K длиной в 256 разрядов, формат которого показан в табл. 1. В первой строке таблицы — номера j разрядов кода K , а во второй — цифры k_j , ($j = \overline{0, 255}$) кода K .

Таблица 1

	255	254	...	0
$K =$	k_{255}	k_{254}	...	k_0

Таблица 2

	31	30	...	0
$K7 =$	k_{255}	k_{254}	...	k_{224}
$K6 =$	k_{223}	k_{222}	...	k_{192}
$K5 =$	k_{191}	k_{190}	...	k_{160}
$K4 =$	k_{159}	k_{158}	...	k_{128}
$K3 =$	k_{127}	k_{126}	...	k_{96}
$K2 =$	k_{95}	k_{94}	...	k_{64}
$K1 =$	k_{63}	k_{62}	...	k_{32}
$K0 =$	k_{31}	k_{30}	...	k_0

Таблица 3

	63	62	...	0
$N =$	n_{63}	n_{62}	...	n_0

i записан элемент замены — четырехразрядное целое положительное двоичное число $0 \leq H_{ij} < 2^4$. Общий размер таблицы замен составляет 512 разрядов (4 разряда $\times$ 16 элементов $\times$ 8 строк).

Основной шаг криптографического преобразования. Весь массив данных, подлежащих шифрованию, разбивают на отдельные блоки длиной в 64 разряда. Основной шаг криптографического преобразования задает алгоритм обработки одного блока данных N , формат которого показан в табл. 3.

На рис. 1 представлена функциональная схема алгоритма для основного шага. Этот алгоритм многократно используется в базовых циклах.

Поэтому блок 0 алгоритма имеет вход, на который подаются:

- очередной блок данных N длиной в 64 разряда;
- очередной 32-разрядный фрагмент ключа K .

В блоке 0 определяются исходные данные для реализуемого основного шага:

- число G получает значение K текущего ключевого фрагмента кода K : или $K0$, или $K1$, или ..., или $K7$, номер I ключевого фрагмента K определяется на входе в блок 0;
- преобразуемый блок данных N длиной в 64 разряда (его формат показан выше) разбивается на две части по 32 разряда каждая: $N2$ — старшая (табл. 4) и $N1$ — младшая (табл. 5).

Таблица 4

	31	30	...	0
$N2 =$	n_{63}	n_{62}	...	n_{32}

Таблица 5

	31	30	...	0
$N1 =$	n_{31}	n_{30}	...	n_0

Таблица 6

	31	30	...	0
$S =$	s_{31}	s_{30}	...	s_0

Полученные коды в процедуре основного шага выступают как целые, положительные двоичные числа: $0 \leq N2, N1 < 232$.

Так определяются координаты ячейки с элементом замены — числом $H_{L,SL}$. Это число и заменяет содержимое кода $SL := H_{L,SL}$.

Таблица 7

S		$\begin{matrix} j \\ i \end{matrix}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	S	
			S0	3	0	4	A	9	2	D	8	0	E	6	B	1	C	7	F	5
S1	F	1	E	B	4	C	6	D	F	A	2	3	8	1	0	7	5	9	9	S1
S2	9	2	5	8	1	D	A	3	4	2	E	F	C	7	6	0	9	B	F	S2
S3	C	3	7	D	A	1	0	8	9	F	E	4	6	C	B	2	5	3	B	S3
S4	4	4	6	C	7	1	5	F	D	8	4	A	9	E	0	3	B	2	5	S4
S5	0	5	4	B	A	0	7	2	1	D	3	6	8	5	9	C	F	E	4	S5
S6	3	6	D	B	4	1	3	F	5	9	0	A	E	7	6	8	2	C	1	S6
S7	E	7	1	F	D	0	5	7	A	4	9	2	3	E	6	B	8	C	8	S7

Таблица 8

		31	30	...	11	10	9	...	1	0
число сдвигов	0	$S=S_{31}$	S_{30}	...	S_{11}	S_{10}	S_9	...	S_1	S_0
	1	$S=S_{30}$	S_{29}	...	S_{10}	S_9	S_8	...	S_0	S_{31}
	2	$S=S_{29}$	S_{28}	...	S_9	S_8	S_7	...	S_{31}	S_{30}
	...	...	...	...	...	...	...	...	...	...
	11	$S=S_{20}$	S_{19}	...	S_0	S_{31}	S_{30}	...	S_{22}	S_{21}

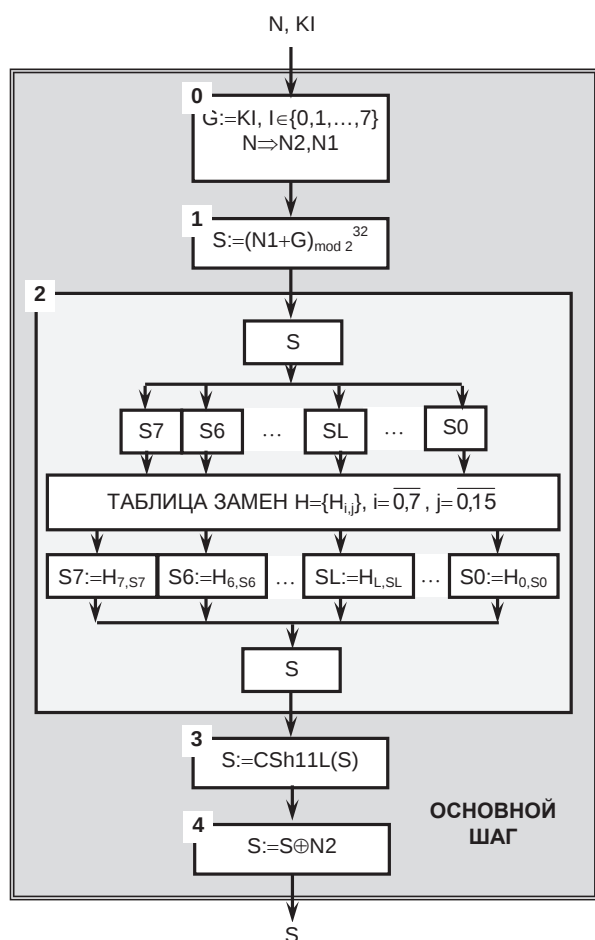


Рис. 1. Алгоритм для основного шага

В блоке 1 (см. рис. 1) выполняется операция сложения чисел N1 и G по модулю 232. Результатом этой операции будет число S (табл. 6). Далее

(блок 2) производится простая замена кода S на содержимое таблицы замен. Для этого 32-разрядный код S разбивается на восемь четырехразрядных фрагментов S7, S6, ..., S0. Номер L фрагмента SL определяет номер строки таблицы замен, а само число SL задает номер ячейки в строке номер L, из которой извлекается элемент замены, а именно, i:=L, L∈{0,1,...,7}, j:=SL, SL∈{0,1,...,15}.

Численный пример. Представим числа S, SL и HL,SL в шестнадцатеричной системе счисления (табл. 7). Слева в колонке S представим исходные значения фрагментов S0, S1, ..., S7. В каждой строке таблицы замен выделены элементы замены HL,SL. Справа в колонке S представлены результаты простой замены.

Блок 3 (см. рис. 1): здесь над полученным в блоке 2 кодом S выполняется циклический (C) сдвиг (Sh) на одиннадцать разрядов (11) влево (L) (т.е. в сторону старших разрядов). Смысл этой операции поясняется табл. 8.

В блоке 4 над символами sv и nv в одноименных разрядах кодов S и N2 выполняется логиче-

ская операция $\oplus$ — суммирование по модулю 2. Результат работы алгоритма основного шага — код S — выводится из блока 4.

Базовые циклы построены из основных шагов. В очередной реализации основного шага используется один из восьми 32-разрядных фрагментов ключа K . По соображениям стойкости шифра в каждом базовом цикле ключ K должен быть использован полностью, а каждый из его фрагментов должен быть использован одинаковое число раз (не менее двух).

Цикл зашифрования. На зашифрование подается ИМ открытых данных, который разбивается на блоки открытых данных (БОД), длиной в 64 разряда каждый: $БОД_m, БОД_{m-1}, \dots, БОД_m, \dots, БОД_1$.

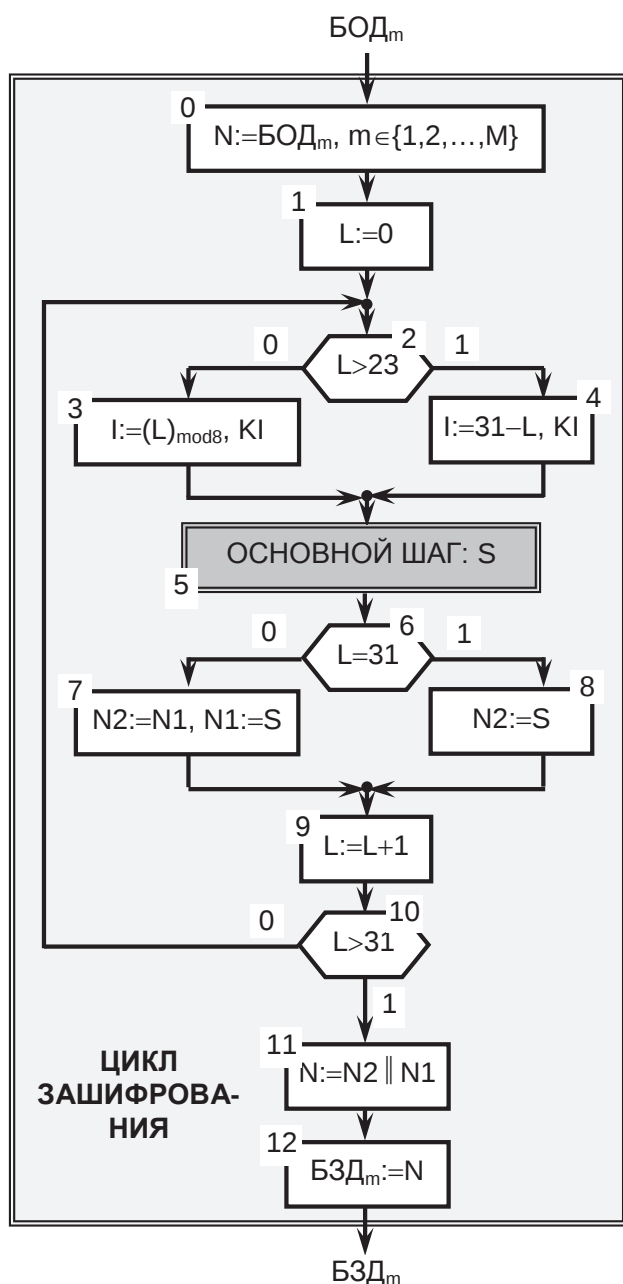


Рис. 2. Алгоритм цикла зашифрования

На рис. 2. представлена функциональная схема алгоритма цикла зашифрования. Этот цикл предназначен для зашифрования одного текущего блока БОД_m и состоит в том, что фрагмент алгоритма между блоками 2 и 9 (тело цикла, важнейшим блоком которого является блок 5 — «Основной шаг») повторяется 32 раза. Очередной блок открытых данных БОД_m подается на вход цикла зашифрования (см. рис. 2).

В блоке 0 коду N придается значение БОД_m. Значение $m \in \{1, 2, \dots, M\}$ определено до входа в цикл зашифрования. В блоке 1 счетчику циклов L задают начальное значение 0. В блоке 2 проверяется условие $L < 23$. Дело в том, что на первых 24 циклах (когда условие в блоке 2 не выполняется) в блок 5 — «Основной шаг» фрагменты ключа подаются в естественном порядке следования: $K_0, K_1, \dots, K_7$. Это достигается тем, что сейчас номер ключевого фрагмента I формируется в блоке 3 так, что при $0 \leq L \leq 23$ трижды получаем последовательность номеров $I = 0, 1, \dots, 7$ и последовательность фрагментов ключа: $K_0, K_1, \dots, K_7$.

В последних восьми циклах, когда $24 \leq L \leq 31$, в блок 5 — «Основной шаг» подаются фрагменты ключа в обратном порядке следования: $K_I = K_7, K_6, \dots, K_0$. Это достигается тем, что в этих циклах значение I формируется в блоке 4, последовательность номеров: $I = 7, 6, \dots, 0$, а вместе с ней и последовательность фрагментов ключа: $K_I = K_7, K_6, \dots, K_0$.

При полученном в блоке 3 или в блоке 4 значении фрагмента ключа K_I реализуется блок 5 алгоритма — «Основной шаг». Результатом его работы будет код S .

В блоке 6 проверяется условие $L = 31$. Во всех циклах, кроме последнего (номер которого и будет 31) реализуется блок 7. Код N_2 получает значение кода N_1 , а сам код N_1 получает значение S . В последнем цикле, когда условие в блоке 6 выполняется, реализуется блок 8 алгоритма. Код N_2 получает значение S , сформированное в последнем цикле, а значение кода N_1 остается тем, которое он получил в предпоследнем цикле.

В блоке 9 значение счетчика цикла L увеличивается на единицу, а в блоке 10 проверяется условие окончания цикла зашифрования. Пока оно не выполняется, управление передается на блок 2, и тело цикла реализуется ещё один раз. Как только условие в блоке 10 выполняется, реализуется блок 11 алгоритма, а именно, путем конкатенации (соединения) кодов N_2 и N_1 (символ этой операции: $\parallel$) формируется код N зашифрованных данных. Полученное значение N и будет текущим блоком зашифрованных данных — БЗД_m, который и

выводится из блока 12 как результат реализации одного цикла зашифрования.

Цикл расшифрования. На расшифрование подается зашифрованный ИМ (ЗИМ), который разбивается на блоки зашифрованных данных БЗД, длиной в 64 разряда каждый: $БЗД_M, БЗД_{M-1}, \dots, БЗД_m, \dots, БЗД_1$.

На рис. 3 представлена функциональная схема алгоритма цикла расшифрования. Этот цикл предназначен для расшифрования одного текущего блока $БЗД_m$ и состоит в том, что фрагмент алгоритма между блоками 2 и 9 (тело цикла, важнейшим блоком которого является блок 5 — «Основной шаг») повторяется 32 раза. Как видно, расшифрование ЗИМ производится практически по тому же алгоритму, что и зашифрование открытых ИМ (см. рис. 2).

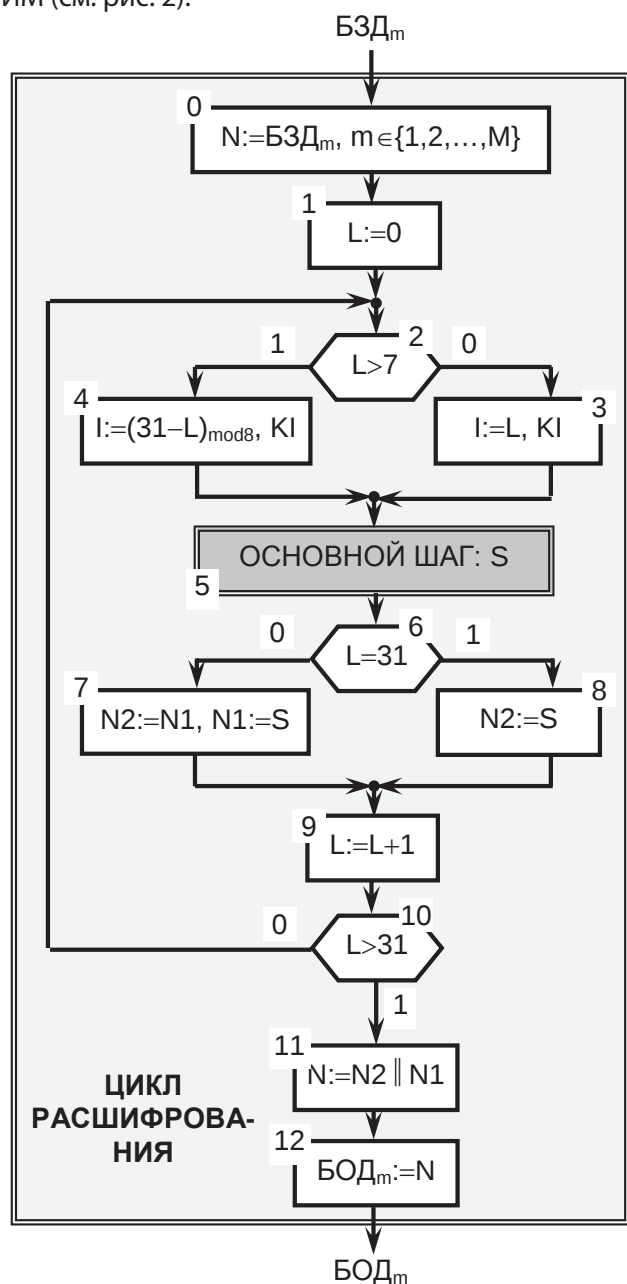


Рис. 3. Алгоритм цикла расшифрования

Очередной блок зашифрованных данных $БЗД_m$ подается на вход цикла расшифрования (с. рис. 3). В блоке 0 коду N придается значение $БЗД_m$. Значение $m \in \{1, 2, \dots, M\}$ определено до входа в цикл расшифрования. В блоке 1 счетчику циклов L задают начальное значение 0. В блоке 2 проверяется условие $L < 7$. Дело в том, что на первых 8 циклах (когда условие в блоке 2 не выполняется) в блок 5 — «Основной шаг» фрагменты ключа подаются в естественном порядке следования: $K_0, K_1, \dots, K_7$. Это достигается тем, что сейчас номер ключевого фрагмента I формируется в блоке 3 так: $I := L$, т.е. при $0 \leq L \leq 7$ получается последовательность номеров $I = 0, 1, \dots, 7$ и последовательность фрагментов ключа: $KI = K_0, K_1, \dots, K_7$.

В следующих 24 циклах, когда $8 \leq L \leq 31$, в блок 5 — «Основной шаг» подаются фрагменты ключа в обратном порядке следования: $K_7, K_6, \dots, K_0$. Это достигается тем, что в этих циклах в блоке 4 номер ключевого фрагмента I формируется так: $I := (31 - L) \bmod 8$, т.е. при $8 \leq L \leq 31$ трижды формируется последовательность номеров: $I = 7, 6, \dots, 0$, а вместе с ней и последовательность фрагментов ключа: $KI = K_7, K_6, \dots, K_0$.

При полученном в блоке 3 или в блоке 4 значении фрагмента ключа KI реализуется блок 5 — «Основной шаг» алгоритма. Результатом его работы будет код S . В блоке 6 проверяется условие $L = 31$. Во всех циклах, кроме последнего (номер которого и будет 31) реализуется блок 7. Код N_2 получает значение кода N_1 , а сам код N_1 получает значение S . В последнем цикле, когда условие в блоке 6 выполняется, реализуется блок 8 алгоритма. Код N_2 получает значение S , сформированное в последнем цикле, а значение кода N_1 остается тем, которое он получил в предпоследнем цикле.

В блоке 9 значение счетчика цикла L увеличивается на единицу, а в блоке 10 проверяется условие окончания цикла расшифрования. Пока оно не выполняется, управление передается на блок 2, и тело цикла реализуется еще один раз. Как только условие в блоке 10 выполняется, реализуется блок 11 алгоритма, а именно, путем конкатенации (соединения) кодов N_2 и N_1 (символ этой операции: $||$) формируется код N расшифрованных данных. Полученное значение N и будет текущим блоком расшифрованных данных $БЗД_m$, который и выводится из блока 12 как результат реализации одного цикла расшифрования.

Режим простой замены. На рис. 4 приведена функциональная схема алгоритма зашифрования в режиме простой замены. Как уже говорилось, на зашифрование подается ИМ открытых данных (ОД).

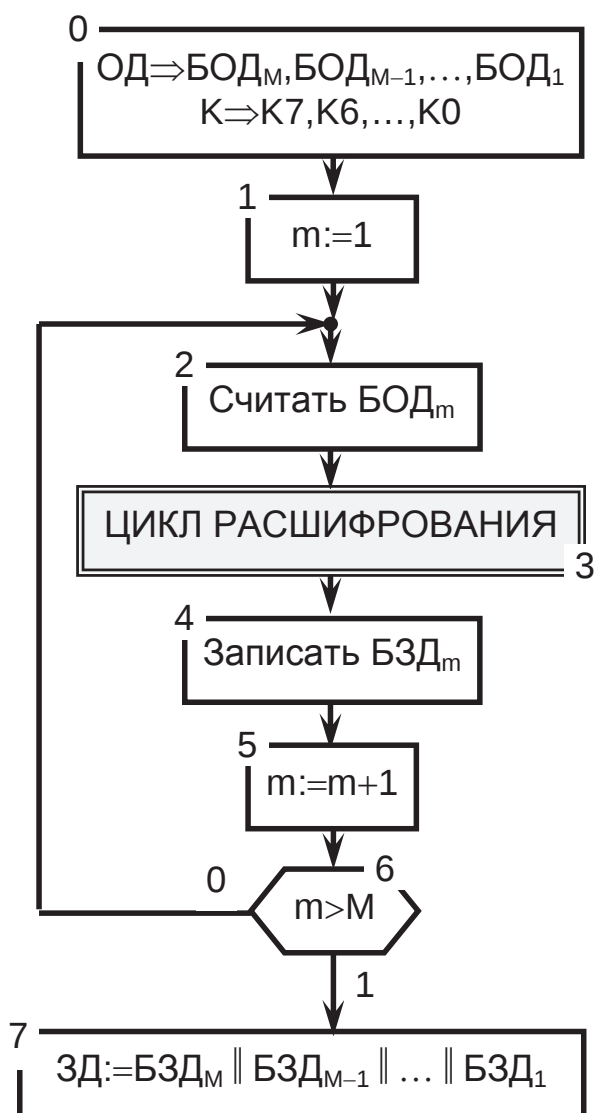


Рис. 4. Алгоритм зашифрования

В блоке 0 производится декомпозиция ($\Rightarrow$) ИМ на M блоков открытых данных: БОД_М, БОД_{М-1}, ..., БОД₁, длиной в 64 разряда каждый. Здесь же и 256-разрядный код ключа K подвергается декомпозиции на ключевые фрагменты: $K_7, K_6, \dots, K_0$, длиной в 32 разряда каждый.

В блоке 1 алгоритма счетчик блоков открытых данных m получает начальное значение 1. Далее (блок 2 алгоритма) считывается очередной блок БОД_м, который подается на цикл зашифрования (блок 3). Результатом работы цикла зашифрования будет очередной блок зашифрованных данных БЗД_м, который фиксируется в блоке 4. В блоке 5 показания счетчика m увеличивают на единицу. В блоке 6 анализируется условие окончания обработки ИМ. Пока оно не выполняется, управление передается на блок 2, и начинается зашифрование следующего блока открытых данных.

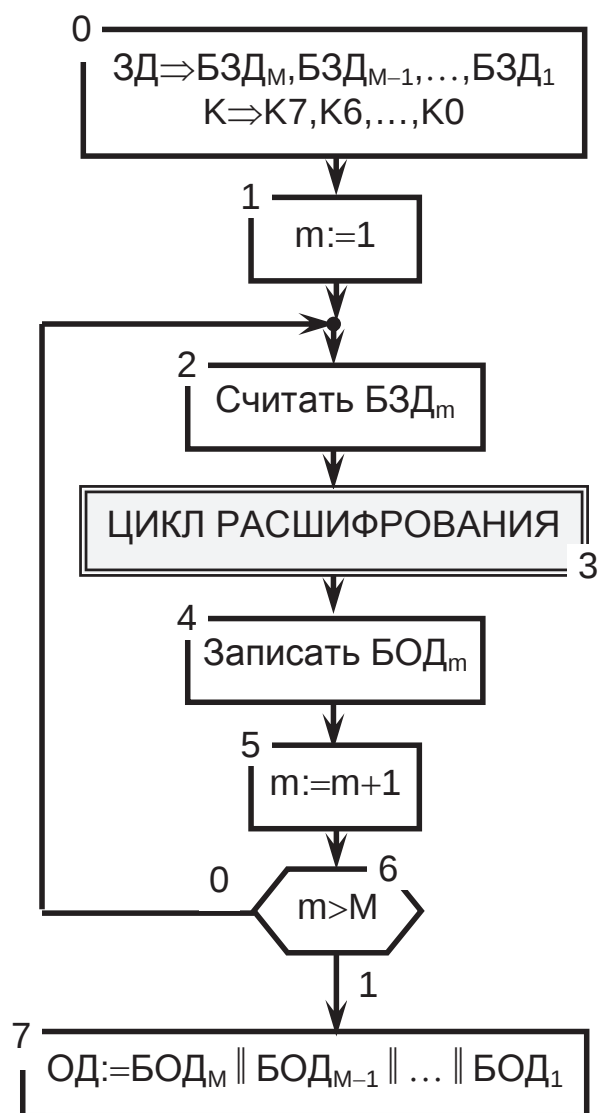


Рис. 5. Алгоритм расшифрования

Как только условие в блоке 6 выполнится, реализуется блок 7 алгоритма. Здесь путем конкатенации ($||$) блоков БЗД_М, БЗД_{М-1}, ..., БЗД₁ формируется массив зашифрованных данных.

На рис. 5 приведена функциональная схема алгоритма расшифрования в режиме простой замены. Как видно, построен он аналогично алгоритму на рис. 4. Отличие состоит в том, что на расшифрование в режиме простой замены подается ИМ зашифрованных данных (ЗД), а результатом работы этого алгоритма будет ИМ ОД.

Особенность режима простой замены заключается в том, что если длина ИМ открытых данных не кратна 64 разрядам, то последний блок БОД_М будет иметь длину менее 64 разрядов, и его нужно удлинять до 64 разрядов с тем, чтобы обрабатывать в режиме простой замены. Но тогда ЗИМ окажется длиннее ИМ открытых данных, что недо-

пустимо снижает стойкость шифра. Поэтому ГОСТ предписывает использовать режим простой замены исключительно для шифрования ключевой информации: ключа K и таблицы замен H , длина которых кратна 64 разрядам.

Режим гаммирования. Суть гаммирования по ГОСТ 28147-89 состоит в том, что зашифровывают не сам блок данных, а некоторое число, вырабатываемое специальным генератором, и потом результат зашифрования — гамму — накладывают на ИМ (блок данных), а именно, над кодами гаммы и ИМ выполняют некоторую операцию. Так получают зашифрованный ИМ — ЗИМ [3]. Расшифрование ЗИМ состоит в наложении на него той же гаммы повторно. Следовательно, процедуры зашифрования и расшифрования в режиме гаммирования одинаковы. Поэтому можно описать применение режима гаммирования к ИМ D (открытых или зашифрованных). А результатом выполнения этого режима будет ИМ гаммированных данных GD (зашифрованных или открытых).

На рис. 6 показана общая схема реализации режима гаммирования, который используется в стандарте. Процедуры зашифрования и расшифрования в режиме гаммирования одинаковы. Поэтому ниже описано применение режима гаммирования к ИМ данных D (открытых или зашифрованных). А результатом выполнения этого режима будет массив гаммированных данных GD (зашифрованных или открытых).

Исходный массив данных D объемом в R разрядов (рис. 6,а) подвергается декомпозиции на M отдельных блоков: $D_M, D_{M-1}, \dots, D_1$ (рис. 6,б). При этом объем первых $M-1$ блоков составляет точно 64 разряда, а блок D_M имеет длину в $r < 64$ разрядов.

Над содержимым одноименных разрядов кодов D_m и G_m ($m=1, \dots, M$) выполняется логическая операция $\oplus$ суммирование по модулю 2.

Для каждого из этих блоков данных формируется своя гамма длиной в 64 разряда: $G_M, G_{M-1}, \dots, G_1$ (рис. 6,в).

Если блок D_M имеет длину $r < 64$ разрядов, то старшие $(64-r)$ разрядов кода G_M отбрасываются (рис. 6,в).

Результатом этой операции будет ансамбль блоков гаммированных (зашифрованных или расшифрованных) данных: $GD_M, GD_{M-1}, \dots, GD_1$ (рис. 6,г).

Путем конкатенации этих блоков получают результат режима гаммирования — массив GD объемом в R разрядов (рис. 6,д).

Особенностью режима гаммирования, определенного стандартом, является то, что очередная гамма G_m формируется с использованием преды-

дущей гаммы G_{m-1} ($m=1, \dots, M$). Иницируется этот процесс с помощью нулевой гаммы G_0 . Код G_0 получают путем зашифрования в режиме простой замены некоторого числа SP длиной в 64 разряда, называемого синхропосылкой (начальным заполнением по терминологии стандарта). В качестве значения SP можно использовать тот или иной отсчет времени (скажем, перед началом процедуры зашифрования). Код SP должен передаваться получателю криптограммы для того, чтобы можно было выполнить её расшифрование.

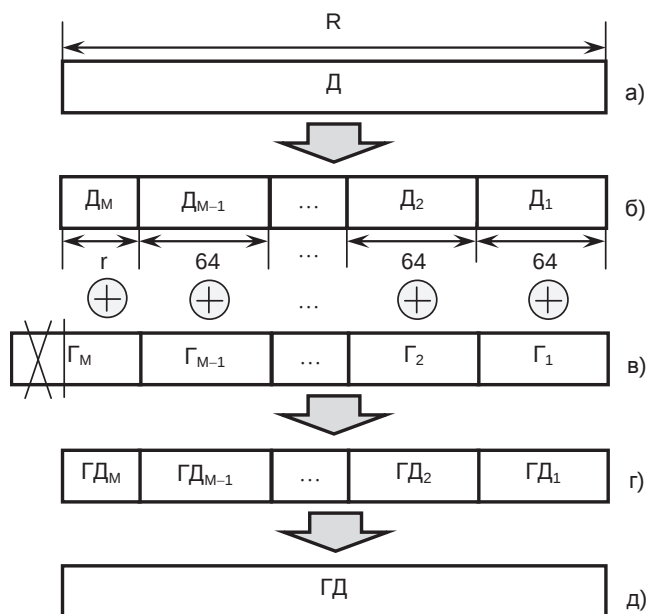


Рис. 6. Режим гаммирования

При формировании гамм выполняются операции суммирования по модулю 2^{32} и по модулю $(2^{32}-1)$. В стандарте под этими операциями понимается следующее.

Имеем числа A и B такие, что $0 \leq A, B \leq 2^{32}-1$. Для их записи достаточно 32 разрядов с номерами 31, 30, ..., 0. Сумма этих чисел $C = A+B$ лежит в пределах

$$0 \leq C \leq 2 \times (2^{32}-1), \quad (1)$$

и для записи C необходимо 33 разряда с номерами 32, 31, 30, ..., 0 (рис. 7).

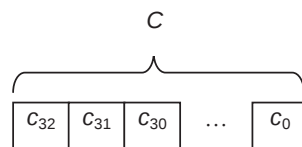


Рис. 7. Запись числа C

Операция $(C)_{\text{mod } 2^{32}}$ в математике определена так: $(C)_{\text{mod } 2^{32}} = C - D \times 2^{32}$,

где D целое положительное число.

Для тех значений C , которые определены неравенствами (1):

$$D = \begin{cases} 0 & \text{при } C < 2^{32}, c_{32} = 0, \\ 1 & \text{при } C \geq 2^{32}, c_{32} = 1. \end{cases} \quad (2)$$

В соответствии с этим стандарт так определяет операцию $(C)_{\text{mod } 2^{32}}$:

$$(C)_{\text{mod } 2^{32}} = \begin{cases} C, & \text{если } C < 2^{32}, \\ C - 2^{32}, & \text{если } C \geq 2^{32}. \end{cases} \quad (3)$$

Это означает, что $(C)_{\text{mod } 2^{32}}$ — суть содержимое разрядов с номерами 31, 30, ..., 0 в записи числа C (рис. 8).

Таким образом, операция $(A+B)_{\text{mod } 2^{32}}$ выполняется за один акт суммирования: сумму $A+B$ фиксируют в разрядах с номерами 31, 30, ..., 0, а старшую цифру c_{32} суммы игнорируют (рис. 8).

Операция $(C)_{\text{mod } (2^{32}-1)}$ в стандарте определена так:

$$(C)_{\text{mod } (2^{32}-1)} = \begin{cases} C, & \text{если } C < 2^{32}, \\ C - 2^{32} + 1, & \text{если } C \geq 2^{32}. \end{cases} \quad (4)$$

Сравнив (3) и (4), можно сказать, что по стандарту

$$(C)_{\text{mod } (2^{32}-1)} = (C)_{\text{mod } 2^{32}} + c_{32}. \quad (5)$$

При $c_{32} = 0$ (когда $C < 2^{32}$) получаем первую строку формулы (4), а при $c_{32} = 1$ (когда $C \geq 2^{32}$) — ее вторую строку.

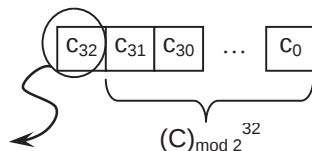


Рис. 8. Результат операции $(C)_{\text{mod } 2^{32}}$

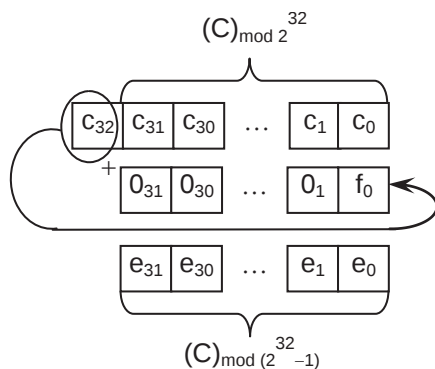


Рис. 9. Результат операции $(C)_{\text{mod } 2^{32}}$

Таким образом, операция $(A+B)_{\text{mod } (2^{32}-1)}$ выполняется за два акта суммирования: в первом акте получают $(A+B)_{\text{mod } 2^{32}}$, а во втором к этому результату прибавляют число $F = 0_{31} 0_{30} \dots 0_1 f_0$, где $f_0 = c_{32}$ (рис. 9). Как видно, в операции цифра c_{32} не отбрасывается, а используется для формирования кода $(C)_{\text{mod } (2^{32}-1)}$.

На рис. 10 приведена функциональная схема алгоритма для режима простого гаммирования. В блоке 0 фиксируется код синхропосылки SP , массив данных D подвергается декомпозиции на M блоков $D_M, D_{M-1}, \dots, D_1$, а код ключа K — на восемь фрагментов: $K_7, K_6, \dots, K_0$.

В блоках 1, 2 и 3 производится зашифрование кода SP в режиме простой замены и получение нулевой гаммы Γ_0 . В блоке 4 счетчику циклов гаммирования m задают начальное значение. Блоки 6, 7, ..., 11 составляют тело цикла гаммирования. В блоке 5 код Γ_0 путем декомпозиции разбивается на две части: старшую Γ_{20} и младшую Γ_{10} .

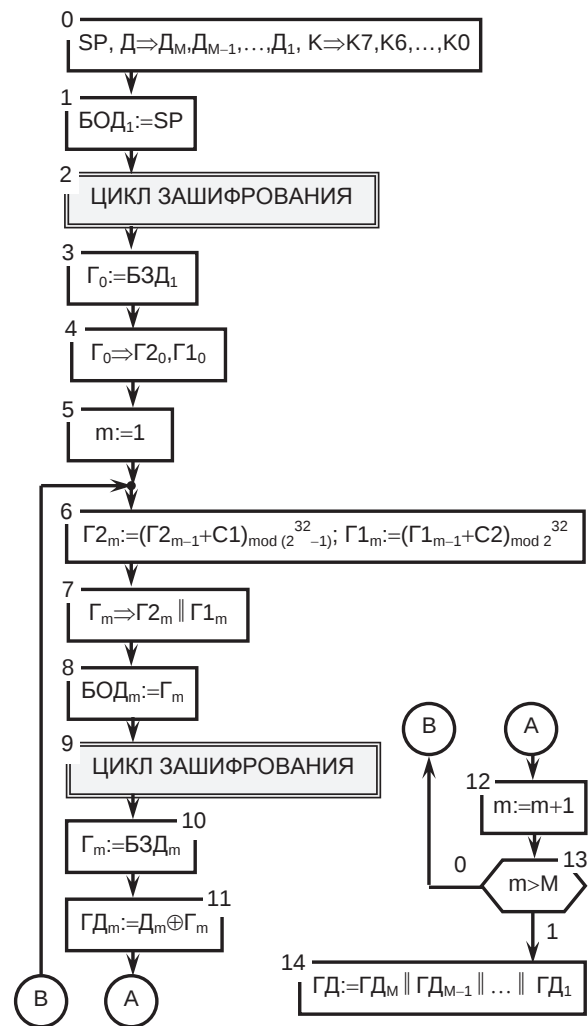


Рис. 10. Алгоритм для режима простого гаммирования

В блоке 6 формируются:

- текущий код Γ_{2_m} как сумма по модулю $(2^{32}-1)$ предыдущего значения $\Gamma_{2_{m-1}}$ и константы $C1$,
- текущий код Γ_{1m} как сумма по модулю 232 предыдущего значения $\Gamma_{1_{m-1}}$ и константы $C2$.

Двоичные 32-разрядные коды $C2$ и $C1$ определены в стандарте в шестнадцатеричном виде (в скобках десятичные значения):

$C2 = 01010101$ (16 843 009);

$C1 = 01010104$ (16 843 012).

В блоке 7 путем конкатенации кодов Γ_{2_m} и Γ_{1_m} формируется код текущей гаммы Γ_m . В блоках 8, 9 и 10 код Γ_m зашифровывают в режиме простой замены. В блоке 11 код Γ_m накладывается на код D_m , а именно, над одноименными разрядами этих кодов выполняется логическая операция $\oplus$ — суммирование по модулю 2. Так формируется блок номер m гаммированных данных ΓD_m .

В блоке 12 показания счетчика циклов гаммирования m увеличиваются на единицу, а в блоке 13 проверяется условие окончания циклов гаммирования. Пока условие $m > M$ не выполняется, управление передается на блок 5, и реализуется еще один цикл гаммирования. Как только условие $m > M$ выполнится, реализуется блок 14. Здесь путем конкатенации блоков гаммированных данных: $\Gamma D_M, \Gamma D_{M-1}, \dots, \Gamma D_1$ формируется массив ΓD гаммированных данных.

Режим гаммирования с обратной связью. Этот режим отличается от режима простого гаммирования тем, что для формирования очередной гаммы Γ_m используют не код предыдущей гаммы Γ_{m-1} , а код предыдущего блока гаммированных данных ΓD_{m-1} . Функциональная схема алгоритма для режима гаммирования с обратной связью приведена на рис. 11.

В блоке 0 фиксируется код синхропосылки SP , массив данных D подвергается декомпозиции на M блоков: $D_M, D_{M-1}, \dots, D_1$, а код ключа K — на восемь фрагментов: $K7, K6, \dots, K0$.

Код синхропосылки SP становится исходным значением для кода Γ_1 (блок 1). В блоке 2 счетчику циклов гаммирования задают начальное значение 1. В блоках 3, 4, ..., 7 текущее значение Γ_m зашифровывают в режиме простой замены. Так получают очередную гамму Γ_m . В блоке 6 над одноименными разрядами гаммы Γ_m и блока данных D_m выполняют логическую операцию $\oplus$ — суммирование по модулю 2. Так формируется очередной блок гаммированных данных ΓD_m . В блоке 7 полученное значение ΓD_m придают коду Γ_m . Из него в следующем цикле будет сформирована новая гамма. В этом и состоит обратная связь при гаммировании.

В блоке 8 показания счетчика циклов гаммирования m увеличиваются на единицу, а в блоке 9 проверяется условие окончания циклов гаммирования. Пока условие $m > M$ не выполняется, управление передается на блок 3, и реализуется еще один цикл гаммирования. Как только условие $m > M$ выполнится, реализуется блок 10. Здесь путем конкатенации блоков гаммированных данных $\Gamma D_M, \Gamma D_{M-1}, \dots, \Gamma D_1$ формируется массив ΓD гаммированных данных.

Отметим особенности двух последних режимов. При зашифровании данных путем простого гаммирования блоки ΓD_m ($m=1, \dots, M$) формируются независимо друг от друга. Криптоаналитик-злоумышленник, не имея ключа K , не сможет раскрыть криптограмму. Однако он может вносить те или иные изменения в её текст путем замены содержимого отдельных разрядов (заменить нули единицами и/или наоборот). При расшифровке такой криптограммы внесенные изменения останутся в открытом тексте, и их трудно обнаружить.

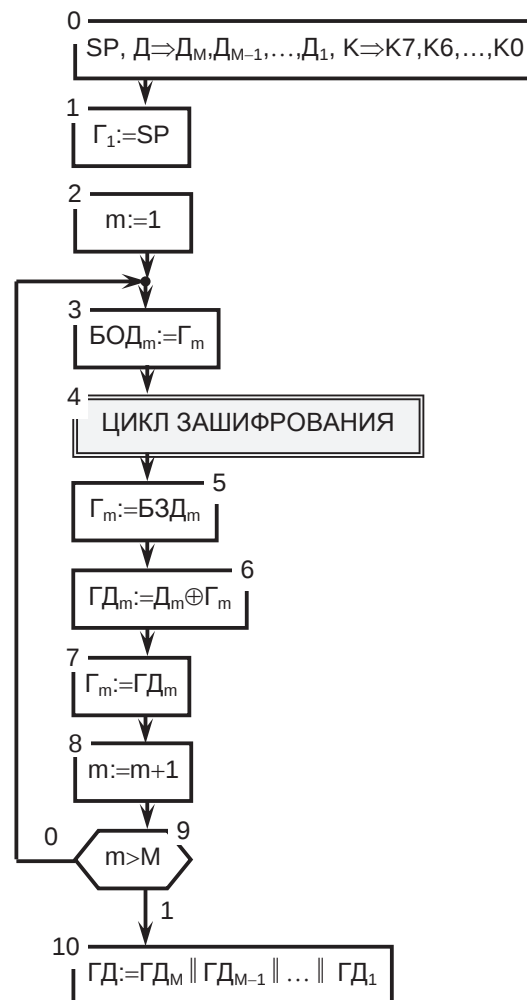


Рис. 11. Алгоритм для режима гаммирования с обратной связью

При зашифровании данных в режиме гаммирования с обратной связью следующий блок гаммированных данных $ГД_m$ формируется с использованием предыдущего блока $ГД_{m-1}$. Изменения, внесенные в блок $ГД_m$, при расшифровке такой криптограммы вызовут изменения во всех последующих блоках открытых данных, и такое повреждение данных легко заметить.

Режим выработки имитовставки. Имитовставка V — это контрольная кодовая комбинация, которая позволяет обнаруживать все случайные или преднамеренные изменения в принятой криптограмме после её расшифровки. Вырабатывается имитовставка из ИМ открытых данных, подлежащих зашифрованию. Имитовставка передается получателю вместе с ИМ зашифрованных данных. После расшифрования ЗИМ из полученного ИМ открытых данных формируют свою имитовставку V^0 . По результатам сравнения кодов V и V^0 делается вывод о наличии или отсутствии внесенных в исходный ИМ изменений.

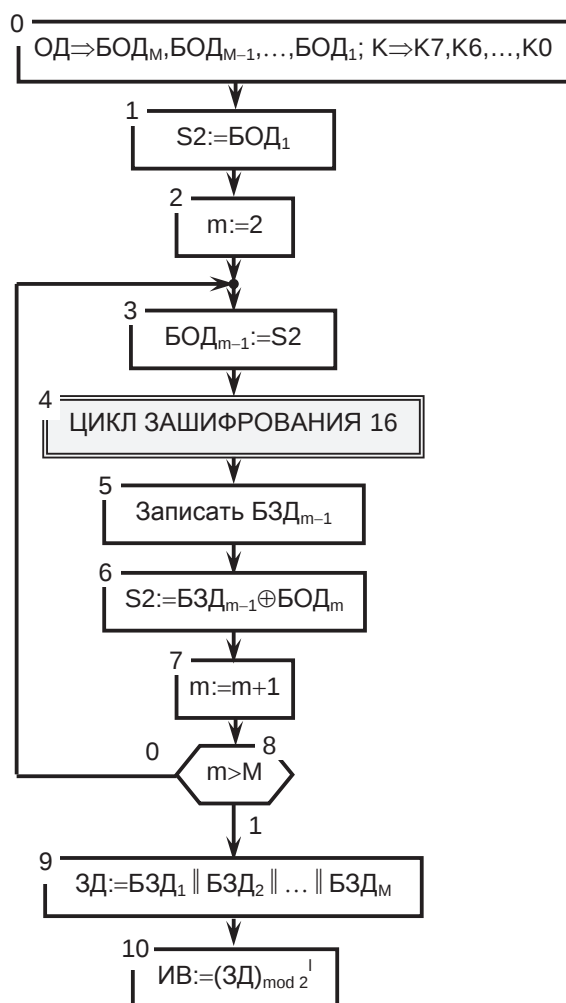


Рис. 12. Алгоритм для режима выработки имитовставки

На рис. 12 приведена функциональная схема алгоритма для режима выработки имитовставки. ИМ открытых данных подвергается декомпозиции на M блоков: БОД $_M$, БОД $_{M-1}$, ..., БОД $_1$, а код ключа K — на фрагменты: K_7 , K_6 , ..., K_0 (блок 0). Для режима выработки имитовставки $M \geq 2$.

В блоке 1 вспомогательной переменной $S2$ придают значение БОД $_1$. В блоке 2 счетчику циклов выработки имитовставки m задают начальное значение 2. Блоки 3, 4, 5, 6 составляют тело цикла выработки имитовставки. Текущее значение $S2$ присваивают блоку БОД $_{m-1}$, который в блоке 4 подвергается зашифрованию в режиме простой замены. Особенностью режима выработки имитовставки является то, что в цикле зашифрования (блок 4 — «Зашифрование 16») основной шаг реализуется не 32, а 16 раз.

Результат зашифрования БЗД $_{m-1}$ фиксируется в блоке 5, а в блоке 6 над одноименными разрядами кодов текущего результата зашифрования БЗД $_{m-1}$ и очередного блока открытых данных БОД $_m$ выполняют логическую операцию $\oplus$ — суммирование по модулю 2. Результатом этой операции будет код $S2$ на следующий цикл выработки имитовставки.

В блоке 7 показания счетчика m увеличивают на единицу, а в блоке 8 проверяется условие окончания циклов выработки имитовставки. Пока условие $m > M$ не выполняется, управление передается на блок 3, и реализуется еще один цикл выработки имитовставки. Как только условие $m > M$ выполнится, реализуется блок 9. Здесь путем конкатенации блоков зашифрованных данных: БЗД $_M$, БЗД $_{M-1}$, ..., БЗД $_1$ формируется массив $ЗД$ зашифрованных данных.

В блоке 10 формируется собственно код имитовставки (ИВ) путем выделения содержимого l младших разрядов кода $ЗД$ (операция $(ЗД)_{mod 2^l}$). Длина l кода ИВ определяется действующими криптографическими требованиями. При этом учитывается, что вероятность навязывания ложных данных $p_n = 2^{-l}$. Например, при $l = 32$ эта вероятность $p_n = 0,233 \times 10^{-9}$.

Сравнительный анализ ГОСТ 28147-89 и американского стандарта DES-75 (Data Encryption Standard 1975 year). Система блочного шифрования DES [1, 3, 6—8] на основе принципов «рассеивания» (распространения влияния одного символа ИМ на множество символов ЗИМ с целью скрытия статистических свойств ИМ) и «перемешивания» (преобразования, усложняющего восстановление взаимосвязи статистических свойств

ИМ и ЗИМ) [9] остаётся на протяжении многих лет стандартом в США. Да и во всем мире еще долгое время будут использоваться системы шифрования на основе DES и ГОСТ, которые являются стойкими алгоритмами шифрования в том смысле, что неизвестно методов их взлома, кардинально отличающихся от метода сплошного перебора всех возможных значений ключей.

И тот, и другой алгоритм в режиме простой замены оперируют с блоками длиной в 64 разряда. Но у DES длина ключа составляет 56 разрядов по сравнению с 256 разрядами ключа ГОСТ. Кроме того, в DES всего 16 циклов шифрования, а в ГОСТ — 32 цикла.

Режим простой замены имеет недостатки. В частности, одинаковые блоки открытых данных на одном и том же ключе порождают одинаковые же блоки зашифрованных данных. А это дает некоторую информацию о тех данных, которые были зашифрованы. При использовании простой замены также легко произвести незаметную подмену одного зашифрованного блока другим блоком, зашифрованным на том же ключе.

Но в ГОСТ 28147-89, как известно, кроме режима простой замены, который используется только для генерации ключей, имеется еще и два режима гаммирования. Одинаковые блоки открытых данных порождают разные блоки гаммированных

данных, даже если используются одинаковые ключи, но разные синхропосылки. Кроме режимов зашифрования в ГОСТ предусмотрен режим выработки имитовставки, что позволяет обнаруживать подмены в ЗИМ.

Следовательно, есть основания полагать, что современные высокопроизводительные вычислительные средства дают возможность специальным службам, таким, например, как Агентство национальной безопасности США, раскрывать сообщения, зашифрованные по алгоритму DES [3]. Вместе с тем в отношении отечественного ГОСТ 28147-89 на сегодняшний день не известно никаких реальных подходов, позволяющих взломать шифр, не имея ключа.

Таким образом, представляется необходимым для обеспечения требуемого уровня защищённости циркулирующей в ГАС РФ «Правосудие» привилегированной информации использовать криптографические алгоритмы ГОСТ 28147-89 как во внутреннем — закрытом контуре, так и во внешнем — публичном контуре информационного взаимодействия территориально распределённых информационно-вычислительных сегментов объектов автоматизации: Верховного Суда РФ, судов общей юрисдикции, органов Судебного департамента, центров подготовки и обучения, центров поддержки и др.

Рецензент: Федичев Андрей Валерьевич, кандидат технических наук, директор ФБУ «Научный центр правовой информации при Министерстве юстиции Российской Федерации», Российская Федерация, г. Москва

E-mail: fedichev@scli.ru

Литература

1. Баричев С. Г., Гончаров В. В., Серов С. Е. Основы современной криптографии. М.: Горячая линия-Телеком, 2011. 175 с.
2. Ловцов Д. А. Проблема информационной безопасности ГАС РФ «Правосудие» // Российское правосудие. 2012. № 5. С. 103—109.
3. Ловцов Д. А. Контроль и защита информации в АСУ. М.: ВА им. Петра Великого, 1991. 172 с.
4. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74.
5. Ловцов Д. А. Информационная надёжность функционирования телематической сети ГАС РФ «Правосудие» // Правовая информатика. 2018. № 1.
6. Малюк А. А., Пазизин С. В., Погужин Н. С. Введение в защиту информации в автоматизированных системах. М.: Горячая линия-Телеком, 2011. 146 с.
7. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. М.: Горячая линия-Телеком, 2011. 232 с.
8. Хоффман Л. Дж. Современные методы защиты информации. М.: Сов. радио, 1980. 246 с.
9. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетики. М.: Иностранная литература, 1963. С. 333—402.

ГОСУДАРСТВЕННАЯ СИСТЕМА КООРДИНАЦИИ ИНФОРМАТИЗАЦИИ КАК МЕХАНИЗМ ФОРМИРОВАНИЯ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Троян (Фадеева) Н.А.*

Ключевые слова: информационные системы, информационное общество, правовая информация, базы данных, электронные государственные реестры, электронные государственные регистры, нормативный правовой акт, межведомственное электронное взаимодействие.

Аннотация.

В статье рассматриваются вопросы использования современных информационно-телекоммуникационных технологий для совершенствования доступа к информационным ресурсам Минюста России. Обсуждается актуальный вопрос в информационном законодательстве – отсутствие единого понятийного аппарата терминов и определений в сфере информационно-коммуникационных технологий. Затронуты важные вопросы унификации требований к созданию и эксплуатации государственных информационных систем. Рассматривается проблема единства законодательных норм, устанавливающих правовой режим федеральных информационных систем. Анализируется современное федеральное законодательство об информационных системах, сравниваются используемые подходы к нормативному закреплению целей создания.

DOI: 10.21681/1994-1404-2018-1-60-67

На современном этапе развития информационного общества использование информационно-коммуникационных технологий и информационных ресурсов приобретает все большую значимость.

Утверждение ряда программных документов доказывает актуальность поставленной Президентом России задачи по переходу на новый технологический уровень¹.

Сегодня деятельность органов и должностных лиц государственного и муниципального управления направлена на повышение качества предоставления государственных и муниципальных услуг, выбор и использование оптимальных

способов организации предоставления публичных услуг с учетом всех принципов и факторов, внедрение и развитие прогрессивных рыночных механизмов в сочетании с мерами социальной поддержки населения. Управление процессом организации и предоставлением государственных и муниципальных услуг является важнейшей составной частью государственного и муниципального управления.

Функция предоставления государственных и муниципальных услуг населению является первичной функцией в деятельности органов государственного и муниципального управления².

Одним из важнейших направлений региональной информатизации является обеспечение предоставления государственных и муниципальных услуг в электронной форме.

В 2010 г. для решения этих актуальных задач был принят Федеральный закон РФ № 210 от 27 июля (в ред. 03.07.2016) «Об организации

¹ Постановление Правительства РФ от 27 декабря 2012 г. № 1406 «О Федеральной целевой программе «Развитие судебной системы России на 2013–2020 годы» // Собрание законодательства Российской Федерации, 2013, № 1, ст. 13;

Распоряжение Правительства РФ от 1 ноября 2013 г. № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в РФ на 2014–2020 годы и на перспективу до 2025 года» // URL: <http://www.pravo.gov.ru>;

Послание Президента Федеральному Собранию 12 декабря 2012 года // URL: <http://kremlin.ru/events/president/news/17118>.

² Комментарий к Федеральному закону от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (постатейный) // (Амелин Р.В., Ведяев Е.С., Викулов А.М., Григорьева Е.А., Гребенникова А.А., Мокиев М.М., Филатова А.В., Чаннов С.Е.) // СПС «Консультант Плюс», 2014.

* Троян (Фадеева) Наталья Анатольевна, старший научный сотрудник федерального бюджетного учреждения «Научный центр правовой информации при Минюсте России», Российская Федерация, г. Москва.

E-mail: n-fadeeva@yandex.ru

предоставления государственных и муниципальных услуг»,³ который регламентирует вопросы государственной информатизации по нескольким важным направлениям:

- предоставление государственных услуг в электронной форме (ст. 10);
- создание Единого портала государственных услуг и государственной информационной системы государственных и муниципальных платежей (ст. 21 и 21.3);
- формирование инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме (ст. 19);
- создание базовых государственных информационных ресурсов, использование единой системы межведомственного электронного взаимодействия и подключаемых к ней региональных систем межведомственного электронного взаимодействия по межведомственному запросу органа, предоставляющего государственную услугу (ст. 7.1).

Реализация Федерального закона уже сегодня позволяет получить социально-экономический эффект в виде:

- повышения доступности государственных услуг;
- снижения коррупционных рисков за счет минимизации случаев прямого контакта граждан с должностными лицами органов государственной власти;
- сокращения расходов на содержание государственного аппарата за счет автоматизации ряда управленческих процессов (межведомственное взаимодействие, обработка входящей информации, подготовка необходимых документов);
- получения оперативной обратной связи без посещения органов власти и возможности контроля процесса предоставления услуги гражданами;
- удобства ведения общественного контроля деятельности федеральных органов государственной власти.

Нельзя оставить без внимания Концепцию региональной информатизации, утвержденной распоряжением Правительства Российской Федерации от 29.12.2014 № 2769-р⁴, где основными целями являются повышение качества жизни граждан

за счет использования информационных и телекоммуникационных технологий, выравнивание уровня развития информационного общества в субъектах Российской Федерации, а также формирование эффективной системы государственного управления на основе использования информационных и телекоммуникационных технологий. В число актуальных задач входит формирование региональной информационно-телекоммуникационной инфраструктуры, необходимой для информационного взаимодействия, а также обеспечение комплексного управления внедрением информационно-коммуникационных технологий в субъектах Российской Федерации.

Эта Концепция соответствует основным направлениям государственной политики в области информатизации, сформулированным в Стратегии развития информационного общества в Российской Федерации, утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212, Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года, утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, государственной программе Российской Федерации «Информационное общество (2011–2020 годы)», утвержденной постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)».

В начале 1990-х годов, когда законодательство в сфере информации, информационных и телекоммуникационных технологий только формировалось, основной задачей было создание информационного законодательства. В настоящее время направление развития несколько изменилось, начался новый его этап. Сейчас, когда массив законодательства в данной сфере достаточно велик, появилась необходимость другого системного подхода к нормотворчеству и перехода к ответственному преобразованию. Это тем более важно, что за период существования и применения законодательства в сфере информации, информационных и телекоммуникационных технологий отчетливо выявились упущения и пробелы, допущенные при разработке соответствующих законодательных актов, которые приводят к отрицательным последствиям.

Несмотря на интенсивное развитие законодательства в сфере информации, информационных и телекоммуникационных технологий, многие

³ Собрание законодательства Российской Федерации. 02.08.2010, № 31, ст. 4179.

⁴ Распоряжение Правительства Российской Федерации от 29.12.2014 № 2769-р // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 08.01.2015 // Собрание законодательства Российской Федерации, № 2, 12.01.2015, ст. 544.

проблемы все еще не решены, а по отдельным вопросам, как показала практика, требуется существенная корректировка уже принятых нормативных правовых актов. Поэтому такое направление региональной информатизации, как предоставление государственных и муниципальных услуг в электронной форме, тоже имеет ряд недостатков и нерешенных проблем.

По данным мониторинга качества предоставления государственных и муниципальных услуг в электронной форме за 2013 год, проведенного Министерством экономического развития Российской Федерации, формы получения указанных услуг в федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)» реализованы менее чем на 5 % от общего количества услуг органов государственной власти субъектов Российской Федерации, размещенных на Едином портале, при этом надо отметить, что большая часть функций неработоспособна, что приводит к невозможности дистанционного получения гражданами этих услуг.

По состоянию на начало 2014 года 40 % региональных порталов государственных и муниципальных услуг используют системы регистрации и авторизации, несовместимые с федеральной государственной информационной системой «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – Единая система идентификации и аутентификации), что приводит к невозможности для граждан использовать одну учетную запись для получения государственных и муниципальных услуг на разных порталах.

Значительные расходы были понесены на внедрение информационно-коммуникационных технологий в экономике и социальной сфере субъектов Российской Федерации, прежде всего в здравоохранении и образовании. Однако формирование информационно-телекоммуникационной инфраструктуры органов государственной власти, а также государственных и муниципальных учреждений часто осуществляется изолированно, не учитывает необходимость совместной работы информационных систем и не всегда направлено на повышение качества предоставляемых гражданам государственных и муниципальных услуг. Это приводит к необоснованному росту числа используемых программно-аппаратных решений,

избыточным расходам и снижает эффективность использования информационно-коммуникационных технологий в регионах.

За 2012–2015 годы расходы федеральных органов государственной власти на создание и использование информационно-телекоммуникационных технологий составили более 417 млрд рублей. Для повышения эффективности реализации планируемых мероприятий принято Постановление Правительства Российской Федерации от 14.11.2015 № 1235 «О федеральной государственной информационной системе координации информатизации» (вместе с Положением о федеральной государственной информационной системе координации информатизации⁵), утверждающее правила подготовки планов информатизации.

Приказом Министерства связи и массовых коммуникаций Российской Федерации № 120 от 03.05.2014 утверждены прилагаемые Требования, обеспечивающие технологическую совместимость информационных систем организаций, подключаемых к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме с указанной инфраструктурой, к каналу связи и используемым для его защиты средствам криптографической защиты информации, а также особенностей использования стандартов и протоколов при обмене данными в электронной форме между информационными системами указанных организаций и инфраструктурой⁶. Технологическая совместимость государственных информационных систем обеспечивает беспрепятственный обмен сведениями между органами власти в электронной фор-

⁵ Постановление Правительства Российской Федерации от 14.11.2015 № 1235 «О федеральной государственной информационной системе координации информатизации» // Собрание законодательства Российской Федерации, 23.11.2015, № 47, ст. 6599.

⁶ Приказ Министерства связи и массовых коммуникаций Российской Федерации от 03.05.2014 № 120 «Об утверждении требований, обеспечивающих технологическую совместимость информационных систем организаций, подключаемых к инфраструктуре, обеспечивающих информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме с указанной инфраструктурой, к каналу связи и используемым для его защиты средствам криптографической информации, а также особенностей использования стандартов и протоколов при обмене данными в электронной форме между информационными системами указанных организаций и инфраструктурой» // Российская газета, № 229, 08.10.2014.

ме. В Федеральном законе № 210-ФЗ от 27.07.2010 статья 19 «Общие требования к использованию информационно-телекоммуникационных технологий при предоставлении государственных и муниципальных услуг» предусматривает утверждение Минкомсвязью России требований к технологической совместимости государственных информационных систем, стандартам и протоколам обмена данными в электронной форме. Вместе с тем аналогичное полномочие, только несколько в другой интерпретации – «утверждают стандарты предоставления данных в рамках межведомственного взаимодействия», – закрепляется Правительством Российской Федерации уже за органами государственной власти, обладающими такой информацией. Эти Правила обеспечения перехода федеральных органов исполнительной власти, государственных корпораций, наделенных соответствующими федеральными законами полномочиями по предоставлению государственных услуг, и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде при предоставлении государственных услуг утверждены Постановлением Правительства Российской Федерации от 28 декабря 2011 г. № 1184 «О мерах по обеспечению перехода федеральных органов исполнительной власти, государственных корпораций, наделенных соответствующими федеральными законами полномочиями по предоставлению государственных услуг, и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде». Выявленная правовая коллизия не позволяет своевременно принимать подзаконные правовые акты в развитие Федерального закона и осложняет его применение на практике. На данном этапе для комплексного решения этой проблемы в Государственной Думе РФ подготовлен законопроект об утверждении единых требований к создаваемым государственным информационным системам.

В соответствии с Постановлением Правительства Российской Федерации от 8 сентября 2010 г. № 697 (в ред. от 05.12.2014) «О единой системе межведомственного электронного взаимодействия» (вместе с Положением о Единой системе межведомственного электронного взаимодействия)⁷ утверждено Положение о Еди-

ной системе межведомственного электронного взаимодействия; в настоящее время функцию по обмену данными между государственными информационными системами выполняет Единая система электронного взаимодействия. Технические требования к взаимодействию утверждены Приказом Министерства связи и массовых коммуникаций Российской Федерации от 27.12.2010 № 190 «Об утверждении технических требований к взаимодействию информационных систем в Единой системе межведомственного электронного взаимодействия»⁸; документ утратил силу в связи с изданием Приказа Минкомсвязи России от 23.06.2015 № 210 «Об утверждении технических требований к взаимодействию информационных систем в Единой системе межведомственного электронного взаимодействия»⁹. Необходимо заметить, что поручение Правительства РФ органам государственной власти субъектов РФ создавать информационные системы по аналогии с федеральной системой межведомственного электронного взаимодействия носит рекомендательный характер, что де-юре позволяет создавать региональные информационные системы без учета федеральных рекомендаций.

В российской правовой литературе высказываются иные точки зрения, например, в монографии Терещенко Л.К. [1] электронная форма предоставления государственных и муниципальных услуг предполагает взаимодействие органов, предоставляющих государственные услуги, органов, предоставляющих муниципальные услуги, организаций, участвующих в предоставлении государственных и муниципальных услуг или организующих предоставление государственных и муниципальных услуг, что требует единых технических

(вместе с Положением о единой системе межведомственного электронного взаимодействия) // Собрание законодательства Российской Федерации, 20.09.2010, № 38, ст. 4823. Изменения, внесенные Постановлением Правительства РФ от 05.12.2014 № 1327, вступили в силу по истечении 7 дней после дня официального опубликования (опубликовано на Официальном интернет-портале правовой информации, URL: <http://www.pravo.gov.ru>, 10.12.2014).

⁸ Приказ Министерства связи и массовых коммуникаций Российской Федерации от 27.12.2010 № 190 «Об утверждении технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия» // Бюллетень нормативных актов федеральных органов исполнительной власти, № 9, 28.02.2011.

⁹ Приказ Министерства связи и массовых коммуникаций Российской Федерации от 23.06.2015 № 210 «Об утверждении технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия» // Официальный интернет-портал правовой информации, <http://www.pravo.gov.ru>, 27.08.2015.

⁷ Постановлением Правительства Российской Федерации от 8 сентября 2010 г. № 697 (в ред. от 05.12.2014) «О Единой системе межведомственного электронного взаимодействия»

решений и совместимости информационных систем, включая государственные и муниципальные информационные системы, составляющие информационно-технологическую и коммуникационную инфраструктуру.

Технические стандарты и требования, включая требования к технологической совместимости информационных систем, требования к стандартам и протоколам обмена данными в электронной форме при информационно-технологическом взаимодействии информационных систем, должны устанавливаться Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. В связи с этим представляется полезным анализ опыта стран Евросоюза. Изучение европейского опыта обеспечения межгосударственной и межведомственной совместимости оказания публичных услуг и ее условий было бы полезно как для Российской Федерации, так и для государств ЕвразЭС¹⁰.

Анализ действующего законодательства позволяет утверждать, что назревает необходимость четкого разграничения полномочий между Российской Федерацией и субъектами Российской Федерации в сфере информатизации. Необходимо унифицировать требования к созданию и эксплуатации государственных информационных систем. Кроме того, нельзя оставить без внимания и тот факт, что появилась необходимость сформировать единый понятийный аппарат терминов и определений в сфере информационно-коммуникационных технологий. Многие проблемы связаны именно с отсутствием такого аппарата. Следует иметь в виду, что все государственные программы содержат задачу объединения усилия, которые предпринимались различными ведомствами, министерствами, региональными властями, выработав некие единые правила, подходы, решения, стандарты.

В настоящее время объективно назрела необходимость систематизации и унификации законодательства в сфере разработки и использования федеральных информационных систем. Если в конце 2000-х гг. на уровне федеральных законов были закреплены положения, касающиеся лишь нескольких информационных систем, то в настоящее время их счет идет на десятки.

Нормы, устанавливающие правовой режим федеральных информационных систем, характеризуются отсутствием единой юридической техники и единого подхода к законодательному регулированию государственных информационных систем.

Начиная с 2010 года, в информационной сфере принят ряд документов в целях повышения эффективности планирования, создания и использования информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти, иных государственных органов и органов управления государственными внебюджетными фондами: в соответствии с Постановлением Правительства Российской Федерации от 24.05.2010 № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов» были утверждены Правила подготовки планов информатизации государственных органов и Правила проведения экспертной оценки документов, используемых в рамках планирования, создания и использования информационно-коммуникационных технологий в деятельности государственных органов. Постановлением Правительства Российской Федерации от 25.04.2012 № 394 были внесены изменения в Положение о координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов, Правила подготовки планов информатизации государственных органов и отчетов об их выполнении (в ред. Постановления Правительства РФ от 25.04.2012 № 394).

Постановлением Правительства Российской Федерации от 14.11.2015 № 1235 «О федеральной государственной информационной системе координации информатизации» было утверждено Положение о федеральной государственной информационной системе координации информатизации. Целью создания системы координации является повышение эффективности и результативности использования информационно-коммуникационных технологий в деятельности субъектов системы координации. Система координации обеспечивает формирование единого информационного пространства для поддержки принятия управленческих решений в сфере государственного управления информационно-коммуникационными технологиями, создаваемыми или используемыми федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации.

¹⁰ Терещенко Л.К. Модернизация информационных отношений и информационного законодательства: монография. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, «ИНФРА-М», 2013. С. 227.

Создание и развитие системы координации осуществляются на основе следующих принципов:

- исключение дублирования информации посредством соблюдения правил ее однократного ввода и многократного использования;
- использование результатов, полученных в ходе реализации государственной программы Российской Федерации «Информационное общество (2011–2020 годы)», утвержденной постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)»;
- преимущественное хранение в базах данных системы координации только уникальных (эталонных) сведений;
- открытость для интеграции с существующими и создаваемыми государственными и иными информационными ресурсами, ведомственными и межведомственными информационными системами на основе единых форматов информационного взаимодействия;
- обеспечение полноты, достоверности, актуальности и целостности информации, размещаемой в системе координации;
- безвозмездность предоставления информации, размещенной в системе координации, для всех заинтересованных лиц, имеющих право доступа.

За координацию внедрения информационных технологий в деятельность госорганов с 2010 года отвечает Министерство связи и массовых коммуникаций Российской Федерации, в обязанности которого входит проведение экспертизы ведомственных планов. Постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676 (ред. от 14.11.2015) «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»¹¹ были утверждены Требования к порядку этих процессов в целях повышения эффективности реализации полномочий органов ис-

полнительной власти в результате использования информационно-коммуникационных технологий.

Приказом Министерства связи и массовых коммуникаций Российской Федерации от 11.02.2016 № 44 «Об утверждении правил размещения информации в федеральной государственной информационной системе координации информатизации»¹² определены требования к размещению информации в федеральной информационной системе координации информатизации.

Эта система обеспечивает формирование единого информационного пространства для поддержки принятия управленческих решений в сфере государственного управления информационно-коммуникационными технологиями, создаваемыми или используемыми госорганами различного уровня – от федерального до муниципального.

Также определено, что размещение информации в системе координации осуществляется посредством заполнения полей экранных форм веб-интерфейса:

- федеральными органами исполнительной власти;
- высшими органами исполнительной власти субъектов РФ и исполнительными органами государственной власти субъектов РФ;
- иными государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями, государственными и муниципальными учреждениями;
- органами управления государственными внебюджетными фондами.

Отдельные сведения могут размещаться субъектами системы координации посредством информационного взаимодействия информационных систем субъектов системы координации с системой координации при обеспечении соблюдения установленных Правил.

Установлено, что субъекты системы координации для организации размещения информации в системе:

- определяют уполномоченных должностных лиц, ответственных за размещение информации;

¹¹ Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 (ред. от 14.11.2015) «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // Собрание законодательства Российской Федерации, 13.07.2015, № 28, ст. 4241.

¹² Приказ Министерства связи и массовых коммуникаций Российской Федерации от 11.02.2016 № 44 «Об утверждении правил размещения информации в федеральной государственной информационной системе координации информатизации» // Бюллетень нормативных актов федеральных органов исполнительной власти, № 27, 04.07.2016.

- обеспечивают получение указанными лицами квалифицированных сертификатов ключей проверки электронной подписи и средств электронной подписи;
- осуществляют регистрацию указанных лиц и присоединение их к профилю субъекта системы в «Единой системе идентификации и аутентификации»;
- направляют в Минкомсвязи России заявку для обеспечения доступа указанных лиц к системе координации;
- принимают ведомственные акты, содержащие мероприятия по подготовке субъекта системы координации к эксплуатации системы и порядок формирования и представления структурными подразделениями информации и документов, подлежащих размещению в системе координации.

Новый реестр должен стать гораздо масштабней, чем реестр государственных информационных систем Роскомнадзора, который с 1 декабря 2015 года вывели из эксплуатации в связи с созданием федеральной государственной информационной системы координации информатизации. В нем будут накапливаться сведения и документация по всем государственным информационным системам не только федеральных государственных органов, но и органов исполнительной власти субъектов РФ. Это создание нового, некоего «супер-реестра» государственной информатизации, аналогов которому по объему сведений и документов, предполагаемых к накоплению в реестре, еще не было [2].

Федеральная государственная информационная система координации информатизации (ФГИС КИ) была запущена в опытную эксплуатацию в сентябре 2016 года. Государственные органы в ней уже работают. Промышленная эксплуатация системы должна начаться к 2018 году.

Приказ Минкомсвязи устанавливает обширный список сведений, о которых государственные органы должны будут вносить сведения в реестр:

- информация о субъекте контроля;
- наименование государственной информационной системы;
- номер записи в реестре территориального размещения технических средств информационных систем;
- тип мероприятия по информатизации;
- номер мероприятия по информатизации;
- правовое основание мероприятия по информатизации;

- реквизиты заключения Минкомсвязи, предусмотренного положением о координации мероприятий по использованию ИКТ в деятельности госорганов;
- ТЗ на создание (развитие) государственной информационной системы;
- этап мероприятия по информатизации;
- перечень документации на государственную информационную систему;
- требования к приемке работ;
- проектная документация;
- рабочая документация;
- документация на ПО государственной информационной системы;
- пусконаладочные работы;
- предварительные испытания государственной информационной системы;
- опытная эксплуатация государственной информационной системы;
- приемочные испытания государственной информационной системы;
- решения по организационной структуре;
- подготовка должностных лиц субъекта контроля;
- срок эксплуатации государственной информационной системы;
- регламентные работы;
- правовые акты, связанные с выводом государственной информационной системы из эксплуатации;
- срок вывода государственной информационной системы из эксплуатации;
- срок хранения информации;
- основание для вывода государственной информационной системы из эксплуатации.

Выполнение государственных программ позволило обеспечить основу реализации программ в части внедрения информационных технологий в деятельность органов государственной власти и организации предоставления государственных услуг. Создан ряд государственных информационных систем, включая Единый портал государственных и муниципальных услуг (функций), портал государственных и муниципальных закупок, государственную автоматизированную систему «Управление», Интернет-узел для обеспечения бесперебойной работы Интернет-ресурсов Президента Российской Федерации и Правительства Российской Федерации, информационную систему поддержки деятельности многофункциональных центров предоставления государственных и муниципальных услуг для субъектов Российской Федерации, создана сеть удостове-

ряющих центров и сеть общественного доступа к государственным услугам; разработаны опытные образцы оборудования и программных средств для анализа реализации и прогнозирования выполнения работ по приоритетным национальным проектам, мониторинга и оценки эффективности управления бюджетными ресурсами, информационно-поисковых систем хранения и обработки мультимедийной информации [3].

Подводя итог, можно заключить, что назначение системы определяется через ее основные функциональные возможности. Функционал автоматизированной информационной системы можно рассматривать как детализацию ее цели; кроме

того, он может также выступать в качестве критерия корректности иных положений, закрепленных в законе (информационный ресурс системы, вопросы предоставления информации в систему и др.) [4].

Обязательность нормативного закрепления цели создания системы, как и других элементов ее правового режима, следует установить законодательно. Актуальность этой задачи нельзя недооценивать. Государственные автоматизированные информационные системы выступают в качестве вспомогательного средства регулирования общественных отношений и в этом качестве должны быть полно и органично вписаны в систему права.

*Рецензент: **Ниесов Владимир Александрович**, кандидат технических наук, профессор (МАОУ), профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.*

E-mail: vniesov@yandex.ru

Литература

1. Терещенко Л.К. Модернизация информационных отношений и информационного законодательства: монография. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, «ИНФРА-М», 2013. С. 227.
2. Попов Д.А. Государственная информатизация: анализ правоприменительной практики // Информационное право. 2014. № 3. С. 16–20.
3. Троян (Фадеева) Н.А. Информационные ресурсы Минюста России в сети Интернет // Мониторинг правоприменения. 2016. № 4. С. 64–68.
4. Амелин Р.В. Цель создания как элемент правового режима федеральной информационной системы // Журнал российского права. 2015. № 1.

ABSTRACTS, KEYWORDS AND REFERENCES

ON THE OKINAWA CHARTER ON GLOBAL INFORMATION SOCIETY AND THE GOALS OF DEVELOPMENT OF RUSSIAN COMMUNICATION SYSTEMS

Sergei Bochkov, Board Chairman of the Non-Profit Partnership "Non-Governmental Innovation Centre", Moscow, Russian Federation.

E-mail: vss-05@mail.ru

Grigorii Makarenko, Head of the Department for the Development of Scientific Periodicals of the Federal State-Funded Institution "Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation", Moscow, Russian Federation.

E-mail: monitorlaw@yandex.com

Andrei Fedichev, Ph.D. (Technology), Director of the Federal State-Funded Institution "Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation", Moscow, Russian Federation.

E-mail: fedichev@scli.ru

Keywords: *globalism of the Internet, information aggression, information technologies, security threats, information security threats, information cost, third nature of the Universe, hardware backdoors.*

Abstract. *Purpose of the paper: to improve teaching information technology law rapidly developing under the conditions of building the information society, in the system of higher education.*

Method used: multi-faceted theoretical and applied analysis of lines of modernisation of teaching 'information cycle' disciplines in higher education institutions.

Results obtained: a justification is given for three basic lines as well as conceptual and didactical aspects of modernisation of successive 'multi-level' (average Professional Specialist program — Bachelor program — Master program — Postgraduate program) teaching of pragmatically topical 'information cycle' disciplines, including those pertaining to information technology law as well as information and cybernetics, oriented at using innovative teaching technologies, their logical sequence and subject content, corresponding to the state of the art level of research and education.

A justification is given for a conceptual separation of authors' training courses and classes conducted in unorthodox (active and interactive) forms in education levels. Advantages and drawbacks of innovative teaching technologies and forms of students' research work based on the teaching experience at the Russian State University of Justice are identified.

References

1. Bochkov S.I. Informatsionnoe obshchestvo: poisk sotsial'nykh determinant formirovaniia massovogo, gruppovogo i individual'nogo soznaniia, URL: <http://np-nic.ru/publikatsii/filosofiya/5>.
2. Bochkov S.I., Fedichev A.V. O tsennosti informatsii na razlichnykh etapakh zhiznennogo tsikla, *Pravovaia informatika*, 2016, No. 3, pp. 35-40.
3. Klianchin A.I. Katalog zakladok ANB (SPIGEL). Chast' 1. Infrastruktura, *Voprosy kiberbezopasnosti*, 2014, No. 2(3), pp. 60-65.
4. Klianchin A.I. Katalog zakladok ANB (SPIGEL). Chast' 2. Rabochee mesto operatora, *Voprosy kiberbezopasnosti*, 2014, No. 4(7), pp. 60-68.
5. Makarenko D.G. Obshchestvennoe doverie kak resurs vlasti i upravleniia, *Biulleten' nauki i praktiki*, 2016, No. 8 (9), pp. 129-132.
6. Makarenko D.G. Printsip doveriia kak determinanta effektivnogo pravovogo regulirovaniia obshchestvennykh otnoshenii: pravovoe obespechenie, *Monitoring pravoprimeneniia*, 2017, No. 4 (25), pp. 15-22, DOI: 10.21681/2226-0692-2017-4-15-22.
7. Makarenko D.G. Sistema sotsial'no-pravovogo regulirovaniia kak obshchaia sreda vzaimodeistviia prava i doveriia, *Vestnik Vladimirovskogo iuridicheskogo instituta*, 2017, No. 2 (43), pp. 158-161.

8. Pocheptsov G.G. Kommunikatsii i gumanitarnye izmeneniia, Elektronnoe SMI "Media Sapiens", URL: http://www.osvita.mediasapiens.ua/trends/1411978127/kommunikatsii_i_gumanitarnye_izobreteniya/.
9. Leont'ev B.B., Makarenko G.I. Tret'ia priroda vselennoi, Pravovaia informatika, 2016, No. 4, pp. 4-9.
10. Pligin V.N., Makarenko G.I. Strana nuzhdaetsia v obnovlenii obshchestvennykh dogovorov v sovremennom rossiiskom obshchestve, Monitoring pravoprimeneniia, 2015, No. 1 (14), pp. 4-11.
11. Dmitrii Lovtsov, Dmitrii Makarenko, Andrei Fedichev, Architecture of the National Classification of Legal Regimes of Restricted Access Information, Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies (BIT 2017), Moscow, Russia, December 6-7, 2017, pp. 70-73.

AN EFFICIENT CONTROL ALGORITHM FOR PROCESSING JUDICIAL STATISTICAL INFORMATION

Roman Borisov, Ph.D. (Technology), Associate Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.

E-mail: bestseller@bk.ru

Keywords: judicial statistical information, control algorithm, efficiency, resource-intensive task, load sharing methods, load distribution planning system, concurrency control, non-structured data array.

Abstract.

Purpose of the paper: improving methods of preliminary processing of judicial statistical information.

Method used: development and experimental analysis of parallel control algorithms for efficient processing of judicial statistical information.

Results obtained: the importance of the problem of search for efficient methods of preliminary processing of judicial statistical information and the need to optimise the use of available computing resources are shown. A review of existing calculations planning methods is carried out. It is shown that universal methods of load distribution are low efficient for specific sets of tasks, which is related to individual possibilities for parallelising tasks and specific features of a particular computing system. An approach is proposed for organising a system planning load distribution between computing nodes in processing judicial statistical information using cloud technologies. It is shown that in order to create an efficient approach it is necessary to have information about the possibilities of solving each problem using a specific hardware and software set of the computer complex. For this purpose, a training algorithm is implemented in the planning system which collects information about the parameters of the computing task, the available resources, and the required parameters of the results of calculations. This information is formalised in the form of a processing models database and is refined in the process of solving application problems. The more problems are solved, the more extensive the models database and the greater the probability of obtaining a solution which is close to optimal. The minimum time for solving tasks using a dedicated set of resources was chosen as an optimisation criterion for the planning system. It is assumed that each task has a priority level and a solution deadline after which the results become irrelevant. It is shown that for processing judicial statistical information, one of the most popular resource-intensive computing tasks of this class is the task of search for specified messages in an unstructured data array. Planning means distributing the highest priority tasks between the available resources so that the number of tasks to be solved is maximised and the solution deadline values for the tasks should not be exceeded. The remaining tasks are distributed in accordance with the priorities for resources as they are being released. The approach remains operational as the configuration of computer system changes, when either some of its elements fail or individual nodes are connected to the computer system.

The mathematical foundations of the formation of models of plans for solving typical problems are given. The results of experimental studies are presented. A comparative evaluation of the proposed approach with the most popular dispatching and calculations managing algorithms is carried out.

References

1. Neural Network and Regression Based Processor Load Prediction for Efficient Scaling of Grid and Cloud Resources, M. T. Imam et al., 14th Intern. Conf. on Computer and Information Technology (ICCIT), IEEE, 2011, pp. 333-338.

2. Performance Evaluation and Optimization of an Adaptive Scheduling Approach for Dependent Grid Jobs with Unknown Execution Time, M. Ch tepen et al., 18th World IMACS / MODSIM'09 Congress. Cairns, Australia, 13-17 July 2009, pp. 1003-1009, URL: <http://www.mssanz.org.au/modsim09/C5/ch tepen.pdf> (data obrashcheniia: 12.02.2018).
3. Astrikov D. Iu., Kuz'min D. A. Issledovanie metodov otsenki effektivnosti vychislitel'nykh sistem na osnove funktsional'nykh modelei, Vestnik Sibirskogo gosudarstvennogo aerokosmicheskogo universiteta im. akademika M. F. Reshetneva, 2016. T. 17, No. 2, pp. 295-301.
4. Borisov R. S. Chernykh A. M. Dinamicheskaiia balansirovka nagruzki geterogennoi vychislitel'noi sistemy, Vestnik komp'iuternykh i informatsionnykh tekhnologii, 2017, No. 10, pp. 28-34.
5. Borisov R. S. Apparatno-orientirovannaia model' vzaimodeistviia otkrytykh sistem, Elektrotekhnicheskie i informatsionnye komplekсы i sistemy, 2011. T. 7, No. 1, pp. 21-25.
6. Vashchekin A. N., Vashchekina I. V. Informatsionnoe pravo: prikladnye zadachi i matematicheskie metody, Informatsionnoe pravo, 2017, No. 3, pp. 17-21.
7. Vashchekin A. N., Vashchekina I. V. Informatsionno-programmnoe obespechenie ratsional'nogo raspredeleniia sudebnykh del, Pravovaia informatika, 2017, No. 4, pp. 24-30.
8. Efimenko A. A. Integrirovannaia intellektual'naia tekhnologiiia optimizatsii parallel'nykh algoritmov v vysokoproizvoditel'nykh vychislitel'nykh sistemakh, Trudy Mezhdunar. nauch.-prakt. konf. "Sovremennye tendentsii v nauke, tekhnike, obrazovanii" (31 ianvaria 2016 g.). Smolensk: "Novalenso", 2016, pp. 59-61.
9. Korolev V. T., Lovtsov D. A., Radionov V. V. Sistemnyi analiz. Chast' 2. Logicheskie metody, pod red. D. A. Lovtsova. M.: RGUP, 2017. 160 s.
10. Lovtsov D. A., Bogdanova M. V., Parshintseva L. S. Pakety prikladnykh programm dlia mnogoaspektnogo analiza sudebnoi statisticheskoi informatsii, Pravovaia informatika, 2017, No. 1, pp. 28-36.
11. Lovtsov D. A., Bogdanova M. V., Parshintseva L. S. Pravovaia statistika prestupnosti v sovremennykh usloviakh, Pravovaia informatika, 2017, No. 4, pp. 40-48.
12. Lovtsov D. A., Niesov V. A. Aktual'nye problemy sozdaniia i razvitiia edinogo informatsionnogo prostranstva sudebnoi sistemy Rossii, Informatsionnoe pravo, 2013, No. 5, pp. 13-18.
13. Lovtsov D. A., Chernykh A. M. Modernizatsiia sistemy sudebnoi statistiki na osnove novoi geoinformatsionnoi tekhnologii, Pravovaia informatika, 2016, No. 1, pp. 7-14.
14. Chubukova S. G. Strategii razvitiia informatsionnogo obshchestva i napravleniia razvitiia zakonodatel'stva, Pravovaia informatika, 2017, No. 2, pp. 67-72.

INFORMATION EXCHANGE IN THE LAWYER'S PROFESSIONAL ACTIVITIES: INVESTIGATION OF SPECIFIC FEATURES OF COMMUNICATIVE ACTIVITY

Andrei Vashchekin, Ph.D. in Economics, Associate Professor, Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Russian Federation, Moscow.

E-mail: vaschekin@mail.ru

Dar'ia Shevchenko, Lawyer, OOO Neftemashservis-S company, Moscow, Russian Federation.

E-mail: dasha121sheva@mail.ru

Keywords: lawyer, respondent, communicative activity, information interaction, observation, survey, expert assessments, indicator, parameter, information model, diagram.

Abstract.

Purpose of the work: studying the communicative qualities a lawyer should have, including the ability to establish and maintain contact with the respondent, the skill to overcome psychological barriers in the communication process, the ability to adequately assess the person's personality and the lawyer's own behaviour, to react to emerging circumstances in the process of information exchange, to have the skills of verbal and non-verbal communication means.

Methods used: observation, sociological survey, and expert assessments smoothed by computations conducted on the basis of analysis of hierarchies.

Results obtained: a justification is given for introducing the concept of communicative activity (professional communication) of a lawyer in the broad sense of the word, which is understood as the process of establishing and developing interaction between a lawyer and any respondent, the content of the interaction being: exchange of information, achievement of mutual understanding, exerting a motive-generating influence on the respondent with a view to engage the latter in a joint activity.

The study showed that global informatisation and widespread introduction of information and computer tools, resources, and technologies bringing about changes in social and production relations do not reduce the importance of traditional forms of information exchange, and first of all speech communicative activity, for the practical lawyer. Therefore, goal-oriented raising of the general level of information training for practical lawyers should also be supplemented with a comprehensive mastering of the rules of information interaction.

References

1. Bykanova O.A., Akhmadeev R.G. Diversifikatsiia portfel'nykh investitsii suverennykh fondov, Azimut nauchnykh issledovani: ekonomika i upravlenie, 2016, t. 5, No. 4 (17), pp. 59-63.
2. Vashchekin A.N., Vashchekina I.V. Informatsionnoe pravo: prikladnye zadachi i matematicheskie metody, Informatsionnoe pravo, 2017, No. 3, pp. 17-21.
3. Vashchekina I.V., Vashchekin A.N. Informatsionnyi obmen mezhd urovniami ierarkhii v bankovskikh, promyshlennykh i torgovykh sistemakh, Nauchnoe obozrenie. Ekonomicheskie nauki, 2017, No. 3, pp. 51-59.
4. Vashchekina I.V. Perspektivy reformirovaniia organizatsionnoi struktury platezhnoi sistemy v Rossii, Nauka i praktika, No. 4 (16), 2014, pp. 5-14.
5. Ershov V.V., Lovtsov D.A. Kontseptsii nepreryvnoi informatsionnoi podgotovki iurista, Informatsionnoe pravo, 2007, No. 3, pp. 29-34.
6. Kosov M.E. Ideologicheskii podkhod v issledovanii nelegal'noi ekonomiki, Vestnik Moskovskogo universiteta MVD Rossii, 2011, No. 7, p. 40.
7. Lovtsov D. A. Sovremennaia kontseptsii nepreryvnoi informatsionnoi podgotovki iurista, Rossiiskoe pravosudie, 2013, No. 5, pp. 57-66.
8. Lovtsov D. A. Modernizatsiia informatsionno-pravovogo obrazovaniia v usloviakh formirovaniia informatsionnogo obshchestva, Pravovaia informatika, 2017, No. 4, pp. 4-13.
9. Pichkurenko E.A. Testovye zadaniia "Intellektual'naia labil'nost'", Ekonomika. Pravo. Pechat'. Vestnik KSEI, 2011, No. 4-6 (50-52), pp. 214-218.
10. Polevaia M.V. Obobshchennyi podkhod k otsenke effektivnosti personala na osnove nechetkikh otnoshenii, Transportnoe delo Rossii, 2015, No. 4, pp. 107-109.
11. Slavianov A.S. Podderzhka priniatiia upravlencheskikh reshenii v period provedeniia innovatsionnoi modernizatsii proizvodstva na osnove modeli zhiznennogo tsikla predpriatiia, Kontrolling, 2017, No. 1 (63), pp. 26-31.
12. Tontoeva T.V. K voprosu o kommunikativnoi deiatel'nosti iurista, Sovremennye nauchnye issledovaniia i innovatsii, 2016, No. 3 [Elektronnyi resurs], URL: <http://web.snauka.ru/issues/2016/03/65327>.
13. Akhmadeev R.G., Kosov M.E., Bykanova O.A., Korotkova E.V., Mamrukova, O.V. Assessment of the tax base of the consolidated group of taxpayers in Russia using the method of polynomial interpolation, Indian Journal of Science and Technology, 2016, No. 9 (12), p. 89533.
14. Vashchekin A.N., Khrustalev M.M. Studying stability of the econometric model of non-antagonistic game of the wholesale market subjects, Automation and Remote Control, 2005, T. 66, No. 10, pp. 1677-1689.

INFORMATION TECHNOLOGIES IN THE STATISTICAL ANALYSIS OF MARKETING RESEARCH

Dmitrii Lovtsov, Doctor of Science (Technology), Professor, Honoured Scholar of the Russian Federation, Deputy Director for Research of Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences, Head of the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.

E-mail: dal-1206@mail.ru

Marina Bogdanova, Doctor of Science (Economics), Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.

E-mail: bogdanovamv2009@yandex.ru

Lidiia Parshintseva, Ph.D. (Economics), Associate Professor at the Department of Statistics of the State University of Management, Moscow, Russian Federation.

E-mail: lsfantelina@yandex.ru

Keywords: information technologies, applied software packages, marketing, marketing research, key macroeconomic indicators, laws, statistical methods, marketing research market volume, main stages of the study, methodological diagram.

Abstract.

Purpose of the work: increasing the efficiency of multi-aspect statistical analysis of the state of marketing research based on the use of modern information and software tools.

Methods used: comparative analysis of the dynamics of marketing research market volume, comparative technical and economic analysis of existing statistical methods and information and software tools.

Results obtained: based on the application of the R software environment and MS Excel table processor, an assessment of the volume and dynamics of marketing research in Russia over the last ten years as one of the most interesting and popular marketing tools is carried out, a comparative analysis of marketing research market volume dynamics is performed, in comparable prices with the dynamics of the main macroeconomic indicators, and the role of statistical methods and information and software tools in conducting marketing research is shown and their brief description is given. A justification for the methodological diagram of productive marketing research is provided.

Recommendations on using information technologies for solving applied analytical problems and on selecting appropriate statistical software tools as well as the results of experimental analysis are given.

References

1. Alekseeva A. Iu., Echevskaia O. G., Kovaleva P. S. Analiz sotsiologicheskikh dannykh s primeneniem paketa SPSS, Novosibirsk: RITs NGU, 2003, 112 pp.
2. Berestneva O.G., Marukhina O.V., Shevelev G.E. Prikladnaia matematicheskaia statistika, Tomsk: Izd-vo Tomskogo politekh. un-ta, 2012, 188 pp.
3. Berns E. S., Bush R. F. Osnovy marketingovykh issledovaniy s ispol'zovaniem MS Excel, M.: Vil'iams, 2005, 704 pp.
4. Bogdanova M. V., Parshintseva L. S. Sovremennye sredstva elektronnoi obrabotki sotsial'no-ekonomicheskoi informatsii, Vestnik universiteta, 2017, No. 5, pp. 10-15.
5. Lovtsov D. A. Imitatsionno-igrovoe modelirovanie funktsionirovaniia i razvitiia sovokupnosti krupnomasshtabnykh ergasistem, Trudy XVI Mezhdunar. nauch.-metod. konf. "Informatika: problemy, metodologiya, tekhnologii" (11-12 fevralia 2016 g.), VGU, Voronezh: izd-vo "Nauch.-issled. publikatsii", 2016, pp. 78-86.
6. Lovtsov D. A., Bogdanova M. V. Problema upravleniia investitsiyami oboronnykh proektov Rossii, Obozrevatel'-Observer, 2000, No. 8, pp. 53-57.
7. Lovtsov D. A., Bogdanova M. V., Parshintseva L. S. Osnovy statistiki, pod red. D. A. Lovtsova, M.: RGUP, 2017, 160 pp.
8. Lovtsov D. A., Bogdanova M. V. Informatsionno-statisticheskie pokazateli kachestva proektnykh investitsii, NTI RAN. Ser. 2. Inform. protsessy i sistemy, 2000, No. 12, pp. 28-36.
9. Lovtsov D. A., Bogdanova M. V. Ekonomiko-pravovoe regulirovanie oborota rezul'tatov intellektual'noi deiatel'nosti predpriatii promyshlennosti Rossii, Ekonomika, statistika i informatika. Vestnik UMO, 2013, No. 1, pp. 53-56.
10. Lovtsov D. A., Bogdanova M. V., Parshintseva L. S. Pakety prikladnykh programm dlia mnogoaspektnogo analiza sudebnoi statisticheskoi informatsii, Pravovaia informatika, 2017, No.1, pp. 28-36.
11. Lovtsov D. A., Bogdanova M. V., Parshintseva L. S. Pravovaia statistika prestupnosti v sovremennykh usloviakh, Pravovaia informatika, 2017, No. 4, pp. 40-48.
12. Lovtsov D. A., Chernykh A. M. Modernizatsiya sistemy sudebnoi statistiki na osnove novoi geoinformatsionnoi tekhnologii, Pravovaia informatika, 2016, No. 1, pp. 7-14.
13. Ob»edinenie issledovatelei rynka i obshchestvennogo mneniia OIROM [Elektronnyi resurs]. Rezhim dostupa: <http://oirom.ru/> (data obrashcheniia: 20.03.2018 g.)
14. RAMU -- Rossiiskaia assotsiatsiya marketingovykh uslug [Elektronnyi resurs]. Rezhim dostupa: <https://www.ramu.ru/> (data obrashcheniia: 20.03.2018 g.)
15. Federal'naia sluzhba gosudarstvennoi statistiki Rosstat [Elektronnyi resurs]. Rezhim dostupa: www.gks.ru (data obrashcheniia: 21.03.2018).

INFORMATION RELIABILITY OF FUNCTIONING OF THE TELEMATIC NETWORK OF THE STATE AUTOMATED SYSTEM OF THE RUSSIAN FEDERATION “PRAVOSUDIIE” [“JUSTICE”]

Dmitrii Lovtsov, Doctor of Science (Technology), Professor, Honoured Scholar of the Russian Federation, Deputy Director for Research of Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences, Head of the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.

E-mail: dal-1206@mail.ru

Keywords: information reliability, telematic network, State Automated System of the Russian Federation “Pravosudie” [“Justice”], privileged information, government standard (GOST), Domain Name System (DNS), Border Gateway Protocol (BGP), international technical legal standards (RFC, “Requests for Comments”), Public Key Infrastructure (PKI), cryptographic algorithms, covert information channel (CIC).

Abstract.

Purpose of the work: formation of a productive theoretical and legal basis for the creation and development of a telematic network of the State Automated System (SAS) of the Russian Federation (RF) “Pravosudie” [“Justice”] with an increased information reliability.

Method used: comprehensive theoretical and applied analysis and development of information and mathematical support of the information reliability of functioning of the telematic network of the SAS of the RF “Pravosudie” [“Justice”].

Results obtained: a mathematical formulation of the problem of situational control of the protected exchange of privileged information in the conditions of impact of significant random and deliberate destabilising factors in a telematic network with an arbitrary topological structure is justified and decomposed, a method for solving this complex problem is proposed, and organisational-cum-legal and technological measures are determined within the framework of international legal standardisation of the main network-forming protocols of the Internet global network as an efficient way to solve the problem of ensuring information reliability of the telematic network of the SAS of the RF “Pravosudie” [“Justice”].

A number of measures to be carried out at the government level in order to ensure the required level of information reliability of operation for the telematic network of the SAS of the RF “Pravosudie” [“Justice”] and its users are proposed.

References

1. Kabelev D. B. O reshenii zadachi rasprostraneniia i khraneniia otkrytykh kliuchei v ASBR Moskovskogo regiona, Obozrenie prikladnoi i promyshlennoi matematiki (v Rossiiskoi Federatsii), 2002, t. 9, vyp. 1, pp. 18-25.
2. Lovtsov D. A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem, Pravovaia informatika, 2017, No. 3, pp. 66-74.
3. Lovtsov D. A. Informatsionnye pokazateli effektivnosti funktsionirovaniia ASU slozhnymi dinamicheskimi ob»ektami, Avtomatika i Telemekhanika, 1994, No. 12, pp. 143-150.
4. Lovtsov D. A. Modeli izmereniia informatsionnogo resursa ASU, Avtomatika i Telemekhanika, 1996, No. 9, pp. 3-17.
5. Lovtsov D. A., Ermakov I. V. Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme, NTI RAN. Ser. 2. Inform. protsessy i sistemy, 2005, No. 2, pp. 1-7.
6. Lovtsov D. A. Informatsionnye otsenki tekhnologicheskoi effektivnosti pererabotki informatsii, NTI RAN. Ser. 2. Inform. protsessy i sistemy, 1997, No. 11, pp. 22-26.
7. Lovtsov D. A. Obespechenie informatsionnoi bezopasnosti v rossiiskikh telematicheskikh setiakh, Informatsionnoe pravo, 2012, No. 4, pp. 3-7.

8. Lovtsov D. A. Informatsionnaia teoriia ergasistem: Tezaurus, M.: Nauka, 2005, 248 pp.
9. Lovtsov D. A., Kabelev D. B. Situatsionnoe upravlenie zashchishchennym obmenom privilegirovannoi informatsiei v ASU spetsial'nogo naznacheniiia, Trudy XXKh Vseross. nauch.-tekhn. konf. "Problemy effektivnosti i bezopasnosti funktsionirovaniia slozhnykh tekhnicheskikh i informatsionnykh sistem" (30 iyunia -- 1 iuliia 2011 g.) v 5-i t. T. 4, RAN, RAO. Serpukhov: Serp. voen. in-t, 2011, pp. 166-169.
10. Lovtsov D. A., Kabelev D. B. Tekhnologiia i problemy ratsional'nogo upravleniia kliuchевой informatsiei v ASU spetsial'nogo naznacheniiia, Trudy XXIKh Vseross. nauch.-tekhn. konf. "Problemy effektivnosti i bezopasnosti funktsionirovaniia slozhnykh tekhnicheskikh i informatsionnykh sistem" (24-25 iyunia 2010 g.) v 5-i t. T. 4, RAN, RAO. Serpukhov: Serp. voen. in-t, 2010, pp. 144-148.
11. Shileiko A. V., Kochnev V. F., Khimushin F. F. Vvedenie v informatsionnuiu teoriiu sistem. M.: Radio i sviaz', 1985.

QUALITY OF A STANDARDISED SYSTEM OF DATA ENCRYPTION ALGORITHMS IN THE STATE AUTOMATED SYSTEM OF THE RUSSIAN FEDERATION "PRAVOSUDIE" ["JUSTICE"]

Vladimir Korolev, Ph.D. (Technology), Professor, Honoured Worker of Higher Professional Education of the Russian Federation, Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.

E-mail: timofeyich@mail.ru

Dmitrii Lovtsov, Doctor of Science (Technology), Professor, Honoured Scholar of the Russian Federation, Deputy Director for Research of Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences, Head of the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.

E-mail: dal-1206@mail.ru

Keywords: main step of cryptoconversion, simple replacement, gambling, imitation insertion, privileged information, State Automated System of the Russian Federation "Pravosudie" ["Justice"], government standard (GOST), covert information channel (CIC), quality.

Abstract.

Purpose of the work: improving the scientific and methodological base of the theory of legal regimes of restricted access to information resources.

Method used: comprehensive theoretical and comparative analysis of cryptographic means of ensuring protection of privileged information from disclosure.

Results obtained: numerical parameters and mathematical operations of standardised procedures for data cryptographic conversion are determined which, on the whole, allows to assess the current state of the problem of ensuring protection of privileged information in the State Automated System (SAS) of the Russian Federation (RF) "Pravosudie" ["Justice"]. A theoretical comparative estimate of the quality of algorithms of encryption in accordance with GOST 28147-89 and DES-75 is given. In order to ensure the required level of protection of privileged information in the SAS of the RF "Pravosudie" ["Justice"] and considering ample opportunities for unauthorised access using covert information channels, it is proposed to use the GOST 28147-89 encryption algorithms both in the internal (closed) and external (public) contour of information interaction.

References

1. Barichev S. G., Goncharov V. V., Serov C. E. Osnovy sovremennoi kriptografii, M.: Goriachaia liniia-Telekom, 2011, 175 pp.
2. Lovtsov D. A. Problema informatsionnoi bezopasnosti GAS RF "Pravosudie", Rossiiskoe pravosudie, 2012, No. 5, pp. 103-109.

3. Lovtsov D. A. Kontrol' i zashchita informatsii v ASU, M.: VA im. Petra Velikogo, 1991, 172 pp.
4. Lovtsov D. A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem, Pravovaia informatika, 2017, No. 3, pp. 66-74.
5. Lovtsov D. A. Informatsionnaia nadezhnost' funktsionirovaniia telematicheskoi seti GAS RF "Pravosudie", Pravovaia informatika, 2018, No. 1.
6. Maliuk A. A., Pazizin S. V., Pogozhin N. S. Vvedenie v zashchitu informatsii v avtomatizirovannykh sistemakh, M.: Goriachaia liniia-Telekom, 2011, 146 pp.
7. Riabko B. Ia., Fionov A. N. Osnovy sovremennoi kriptografii i steganografii, M.: Goriachaia liniia-Telekom, 2011, 232 pp.
8. Khoffman L. Dzh. Sovremennye metody zashchity informatsii, M.: Sov. radio, 1980, 246 pp.
9. Shennon K. Teoriia svyazi v sekretnykh sistemakh, Raboty po teorii informatsii i kibernetiki, M.: Inostrannaia literatura, 1963, pp. 333-402.

A STATE SYSTEM OF INFORMATISATION COORDINATION AS A MECHANISM FOR CREATING A SINGLE INFORMATION SPACE

Natal'ia Troian (Fadeeva), Senior Researcher at the Federal State-Funded Institution "Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation", Moscow, Russian Federation.

E-mail: n-fadeeva@yandex.ru

Keywords: information systems, information society, legal information, databases, state electronic registers, normative legal act, electronic interinstitutional interaction.

Abstract.

Issues of using modern information and telecommunication technologies for improving access to the information resources of the Ministry of Justice of the Russian Federation are considered in the paper. Such a topical question of information technology laws as the absence of a single conceptual framework of terms and definitions in the sphere of information and communication technology is discussed. Important questions of unification of requirements to the creation and operation of government information systems are touched upon. The problem of unity of legal standards which set the legal regime of federal information systems is considered. Modern federal laws on information systems is analysed, a comparison of approaches to laying down the goals of their creation in the law is carried out.

References

11. Tereshchenko L.K. Modernizatsiia informatsionnykh otnoshenii i informatsionnogo zakonodatel'stva: monografiia, M.: Institut zakonodatel'stva i sravnitel'nogo pravovedeniia pri Pravitel'stve RF, "INFRA-M", 2013, p. 227.
2. Popov D.A. Gosudarstvennaia informatizatsiia: analiz pravoprimeritel'noi praktiki, Informatsionnoe pravo, 2014, No. 3, pp. 16-20.
3. Troian (Fadeeva) N.A. Informatsionnye resursy Miniusta Rossii v seti Internet, Monitoring pravoprimereniia, 2016, No. 4, pp. 64-68.
4. Amelin R.V. Tsel' sozdaniia kak element pravovogo rezhima federal'noi informatsionnoi sistemy, Zhurnal rossiiskogo prava, 2015, No. 1.
5. Makarenko G.I., Mikhalevich V.V. Distanttsionnoe okazanie iuridicheskikh uslug naseleniiu cherez sozdanie Vserossiiskogo biuro spravedlivosti, Monitoring pravoprimereniia, 2012, No. 4, pp. 6-11.

Над номером работали:

Начальник РИО	Ю.В. Матвиенко
Шеф-редактор	Г.И. Макаренко
Ответственный секретарь	О.В. Танимов
Редактор-переводчик	Т.В. Галатонов
Дизайн обложки	И.Г. Колмыкова
Верстка	Н.Г. Шабанова