Правовая информатика

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
№ 1, 2021 г.
Выходит 4 раза в год

Зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций
Свидетельство № 015372 от 01.11.1996 г.

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

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 05.03.2021 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://uzulo.su/prav-inf

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс: 34077

LEGAL INFORMATICS

RESEARCH AND PRACTICE JOURNAL
2021, No. 1
The journal is published quarterly.

Registered by the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications
Registration Certificate No. 015372
of the 1st 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

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 5th of March, 2021.
Number of items printed: 100. Free price.

Postal address:
Mikhalkovskaya str., bld. 65/1,
125 438, Moscow, Russia
Telephone: +7 (495) 539-25-29
E-mail: inform360@yandex.com
Guidelines for preparing manuscripts for publication can be found on the website
http://uzulo.su/prav-inf

CONTENTS

The journal can be subscribed to at post offices through the Press of Russia (Pressa Rossii) Catalogue. Publication index: 34077

ПРАВОВАЯ ИНФОРМАТИКА И УПРАВЛЕНИЕ ОТРАСЛЯМИ ЭКОНОМИКИ

Запольский С.В.*

***Ключевые слова**: законотворчество, законы, исполнительная власть, правительство, органы отраслевого управления, контроль, надзор, мониторинг, аудит, правоохранительные органы, статистика, предприятия, корпорации.*

Аннотация.

Цель работы: совершенствование научно-методической базы теории правового регулирования экономических отношений в информационном обществе.

Метод: системный исторический анализ информационных отношений, складывающихся в сфере экономического управления, как предмета информационно-правового регулирования и средства оптимальной организации самого процесса государственного и корпоративного управления экономическим развитием.

Результаты: обосновано разделение информационных отношений в рассматриваемой сфере на прямые и обратные: прямыми являются отношения по нормотворчеству и доведению актов управления до их адресатов, обратными — по сбору и обработке информации о соблюдении законности и хозяйственных результатов; одним из недостатков порядка подготовки законов, по мнению автора, является превалирование мнения исполнительной власти над волеизъявлением представительных органов и позицией экспертно-аналитического сообщества, политических и общественных организаций, а также изъяны в законотворческой технике; контроль, надзор, мониторинг и аудит рассматриваются как объединенные одной целью применения, но юридически различные способы сбора, обработки и реализации экономико-правовой информации, касающейся народного хозяйства; следует более эффективно использовать особенности этих форм движения обратной информации, механизм которого целесообразно строить на данных государственной статистики, на других информационных источниках, включая средства массовой информации и др.; высказывается мнение о нецелесообразности сведения всех обратных связей только к контролю; сделан вывод о том, что правовая информатика должна войти в круг инструментов государственного управления экономикой как неотъемлемая часть этого механизма.

DOI: 10.21681/1994-1404-2021-1-04-12

Правовая информатика — весьма широкое понятие, означающее, помимо прочего, *механизм оборота информации*, необходимой для функционирования органов власти и управления, деятельности организаций производственного и непроизводственного секторов экономики, выполнения контрольными, правоохранительными и юрисдикционными органами возложенных на них функций.

Правовая информатика в этом смысле отличается от правовой информации тем, что носит императивный характер, обязательность принятия и исполнения, приобретает законом определенные формы, обладает способностью отражать юридическое значение действий ее адресатов. Отношения, складывающиеся в сфере *правовой информатики* [6], по их управленческой природе можно подразделить на *прямые*, т. е. исходящие от органов государственного управления общей и специальной компетенции — законы, акты Президента, Кабинета министров, министерств и ведомств, и *обратные* — разнообразную отчетность, акты контроля и надзора, информацию, собираемую другими органами управления, включая средства массовой информации, и др.

В этих информационных потоках главную роль играет предприятие, корпорация, бюджетное учреждение и другие участники экономического оборота — *юридические лица*. Заметим, что в ходе изменений экономической политики деление на производственные и бюджетные (непроизводственные) организации постепенно утрачивает свое значение; и те и другие обладают всей полнотой информационной и управленческой правосубъектности, а не дифференцируются в сфере правоприменения и на унифицированных началах входят в состав (систему) отраслей экономики [10]. Правовая информатика создает общий юридический режим существования и развития отраслей, всех входящих в них организаций.

* ***Запольский Сергей Васильевич, д****октор юридических наук, профессор, заслуженный юрист Российской Федерации, главный научный сотрудник Института государства и права Российской академии наук, г. Москва, Российская Федерация.*
E-mail: zpmoscow@mail.ru

Отрасль экономики — основное структурное образование народного хозяйства, сложившееся в ходе индустриального развития СССР и пришедшее в существенно трансформированном виде в экономику России. Основные изменения, произошедшие с отраслями экономики в связи с переходом на принципы постсоветского хозяйствования, сводятся к отказу от *административного* распорядительства, свойственного плановой экономике СССР, и к широкому использованию экономического регулирования хозяйственной самостоятельности предприятий и производственных структур. Это вызвало существенную перестройку системы органов управления экономикой, в том числе отказу от принадлежности предприятий к тому или иному министерству с «подключением» к министерскому планированию, материально-техническому снабжению, финансированию, управлению трудовыми ресурсами и другим институтам планового управления. В настоящее время, за малым исключением, предприятия, близкие по характеру производства, объединяются либо в так называемые горизонтальные комплексы, либо в вертикально интегрированные структуры [9].

Информационные отношения, складывающиеся в ходе управления отраслями в настоящее время, не могут не отличаться от информационных потоков, присутствующих в отраслях при наличии министерства (центра отрасли), администрирующего вверенную ему совокупность предприятий. Эти изменения продиктованы новой ролью органа отраслевого управления — государственной корпорации, холдинга, компании с превалирующим государственным участием, включающей в себя ряд предприятий. Поскольку в новых организационных структурах все информационные потоки естественным образом делятся на *прямые*, исходящие от органа управления, и *обратные*, связывающие хозяйственный субъект с органом управления, обратимся вначале к изменениям, произошедшим в прямых информационных отношениях [5].

Для предприятия в прошлом наиболее характерной чертой было подчинение (подведомственность) органу отраслевого управления. Соответственно, прямым управленческим отношениям прежде всего была присуща *директивность* полученной информации. Министерство имело право и несло обязанность административно регулировать деятельность предприятия, иного хозяйственного органа. Это предполагало, *во-первых*, требование исполнения актов высших органов власти, которые, как правило, доводились до мест приказом по отрасли. *Во-вторых*, решения самого органа управления отрасли несли, как правило, императивную нагрузку и возлагали на предприятия не только плановые задания, но и управленческие обязанности, обеспечиваемые различными мерами юридической ответственности. Третий вид информационного администрирования — легитимизация действий и решений администрации предприятия — дача разрешений на принятие мер, которые, по существу, входят в полномочия должностных лиц предприятия.

Отметим, что сложившийся тогда стиль управления обеспечивал своеобразную *«информационную колыбель»* — возможность получения предприятием подавляющей части управленческой информации без критической доработки, оценки эффективности. Если к этому присовокупить бланкетность практически всех хозяйственных договоров, заключаемых предприятиями с контрагентами, применение вышестоящими органами принципа «не можешь — научим, не хочешь — заставим», то обосновать вывод об *информационном «иждивенчестве»* хозорганов в плановой экономике не будет казаться жестким. Конечно, речь шла о правовой информатике и не касалась технической и экономической политики, хотя и здесь элементы косности были заметны. Можно предположить, что информационное поле, сложившееся после принятия в 1979 г. постановления Правительства № 695[1] во взаимоотношениях органов отраслевого управления и предприятий, объединений, других субъектов хозяйствования, в конечном счете, развалило к середине восьмидесятых годов советскую экономику.

Впору, отчасти вернувшись, задаться вопросом — что понимается под термином *"управленческая информация"?* На взгляд автора, этим понятием охватывается регулятивный потенциал, заложенный в той или иной структуре управления социальными или экономическими процессами, материализуемый в конкретных планах, программах, административных или финансово-распорядительных актах органа, уполномоченного на руководство хозяйственной системой. В той мере, в какой информация служит управлению, она сама воплощает в себе управленческое воздействие, оформляемое теми или иными техническими средствами, включающими в свой круг и цифровые технологии, внедряемые ныне.

Отсюда следует, думается, важный вывод о том, что никакого иного прямого управленческого воздействия, кроме как *информационно-правового*, не существует, а, следовательно, совершенствование управления тождественно совершенствованию правовой информатики. В этом смысле изменения, произошедшие в сфере правовой информатики, коренным образом преобразовали управление отраслями народного хозяйства. Упразднение отраслевых министерств (за исключением Минпромторга), ориентация на вертикально-интегрированные хозяйственные структуры, появление ряда государственных корпораций и главное — придание первичному звену народного хозяйства правового статуса, зависящего от формы собственности на средства производства, придали управленческой информации новый облик, свободный от этатического воздействия, но задающий вместо директивных указаний условия и правила хозяйственной деятельности.

[1] Постановление ЦК КПСС и Совета Министров СССР «Об улучшении планирования и усилении воздействия хозяйственного механизма на повышение эффективности производства и качества работы» от 12 июля 1979 г. № 659 // СП СССР. 1979. № 18. Ст.118.

Правовой режим налогообложения, ценообразования, таможенного регулирования, кредитования, капиталовложений, управления трудовыми ресурсами и другие стороны хозяйствования получили *информационное обеспечение*, основанное на законе, причем законе, распространяющемся на все отрасли и регионы страны, исключающем привилегии и приоритеты отдельных секторов экономики, кроме тех, которые предоставляются в интересах всего народного хозяйства; обеспечивается соответствие актов исполнительных органов федеральным и региональным законам; права первичного звена народного хозяйства защищены судом, прокурорским надзором и контролем. Иначе говоря, создана достаточно совершенная система правовой информатики, способная конкурировать с аналитическими системами развитых мировых экономик [2].

Однако никакая, самая совершенная информационная система не в состоянии решать свои задачи без качественного информационного контента. К сожалению, приходится признать постоянное снижение юридического качества управленческих решений и, прежде всего, качества федерального законодательства. Энергичный и конструктивный подход к подготовке законов, характерный для начала постсоветского периода, не был поддержан и развит впоследствии. Федеральный законодатель сбился на мелкотемные попытки вдохнуть жизнь в неработающие экономико-правовые конструкции вместо обращения внимания на негативные тенденции в развитии народного хозяйства, на решение частных вопросов.

Неэффективность государственного управления экономикой — слишком объемная тема для отдельной частной статьи. Глядя на проблему с технологической стороны, можно предположить, что качество правовой информатики предопределено во многом характером выбора предметов, разрабатываемых законопроектов и недостатками в их подготовке.

Одной из важнейших причин неэффективности служит то, что подавляющая часть законопроектов готовится исполнительными органами власти и представляется в Государственную Думу правительством; в иных случаях Кабинет Министров представляет заключение по законопроекту, во многом определяющее судьбу инициативы. Дело даже не в том, что этой практикой отсеивается участие многих заинтересованных в законотворчестве организаций и движений. Более значимо отступление от *принципа разделения* государственной власти на законодательную, исполнительную и судебную, закрепленного в статье 10 Конституции РФ. Приоритет исполнительной власти, сложившийся с тех далеких времен, когда депутаты дореволюционных Дум требовали «ответственного министерства» (на нашем языке правительства), продолжает влиять на законодательство, остающееся более продуктом исполнительной власти, нежели законодательной. Речь, конечно, идет не о том или ином конкретном законе, но о законодательной политике в целом. Вряд ли можно считать оптимальным то, что по инициативе Президента РФ и Правительства РФ принимается из года в год не менее 58% всех принятых Государственной Думой законов [13].

Вне сомнения, именно правительство обладает главным массивом информации о состоянии экономики, о социальных и политических процессах, текущих в российском обществе. Казалось бы, кому, как не Правительству, осуществлять основные меры по управлению социальной и экономической жизнью страны? Однако конституционные положения по разделению властей (ст. 10 Конституции РФ) требуют акцента на слове *осуществляют*, но не планируют и не программируют государственное управление. Это уже прошедший этап, когда Совнарком СССР и Совмин СССР были сосредоточением всей власти при декоративном Верховном Совете СССР. Текущий этап политической истории требует несравненно большего участия Федерального Собрания РФ и в первую очередь Государственной Думы в формировании программы законопроектных и законодательных работ. И коли роль Правительства не может умаляться, возможно, имело бы смысл ввести в практику поручения Думы и Совета Федерации Правительству на подготовку законопроекта, а не наоборот, как это фактически имеет место сейчас.

В этом свете крайне позитивно следует оценивать нововведение, появившееся в Конституции РФ в 2020 г., о том, что исполнительная власть осуществляется Правительством РФ под общим руководством Президента РФ (ст. 110 Конституции РФ), чем, думается, будут откорректированы функции Кабинета Министров как органа власти, реализующего свою компетенцию преимущества в сфере руководства министерствами и ведомствами (ч. 3 ст. 110 Конституции РФ) и осуществляющего свои функции исполнительными и распорядительными способами, а не законотворчеством. Нетрудно догадаться, что любой законопроект, вышедший из стен Правительства, будучи результатом работы того или иного министерства (агентства, службы), не может не нести на себе печать ведомственного интереса и тем самым дистанцироваться от общегосударственной потребности в законодательном решении соответствующего вопроса. В руках Кабинета Министров есть важнейший механизм формирования экономической и социальной атмосферы в стране — разработка и представление в Государственную Думу Федерального бюджета и иные исключительные полномочия (ст. 114 Конституции РФ). Представляется, что слишком глубокая вовлеченность Правительства в законотворчество, отвлекая его аппарат от других функций и облегчая жизнь депутатскому корпусу, в конечном счете создает «порочный круг» в законотворчестве и входит в диссонанс с полномочиями Федерального Собрания РФ.

Справится ли Федеральное Собрание и его палаты с огромным объемом информации, требующей анализа для подготовки того или иного законопроекта, особенно если это фундаментальный закон, а не поправки к действующим законам? Но прошлое подсказывает, что такие объемные и важные акты, как Налоговый кодекс

и Бюджетный кодекс, в качестве законопроектов имеют местом рождения именно Государственную Думу. И здесь вырисовывается проблема *информационной недостаточности* российской представительной власти, которую можно назвать и несостоятельностью, и большая зависимость комитетов государственной власти от органов исполнительной власти в этих вопросах и опасность освещения тех или иных потребностей управления экономикой в нужном для исполнительной власти свете. Чем, например, объяснить, что новая редакция Кодекса об административных правонарушениях, действовавшего до января 2020 г., вопреки заверениям Правительства о смене самой концепции этого акта, ничем существенно не отличается от действующей редакции, вобравшей в себя весь негатив административного хаоса, царящего в стране?

Для решения проблемы *качества информации*, лежащей в основе законодательства и законодательных актов как таковых, следует обратиться к мотивам и целям законодателя. К сожалению, в нашей стране за долгий период становления государственной власти сложилась и укрепилась презумпция суровости, императивности и жесткости закона и любой правовой информации, исходящей от власти. На эту историческую презумпцию за годы советской власти наложилась позитивная обязательность и неоспоримость нормативных актов власти (поэтому нормотворчество сконцентрировалось в руках Правительства — СНК). Любой акт, исходящий от СНК — СМ в советский период, содержал новые ограничения, меры ответственности, обязанности, но главное — налагал на адресатов не только правовые, но и политические требования совершения соответствующих действий, достижения результатов и прочее. За редким исключением, правительственными постановлениями осуществлялось юридическое и внеюридическое принуждение к позитивному поведению — и это совершенно естественно для концепции управления в советское время, построенной на подчинении всех субъектов экономической и социальной жизни руководящему центру, буквально диктующему свои императивные требования. Как показала история нашей страны, продолжительное время такой стиль управления (назовем его этатическим) был не только приемлем, эффективен, но и необходим — вспомним войну и восстановление народного хозяйства. Но с известного времени этатическое управление стало все больше и больше демонстрировать свои недостатки и неэффективность.

С реконструкцией социально-экономической формации в начале 90-х годов прошедшего века стиль управления существенно изменился, а управленческое воздействие преследует цель побуждения трудовых коллективов как производственной, так и непроизводственной сфер экономики к саморазвитию, конкуренции и совершенствованию через экономические стимулы и интересы, а государственный интерес рассматривает как кумулятивный, складывающийся из результатов отдельных предприятий и отраслей. Далеко не случайно первичное звено производства рассматривается как основное, решающее проблемы экономического роста. На этом фоне особенно диссонирующими аккордами становятся законодательные акты, воплощающие реликтовые всплески имперской мудрости, которыми, как правило, реализуется управленческий интерес по созданию благоприятных условий для административной [3] прослойки. Примером таких решений следует назвать «регулятивную песочницу» — попытку внести дезорганизацию в механизм управления отраслями путем предоставления льгот и изъятий из единообразного режима хозяйствования отдельных предприятий по непредсказуемым и, скорее всего, субъективным критериям[2].

Резюмируя эту часть изложения, следует заметить, что управленческая информатика нуждается в собственных механизмах обеспечения соответствия требованиям, задачам и стилю управления. Наряду с традиционными — кодификация, справочные информационные службы и фонды, — потенциально большой эффект ожидается от цифровизации, средствами которой будет формироваться новый правовой феномен: устранение из цикла управления профессиональных менеджеров, создающих информационные лагуны, и дезорганизующих экономическое развитие.

Следует признать правовую информатику неотъемлемой частью механизма как государственности, так и корпоративного управления экономическим развитием, имеющей свою организационную форму, принципы функционирования и цели осуществления. Развивающийся процесс перехода на цифровую экономику целесообразно понимать как существенное изменение механизма *управленческой правовой информатики*.

Если правовое воздействие на товаропроизводителей рассчитано на соответствующую реакцию адресата тех или иных управленческих инициатив, то его (товаропроизводителя) реакция, проявляющаяся в виде конкретных хозяйственных решений, также является предметом и объектом правовой информатики. Здесь имеются в виду разнообразные *«обратные связи»* (Н. Винер) хозяйственного органа с управляющими центрами.

Традиционно обратные связи понимаются как контроль вышестоящего органа, налоговых, инспекционных и других органов государства. В последнее время сюда же встроились и специальные подразделения органов вертикально интегрированных структур. Насколько соответствует задачам получения объективных данных о состоянии дел в экономике сведение всех обратных связей к контролю?

Контроль, будь он технологическим, финансовым, операционным, исполнительским или иным другим, в конечном счете предполагает возникновение некоего дополнительного лица, полномочного на изъятие, фик-

[2] Федеральный закон от 31 июля 2020 г. № 250-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации».

сирование, документирование фактических данных, характеризующих состояние производства, и трансформацию полученных данных в юридически значимый документ оценочного характера, способный вызывать ту или правоохранительную реакцию или организационные, кадровые и другие последствия. Полномочиям этого должностного лица корреспондирована обязанность администрации проверяемого хозоргана подвергнуться контролю — выдать документы, иную информацию, дать пояснения и др. Налицо особые, а именно контрольные *информационные правоотношения* представительно-обязывающего типа.

Контроль, несомненно, обладает рядом достоинств и преимуществ. Здесь и оперативность, и углубленная специализация контролеров, и возможность пресечения противоправной деятельности. На стороне контроля — использование сложившихся и закрепленных законодательно процедур осуществления контроля, возможность обжалования, в том числе и в судебном порядке, результатов проверки. Несомненно, контроль был и остается главной информационно-правовой конструкцией, обеспечивающей потребность обратных связей.

Чем же вызвано появление параллельных контролю других информационных средств, число которых медленно, но постоянно растет? В нашей стране еще до начала XX в. произошло разделение государственного контроля и надзора (в первую очередь прокурорского). Впоследствии в силу усложнения экономической жизни возникают и преобразуются самые различные структуры и органы, взять хотя бы советские контрольные органы — рабоче-крестьянская инспекция, наркомат госконтроля, партийно-государственный контроль, народный контроль, каждый из которых существенно отличался от предыдущих. В отраслях народного хозяйства за годы сменилось множество инспекционных органов. В постсоветское время бремя проведения проверок было возложено на еще больший круг агентств, служб, непосредственно на некоторые министерства, был учрежден высший контрольный орган — Счетная Палата и контрольно-счетные органы субъектов федерации.

Необходимо отметить два взаимосвязанных момента. Представляется, что в силу недостаточной информационной эффективности контроля мы не должны продолжать руководствоваться ленинским лозунгом «Социализм — это контроль и учет» и более не понимать контроль как всю систему органов управления. И второе — особенности экономики в современный период требуют использования информационных технологий, «вмонтированных» в хозяйственные отношения и тем самым обладающих большей эффективностью. Одна из них — *финансовый мониторинг*, пришедший из-за границы, но нашедший здесь и развитие, и национальную специфику. В России это механизм предотвращения обналичивания безналичных денежных средств или вывода их за пределы страны, а также борьба с финансированием терроризма. Ряд попыток доказательства относимости финансового мониторинга к контролю, думается, успеха не имели прежде всего потому, что финансовый мониторинг ведется без использования представительно-обязывающего механизма, путем оперативного наблюдения за совершением финансовых операций [11, 12].

Трудно доказуема относимость к контролю и такого вида информационной деятельности, как *аудит*, осуществляемый, как правило, в интересах собственника предприятия или партнеров коммерческого товарищества с целью получения достоверных данных об экономическом положении хозяйствующего субъекта. И в том случае, когда проводится обязательный аудит по решению суда, предметом проверки служит не столько правоохранительный аспект, сколько коммерческое благополучие субъекта хозяйствования.

Не пытаясь принять участие в многолетней дискуссии о соотношении контроля и надзора, нужно заметить, что *надзорные органы* по своим задачам и функциям существенно дистанцированы от органов контроля тем, что надзору предоставлены, как правило, собственные юрисдикционные полномочия, чего у органов контроля не наблюдается. Надзорная деятельность, возложенная на агентства и службы, ведется в режиме инспектирования в *меньшей* мере деятельности, соответствующей администрированию; в *большей* — реальному состоянию поднадзорных объектов при наличии предварительных данных о тех или иных нарушениях или угрозах.

Особое место занимает *надзор, осуществляемый органами прокуратуры*. Созданная несколько веков назад как служба безопасности прокуратура неоднократно меняла функции и цели своей деятельности вплоть до наших дней, став органом наблюдения за соблюдением режима законности и применения специфических мер прокурорского реагирования на факты нарушения закона во всех сферах правонарушения, но с существенным креном в сторону уголовно-процессуальной деятельности. Прокурорский (общий) надзор следовало бы рассматривать как метод осуществления информационной деятельности, касающейся соблюдения законов и других правовых актов в ходе их применения. Управленческую нагрузку в действиях прокуратуры отыскать несложно, но таковая носит сопутствующий, параллельный характер.

Следует также заметить, что надзорные функции нередко соседствуют в компетенции органов управления с основными функциями и задачами — в том случае, когда тот или иной орган обладает возможностями получать и отрабатывать соответствующую информацию, не прибегая к специальным проверкам и обследованиям. В стране также действует большое количество органов с властными полномочиями, осуществляющих надзор за опасными производствами, состоянием природной среды, соблюдением прав и интересов граждан и в других сферах. Хотя законодатель не всегда воспринимает грань между надзором и контролем, в большинстве случаев эта грань все же присутствует. С

учетом того, что закон, иной нормативный правовой акт есть воля государства и концентрированное изложение его политики, *именно информация о соблюдении законности* в конечном счете составляет квинтэссенцию обратных связей. В качестве примера можно было бы привести соотношение компетенции ФНС как органа налогового контроля и налоговой полиции, ныне упраздненной, как органа налогового надзора.

Поскольку контроль есть не что иное, как *информационная процедура*, ориентированная на получение сведений фактического характера о состоянии дел на подконтрольном объекте, его следует рассматривать как этап, противоположный надзору по целям и задачам. В ходе контроля проверяется полнота исполнения должностными лицами подконтрольного объекта (предприятия, организации, органа управления) возложенных на них обязанностей, а также полнота использования ими прав и полномочий. Если надзорная деятельность призвана зафиксировать отступления от законности и имеющихся правил решения в объективном смысле, то контроль своим объектом видит субъективные права и обязанности (компетенцию) должностных лиц.

Мониторинг. Это понятие вошло в юридическую практику относительно недавно, в связи с возникновением необходимости пооперационного наблюдения за криминализированными сферами экономической жизни, прежде всего, с противоправными действиями в сфере денежного обращения. Существо мониторинга состоит в сборе и анализе информации о денежных и связанных с ними операциях, относящихся к сомнительным (подозрительным) сделкам по субъекту их совершения, характеру операций, правовой природе и другим признакам. Соответственно, осуществление мониторинга предполагает анонимность, бесконтактность наблюдения и получение доступа к интересующей информации по ходу совершения денежных сделок, что не предполагает существования специального правового режима взаимоотношения органа мониторинга с наблюдаемым субъектом. В сущности, мониторинг — наиболее эффективный инструмент наблюдения в области обратных связей, и его применение ограничено только техническими возможностями и законоположениями о коммерческой тайне.

В перспективе средствами мониторинга с привлечением современных числовых технологий, возможно, будут осуществлять наблюдение за сохранностью и эффективным использованием природных объектов, строительством, движением материальных ценностей и другими технологическими процессами. Мониторинг уже успешно применяется в управлении транспортом, в ходе проведения выборов, при проведении массовых мероприятий. Есть все основания рассматривать мониторинг как наиболее перспективную информационную процедуру, отличную от надзора и контроля. Это же относится к информационной процедуре, вытекающей из корпоративных отношений — *аудиту*, который нередко включают в круг контрольных отношений.

Заметим, что аудит осуществляется вне сферы государственного принуждения (как уже сказано выше, аудит Счетной палаты РФ и контрольно-счетных органов субъектов Федерации есть проявление прав собственности государства на федеральный и региональный бюджеты соответственно). Аудит в своей основе носит «горизонтальный» характер, его результаты влекут корпоративные правовые последствия, его целью служит поддержание или восстановление режима эффективного распоряжения материальными и финансовыми ресурсами корпоративной структуры. Хотя аудит тесно соприкасается и переплетается с финансовым и другими видами контроля, выделение аудита в отдельное и юридически самостоятельное направление информационного обеспечения экономического управления представляется весьма важным для повышения значения аудита, особенно в сфере функционирования крупных вертикально агрегатированных хозяйственных структур.

Пониманию выше затронутой «великой четверки» (*надзора, контроля, аудита, мониторинга*) как всеобъемлющего и замкнутого круга каналов получения органами власти и управления информации в режиме обратных связей препятствует то, что нередко эта информация происходит от средств массовой информации, от оперативной деятельности правоохранительных органов, из расследования уголовных дел, из других источников. Нередко эти каналы даже более оперативны и эффективны, нежели вышеназванные.

Сверхважное значение имеют *данные государственной статистики* [7, 8], в которой отдельные формы и состояния обретают силу закономерностей и тенденций. Представляется, что вся правоохранительная и аналитическая деятельность в сфере экономической информации должна в своей основе иметь именно статистические данные. «Сегодня налицо дефицит информации. Следовательно, статистика во всем мире — это все, что угодно, кроме самой статистики. На самом деле статистика — это достоверные факты, которые практически устанавливаются так, как устанавливается истина в суде» — пишут ученые-экономисты, оценивая положение дел в сфере статистики [1].

Подобное можно сказать и о других каналах информации, формально не охватываемых «великой четверкой». Можно предположить, что, сводя все обратные информационные потоки к контролю, мы впадаем в логическую ошибку, подменяя множественное единичным и тем самым обедняя и «элементаризируя» сложное информационное и экономико-политическое явление. Поэтому-то обречены на неуспех попытки подготовить приемлемый законопроект о контроле, предпринимаемые раз от раза заинтересованными ведомствами. Предметом закона в этой области должны стать все основные информационные потоки, обслуживающие обратные связи, а не только контроль. Скорее всего, речь может идти о консолидации многих информационно-правовых конструкций, в том числе *методом отражения* содержания

ряда действующих федеральных законов в той мере, в какой эти законы затрагивают обратные информационные отношения. Скорее всего, речь может идти не о федеральном законе, регламентирующем контроль, а о регламентации всех или большей части существующих информационных каналов обратной связи в сфере управления; недооценка иных, нежели контроль, способов получения информации примитивизирует управление, искажает действительную картину происходящего в экономике.

Обращает на себя и то, что в стране отсутствует официальный (легальный) центр обработки всего массива информации, полученной методом обратных связей. Прокурорский, банковский, специализированный надзор «обслуживает» уполномоченные органы, аудит и мониторинг реализуются в сугубо ведомственном порядке, контроль носит отраслевой характер, бóльшая доля информации, полученной в ходе деятельности правоохранительных органов, оседает в закрытых базах данных; межведомственные связи в этой сфере по обмену информации, несмотря на многие предпринимавшиеся в прошлом меры, слабы и малоэффективны.

Думается, есть основания поставить вопрос о создании *механизма концентрации* разнообразной и разнородной экономико-правовой информации в едином фонде. В сущности, этой работой с переменным успехом занимается Счетная Палата РФ, собирая и анализируя опыт финансового контроля, который достаточно близок и к надзору, и к статистике, и к аудиту, и к оперативной и следственной информации, и к мониторингу. Речь идет не об оруэлловском «Большом Брате», а об экономичном распоряжении дорогими в получении сведениями, которые в настоящее время безнадежно устаревают, теряют *актуальность* [4] и бесследно исчезают. Безусловно, в этом случае актуальность приобретает проблема дискреции в оценке полученных данных, но и сейчас далеко не каждое правонарушение вызывает охранительную реакцию и, кроме того, общество и государство должны получить более диверсифицированную шкалу мер правового реагирования на экономические правонарушения, нежели сейчас.

Завершая рассмотрение предмета правовой информатики, подчеркнем ее производность от механизма правового регулирования, действующего в стране, и зависимость от тенденций и перспектив совершенствования этого механизма. В конечном счете речь идет о повышении *качества, достоверности* и *«чистоты»* информации, лежащей в основе законопроектов, принимаемых Федеральным Собранием, и обеспечении всех правообладателей, правоприменителей и правоохранителей полными и недвусмысленными сведениями о правовой среде их деятельности, их правах, обязанностях и долженствованиях во всех сферах экономических и политических отношений.

Литература

1. Болдырев Ю., Абрамов М., Бочаров М., Кашин В., Симчера В. Экономика России: что происходит и что делать. М. : Экономика, 2019. 319 с. ISBN 978-5-282-03524-7.
2. Жарова А. К. Теоретические основания правового регулирования создания и использования информационной инфраструктуры в Российской Федерации : автореф. дисс. ... д-ра юрид. наук: 12.00.13. М., 2020.
3. Запольский С. В. Эффективность администрирования в управлении экономикой // Правовая информатика. 2017. № 3. С. 4—13. DOI: 10.21681/1994-1404-2017-3-04-13.
4. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
5. Ловцов Д. А. Системологические основы эффективного правового регулирования информационных отношений в инфосфере // Мониторинг правоприменения. 2020. № 1(34). С. 37—44. DOI: 10.21681/2226-0692-2020-1-37-44.
6. Ловцов Д. А. Теоретические основы системной информатизации правового регулирования // Правовая информатика. 2019. № 4. С. 12—28. DOI: 10.21681/1994-1404-2019-4-12-28.
7. Ловцов Д. А., Богданова М. В., Лобан А. В., Паршинцева Л. С. Статистика (компьютеризированный курс) / Под ред. проф. Д. А. Ловцова. М. : Рос. гос. ун-т правосудия, 2020. 400 с. ISBN 978-5-93916-834-2.
8. 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. DOI: 10.21681/1994-1404-2017-1-28-36.
9. Михайлов Н. И. Правовое моделирование корпоративных комплексов (интегрированных структур) : монография. М. : ИГП РАН, 2016. 160 с. ISBN 978-5-8339-0168-7.
10. Мошкова Д. М. Правовое регулирование финансирования образовательных и научных организаций: вопросы теории и практики : монография. М. : РГ-Пресс, 2015.
11. Новиков О. В. Информационная роль бухгалтерского (финансового) учета в Российской Федерации // Правовая информатика. 2017. № 4. С. 62—66. DOI: 10.21681/1994-1404-2017-4-62-66.
12. Прошунин М. М. Финансовый мониторинг. М. : Статут, 2009.
13. Черный Ю. А. Некоторые характеристики федерального законодательного процесса в 1994—2011 гг.: статистический материал. М. : НИУ «ВШЭ», 2013. 52 с.

Рецензент: ***Исаков Владимир Борисович,*** *доктор юридических наук, профессор, заслуженный юрист Российской Федерации, действительный государственный советник Российской Федерации 1 класса, заведующий кафедрой теории права и сравнительного правоведения Национального исследовательского университета «Высшая школа экономики», г. Москва, Россия.*
E-mail: visakov@hse.ru

LEGAL INFORMATICS AND MANAGING ECONOMIC SECTORS

Sergei Zapol'skii, *Dr.Sc. (Law), Professor, Meritorious Lawyer of the Russian Federation, Chief Researcher at the Institute of State and Law of the Russian Academy of Science, Moscow, Russian Federation.*
E-mail: *zpmoscow@mail.ru*

Keywords: *law-making, laws, executive power, government, industry branch governing bodies, control, oversight, monitoring, audit, law enforcement agencies, statistics, enterprises, corporations.*

Abstract.

Purpose of the work: improving the scientific and methodological basis for the theory of legal regulation of economic relations in the information society.

Methods used: a systemic historical analysis of information relations in the sphere of economic management as a subject of information and legal regulation and a means of optimal organisation of the process of government and corporate management of economic development.

Results obtained: a justification is given for dividing information relations in the considered area into direct and inverse ones: the direct ones are those concerning rule-making and communicating management instruments to their addressees, the reverse ones, concerning the collection and processing of information on compliance with the law and economic results; one of the shortcomings of the law drafting procedure is, in the author's opinion, the dominance of the opinion of executive power over the will of representative bodies and the position of the expert and analyst community, political and public organisations as well as flaws in the law-making technique; control, oversight, monitoring and audit are considered as united by one application purpose, but legally different ways of collecting, processing and implementing economic and legal information relating to the national economy; it is needed to use more efficiently the features of these forms of reverse information transfer whose mechanism it is would be advisable to build on government statistics data and other information sources, including the media, etc.; an opinion is expressed about the inexpediency of reducing all feedback to control only; a conclusion is made that legal informatics should become a tool of government management of the economy as an integral part of this mechanism.

References

1. Boldyrev Iu., Abramov M., Bocharov M., Kashin V., Simchera V. Ekonomika Rossii: chto proiskhodit i chto delat'. M. : Ekonomika, 2019. 319 pp. ISBN 978-5-282-03524-7.
2. Zharova A. K. Teoreticheskie osnovaniia pravovogo regulirovaniia sozdaniia i ispol'zovaniia informatsionnoi infrastruktury v Rossiiskoi Federatsii : avtoref. diss. ... d-ra iurid. nauk: 12.00.13. M., 2020.
3. Zapol'skii S. V. Effektivnost' administrirovaniia v upravlenii ekonomikoi. Pravovaia informatika, 2017, No. 3, pp. 4-13. DOI: 10.21681/1994-1404-2017-3-04-13 .
4. Lovtsov D. A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016, 316 pp. ISBN 978-5-93916-505-1.
5. Lovtsov D. A. Sistemologicheskie osnovy effektivnogo pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. Monitoring pravoprimeneniia, 2020, No. 1(34), pp. 37-44. DOI: 10.21681/2226-0692-2020-1-37-44 .
6. Lovtsov D. A. Teoreticheskie osnovy sistemnoi informatizatsii pravovogo regulirovaniia. Pravovaia informatika, 2019, No. 4, pp. 12-28. DOI: 10.21681/1994-1404-2019-4-12-28 .
7. Lovtsov D. A., Bogdanova M. V., Loban A. V., Parshintseva L. S. Statistika (komp'iuterizirovannyi kurs), pod red. prof. D. A. Lovtsova. M. : Ros. gos. un-t pravosudiia, 2020, 400 pp. ISBN 978-5-93916-834-2.
8. 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. DOI: 10.21681/1994-1404-2017-1-28-36 .
9. Mikhailov N. I. Pravovoe modelirovanie korporativnykh kompleksov (integrirovannykh struktur) : monografiia. M. : IGP RAN, 2016, 160 pp. ISBN 978-5-8339-0168-7.

10. Moshkova D. M. Pravovoe regulirovanie finansirovaniia obrazovatel'nykh i nauchnykh organizatsii: voprosy teorii i praktiki : monografiia. M. : RG-Press, 2015.
11. Novikov O. V. Informatsionnaia rol' bukhgalterskogo (finansovogo) ucheta v Rossiiskoi Federatsii. Pravovaia informatika, 2017, No. 4, pp. 62-66. DOI: 10.21681/1994-1404-2017-4-62-66 .
12. Proshunin M. M. Finansovyi monitoring. M. : Statut, 2009.
13. Chernyi Iu. A. Nekotorye kharakteristiki federal'nogo zakonodatel'nogo protsessa v 1994-2011 gg.: statisticheskii material. M. : NIU "VShE", 2013, 52 pp.

ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЦИФРОВОЙ ЭКОСИСТЕМЫ ЗДРАВООХРАНЕНИЯ

Карцхия А. А.*

***Ключевые слова**: биометрические данные, право в здравоохранении, информационные технологии, искусственный интеллект, цифровая медицина, телемедицина, цифровое здравоохранение.*

Аннотация.

Цель исследования заключается в определении особенностей применения информационных технологий в правовом регулирования цифрового здравоохранения, а также определении основного понятийного аппарата и структуры правового механизма цифровой экосистемы здравоохранения.

Метод исследования: сравнительно-правовой анализ актуального национального российского и зарубежного законодательства, стратегических документов и международных договоров и соглашений по вопросам цифрового здравоохранения и медицины с учетом структурно-ценностной оценки информационных технологий, применяемых в цифровой медицине.

Результат: исследование выявило особенности начального этапа формирования специального законодательства в области цифрового здравоохранения и цифровой медицины и позволило сделать вывод об исключительной важности нового направления в медицине и перспективности цифрового здравоохранения в современных условиях, что потребует разработки специального законодательства в этой сфере.

DOI:10.21681/1994-1404-1-13-23

Введение

В последние десятилетия цифровые технологии стали широко использоваться в медицине и здравоохранении. Эта тенденция набирает популярность во многих развитых странах, и по мере развития современных технологий и цифровизации медицины идет формирование новой области традиционной медицины — цифровой медицины.

Цифровая медицина развивается бурными темпами благодаря стремительному освоению медициной таких технологий, как искусственный интеллект *(artificial intelligence*), который обеспечивает новые решения для диагностики и лечения; большие данные (*big data*), которые создают облачные хранилища и служат основой предиктивной аналитики; телемедицина и программные приложения, особенно востребованные в эпоху эпидемии; блокчейн-технология (*blockchain tech*), обеспечивающая безопасность и достоверность сведений и обработку биометрических и иных медицинских данных; медицинский Интернет вещей (*IoT*), формирующий экосистему устройств и датчиков для мониторинга и защиты здоровья человека.

В частности, технологии искусственного интеллекта используются для диагностики онкозаболеваний и радиологических обследований (платформа «*Watson Health*» от *IBM* и российская разработка «*TeleMD*»), технология офтальмологических клиник *Google* «*DeepMind Health*», УЗИ-диагностика беременности «*ScanNav*» или диагностика при помощи микроскопа «*BIDMC*», нейронная сеть которого изучает изображения вредоносных бактерий для выявления заболевания крови, и, конечно, всемирно известный робот-хирург «*Da Vinci*» с искусственным интеллектом, который работает во многих клиниках по всему миру[1].

Сфера медицины и биотехнологий становится особой сферой защиты прав и интересов личности и общества, сферой национальной безопасности [3].

Вместе с тем необходимо учитывать современные особенности развития цифровизации в медицине, а также появление новых рисков и негативных факторов в национальных системах здравоохранения. Так, в специальном докладе Всемирному экономическому форуму (Давос, 2021)[2] отмечалось, что глубинные диспропорции в здравоохранении, образовании, финансовой стабильности и технологиях привели к тому, что

[1] World Robotics Statistics. International Federation of Robotics (IFR). URL: https://ifr.org/ downloads/ press2018/WR_Presentation_Industry_and_Service_Robots_rev_5_12_18.pdf.

[2] The Global Risks Report 2021, 16th Edition, World Economic Forum, 2021. URL: https://www.weforum.org/ reports.

* ***Карцхия Александр Амиранович,*** *доктор юридических наук, доцент, профессор кафедры гражданско-правовых дисциплин РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия.*

E-mail: arhz50@mail.ru

кризис пандемии *Covid*-19 непропорционально сильно повлиял на определенные социальные группы и страны. Пробелы в общественном здравоохранении, цифровое неравенство, неравенство в образовании и безработица, возникшие в результате сложного сочетания существующего неравенства и последствий пандемии, в наибольшей степени затрагивают уязвимые группы населения и приводят к «социальной фрагментации», что обусловливает ускоренное развитие возможностей системы здравоохранения среди других ключевых областей реагирования на пандемию *Covid*-19 и последующее совершенствование медицины. Пандемия привела к перенапряжению в национальных системах здравоохранения, выявив их недостаточный потенциал, а число людей без доступа к качественному и доступному медицинскому обслуживанию, образованию или цифровым инструментам возрастает как в развитых, так и в развивающихся странах. Обездоленные социальные группы вступили в кризис пандемии с более низкой устойчивостью в результате неравенства в благосостоянии, финансовой стабильности и безопасности, а также доступа к здравоохранению, образованию и технологиям. Как показано в докладе, в краткосрочной перспективе справедливое и эффективное распределение вакцин находится под угрозой из-за протекционистских тенденций и геополитической напряженности — точно так же, как эти тенденции и напряженность поставили под угрозу основные поставки медикаментов в период пандемии. В долгосрочной перспективе неравный доступ к качественному медицинскому обслуживанию будет сохраняться в результате возрастающей нагрузки на системы здравоохранения во всем мире. Потенциал здравоохранения в некоторых европейских странах уже пострадал от длительных мер жесткой экономии. Неспособность ликвидировать пробелы в общественном здравоохранении усугубит существующую уязвимость человека и создаст риск дальнейших всё возрастающих гуманитарных и экономических потерь.

Стратегическое значение развития цифровой медицины

Большое значение для развития цифрового здравоохранения имеет принятая Всемирной организацией здравоохранения (ВОЗ) Глобальная стратегия развития цифрового здравоохранения на 2020–2025 гг. (далее — Глобальная стратегия)[3], которая основывается на резолюциях, принятых Генеральной Ассамблеей ООН[4] и Всемирной ассамблеей здравоохранения[5], а также ряда региональных докладов ВОЗ и Стратегии электронного здравоохранения (*National eHealth strategy toolkit*)[6]. Глобальная стратегия выделяет значение таких технологий, как Интернет вещей, виртуальная помощь, удаленный мониторинг, искусственный интеллект, аналитика больших данных [15], блокчейн [8], умные носимые устройства, платформы, инструменты, обеспечивающие обмен и хранение данных, а также устройства, обеспечивающие удаленный сбор данных и обмен данными и соответствующей информацией для всей экосистемы здравоохранения. Все эти технологии обеспечивают единый процесс оказания медицинской помощи, который доказал свой потенциал для улучшения результатов здравоохранения за счет улучшения медицинской диагностики, принятия решений о лечении на основе медицинских и биометрических данных, цифровой терапии, клинических испытаний, самостоятельного управления медицинской помощью и ухода за пациентами, ориентированного на человека, а также создания большего количества научно обоснованных знаний, навыков и компетентности для специалистов в области поддержки здравоохранения. В Глобальной стратегии подчеркивается, что она способствует надлежащему использованию цифровых технологий в качестве *цифровых общественных благ*, которые могут быть адаптированы к различным странам и контекстам, чтобы помочь решить ключевые проблемы системы здравоохранения и поддержать справедливость в доступе к цифровым ресурсам. Стратегия способствует защите людей, населения, медицинских работников и систем от *дезинформации* (также называемой инфодемикой), а также от неправомерного использования информации, злонамеренной кибер-деятельности, мошенничества и эксплуатации, ненадлежащего использования медицинских данных, расизма и нарушений прав человека в рамках, установленных международными договорами, обязательными для государств-членов ВОЗ.

Цель Глобальной стратегии заключается в укреплении национальных систем здравоохранения путем применения цифровых медицинских технологий для потребителей, медицинских работников, поставщиков медицинских услуг и промышленности в целях расширения прав и возможностей пациентов и достижения цифрового здоровья для всех социальных групп населения.

В контексте Глобальной стратегии под цифровым здоровьем понимается *«область знаний и практики, связанная с разработкой и использованием цифровых технологий для улучшения здоровья»*. Это определение охватывает и ***электронное (цифровое) здравоохранение*** (*Digital health*), что в конечном итоге расширяет концепцию электронного здравоохранения, включив в нее цифровых потребителей с более широким спектром интеллектуальных и подключенных устройств. Она также охватывает другие виды использования

[3] Global Strategy on Digital Health 2020–2025, WHO, 2019. URL: https://www.who.int/docs/ default-source/documents.

[4] United Nations General Assembly resolutions 73/218 (2019) and 70/125 (2016).

[5] World Robotics Statistics. International Federation of Robotics (IFR). URL: https://ifr.org/ downloads/ press2018/WR_Presentation_Industry_and_Service_Robots_rev_5_12_18.pdf.

[6] The Global Risks Report 2021, 16th Edition, World Economic Forum, 2021. URL: https://www.weforum.org/ reports

цифровых технологий в здравоохранении, включая Интернет вещей, передовые облачные вычисления, аналитику больших данных, искусственный интеллект, объединяющий машинное обучение и робототехнику.

Глобальная стратегия направлена на формирование общего понимания всеми государствами-членами ВОЗ важности цифровых решений в области здравоохранения и подхода к созданию взаимодействующей ***цифровой экосистемы здравоохранения***, которая должна пониматься как цифровая взаимодействующая информационно-технологическая инфраструктура, которая в первую очередь используется медицинским сообществом во всех учреждениях и организациях здравоохранения, включая поставщиков медицинских услуг и производителей медицинского оборудования, а также органы общественного здравоохранения, медуниверситеты и научно-исследовательские учреждения. Взаимодействующая цифровая экосистема здравоохранения должна обеспечивать беспрепятственный и безопасный обмен медицинскими данными между пользователями, поставщиками медицинских услуг, менеджерами систем здравоохранения и службами медицинских данных. Медицинские данные в основном генерируются и обрабатываются между поставщиками медицинских услуг и медицинским сообществом.

В Глобальной цифровой стратегии особая роль отводится ***медицинским данным***, которые должны классифицироваться как конфиденциальные персональные данные или личная идентифицируемая информация, требующая высокого уровня безопасности. В силу этого подчеркивается важность создания прочной *нормативно-правовой* ***базы*** для защиты частной жизни, *конфиденциальности, целостности* и доступности [6] данных и обработки персональных медицинских данных, а также в целях решения проблем кибербезопасности, укрепления доверия, подотчетности и управления, этики, справедливости, наращивания потенциала и грамотности, обеспечения сбора качественных данных и последующего обмена ими для поддержки планирования, ввода в эксплуатацию и преобразования услуг.

Обмен и обработка медицинских данных в контексте ориентированной на человека цифровой экосистемы здравоохранения и в целях обеспечения общественных интересов должны поощряться с согласия пациента [14], если это осуществляется на основе взаимного доверия, защищает частную жизнь пациента и цифровые системы медицины, а также предохраняет от злонамеренного или ненадлежащего использования медицинских данных. Такая система обработки медицинских данных жизненно необходима, поскольку она может способствовать повышению качества процессов и результатов медицинских услуг, оптимальности ухода за пациентами (первичное использование медицинских данных). Это, очевидно, приведет к созданию базы знаний, которая должна быть способна взаимодействовать с другими системами данных, включая, например, данные о социальных детерминантах здоровья и аналогичные реестры. Вторичное использование медицинских данных важно для улучшения качества медицинской помощи и эффективности научных исследований. Это может позволить проводить тестирование, валидацию и бенчмаркинг решений для искусственного интеллекта и анализа больших данных по различным параметрам и настройкам.

При надлежащем использовании цифрового здравоохранения, как определено в Глобальной стратегии, должны учитываться следующие факторы: укрепление здоровья и профилактика заболеваний, безопасность пациентов, этика отношений, интероперабельность, защита *интеллектуальной собственности*, безопасность (конфиденциальность, целостность и доступность) данных, конфиденциальность и экономическая эффективность, а также вовлеченность пациентов и доступность данных. Растущая глобальная проблема *«цифровых отходов»* в связи со здравоохранением и окружающей средой также должна быть надлежащим образом решена.

Основная стратегическая цель этого документа направлена на стимулирование и поддержку каждой страны в создании, адаптации и укреплении своей стратегии в области цифрового здравоохранения таким образом, чтобы она наилучшим образом соответствовала национальному видению, контексту, ситуации и тенденциям в области здравоохранения, имеющимся вариантам политики и действиям, ресурсам и основным ценностям каждого государства — члена ВОЗ.

Такая направленность нацелена на укрепление управления цифровым здравоохранением национального и международного уровня путем создания устойчивых и надежных структур управления и создания потенциала для цифрового здравоохранения на глобальном и национальном уровнях, а также предусматривает укрепление потенциала и навыков, необходимых странам для продвижения, внедрения инноваций и расширения масштабов цифровых технологий здравоохранения. В целом Глобальная стратегия способствует обеспечению стандартов безопасности, конфиденциальности, интероперабельности и этического использования данных в секторе здравоохранения и за его пределами, а также включает принципы этического использования медицинских данных в таких технологиях, как искусственный интеллект и аналитика больших данных и др.

Глобальная стратегия предполагает создание национальных взаимодействующих ***цифровых экосистем здравоохранения*** (*digital health ecosystem*), которые должны быть созданы таким образом, чтобы информационно-технологические инфраструктуры здравоохранения разных стран были совместимы друг с другом и, учитывая различия национального законодательства и политики, могли обмениваться медицинскими данными с инфраструктурами других стран. Информационно-технологическая инфраструктура здравоохранения, которая будет применяться в рамках взаимодействующей цифровой экосистемы здравоохранения,

будет основываться на общепринятой практике использования технологий в секторе общественного здравоохранения, функциональных требованиях и наборе функциональных и технических спецификаций, стандартов и профилей, полученных из них, которые должны основываться на прочной *нормативной правовой базе*, гарантирующей защиту данных, конфиденциальность и целостность персональных медицинских данных [14] и доступность систем цифрового здравоохранения.

В силу своей чувствительности ***данные о здоровье*** (*health data*) должны быть классифицированы как ***конфиденциальные персональные данные***, требующие высокого уровня безопасности. Общий набор основных правовых требований должен утверждаться государствами-членами в рамках руководства ВОЗ по глобальным стандартам интероперабельности для цифрового здравоохранения, служащего основой для ориентации национальной нормативно-правовой базы.

Глобальная стратегия предусматривает не только общий план развития цифровой экосистемы здравоохранения для государств — членов ВОЗ, но и определяет вектор развития законодательства в этой области.

Цифровизация медицины и персональных данных в российском законодательстве

Национальные системы здравоохранения, как утверждают исследователи[7] переживают цифровую революцию. Цифровые продукты для здоровья (*Digital Health*) стали неотъемлемой частью профилактики, диагностики, лечения и управления здоровьем и болезнями. Потребители используют цифровые мобильные приложения (*Digital Medicine*) для контроля своего здоровья, отслеживания физической формы и улучшения самочувствия. Клиницисты (*Digital Therapeutics, DTx*) используют цифровые продукты для здоровья, чтобы получить представление о результатах лечения пациентов, проводить телемедицинские визиты и лечить аспекты болезней, которые иначе не были бы устранены традиционными лекарствами.

Цифровые технологии становятся более портативными, простыми в использовании и доступными — от новых инструментов визуализации до мобильных устройств, что позволяет создавать технологически продвинутые инструменты для лечения и ухода за пациентами[8].

В этой связи следует отметить, что цифровое здравоохранение, которое создается в России, как отмечают специалисты[9], базируется на трех принципах: (1) организация медицинской помощи за счет централизации всех данных в цифровом виде, (2) применение методов искусственного интеллекта для их обработки, (3) обеспечение коммуникации всех участников процесса, включая дистанционный мониторинг здоровья.

Цифровые технологии оказали и оказывают существенное влияние на качество и доступность медицинских услуг, появление новых методик лечения и профилактики заболеваний, повышение качества жизни здорового населения и хронических больных [5, 11, 12]. Кроме того, цифровизация в медицине, как показали исследования [2], позволила достичь нового уровня здравоохранения, включая:

(а) повышение качества диагностики за счет использования систем больших данных и машинного обучения;

(б) применение предсказательной аналитики и систем искусственного интеллекта для оценки влияния на организм новых препаратов;

(в) вследствие достижений в области роботизации и искусственного интеллекта появились новые возможности в трансплантологии при использовании умных имплантов и киберорганов (обучаемые руки, ноги);

(г) создание новых мер мониторинга здоровья пациентов с хроническими заболеваниями;

(д) разработка методик ранней диагностики с использованием данных от умных датчиков и носимых устройств (пульсометров, трекеров активности);

(е) повышение значения персональной медицины и телемедицины;

(ж) создание технологических платформ медицинских услуг для выбора специалиста и оказания медицинских услуг.

Современная телемедицина позволяет пациентам регулярно находиться на связи с медиками, что особенно важно для людей с ограниченными возможностями передвижения или пациентами, наблюдающимися у зарубежного врача.

Оказание медицинской помощи с применением телемедицинских технологий, в соответствии со ст. 36.2 Федерального закона от 21 ноября 2011 г. № 323-ФЗ (ред. от 07.03.2018) «Об основах охраны здоровья граждан в Российской Федерации» осуществляется при дистанционном взаимодействии медицинских работников с пациентами и (или) их законными представителями; это, как правило, дистанционное наблюдение (осмотр) или консультации (консилиумы врачей) в режиме реального времени[10]. При оказании медицинской помощи с применением телемедицинских технологий [19] применяются также технологии идентификации и аутентификации пациентов в соответствии с федеральной государственной *Единой системой идентификации и аутентификации* (ЕСИА).

В связи с этим в Российской Федерации активно разрабатывается правовая база цифровой медицины[11].

[7] Digital medicine: implications for healthcare leaders / Jeff Goldsmith, Medical informatics, 2003. URL: http://book.itep.ru/depository/it_med GS_DIGITAL_MED_ 1199.pdf .

[8] Global Strategy on Digital Health 2020–2025, WHO, 2019. URL: https://www.who.int/docs/ default-source/documents.

[9] United Nations General Assembly resolutions 73/218 (2019) and 70/125 (2016).

[10] Resolutions WHA58.28 (2005), WHA66.24 (2013), WHA69.24 (2016) and WHA71.7 (2018).

[11] WHO, ITU. National eHealth strategy toolkit. Geneva: World Health Organization and International Telecommunication Union. URL: https://apps.who.int/iris/handle/10665/752119, accessed 17 December 2019. Adopted in United Nations General Assembly resolution 70/1 (2015).

Цифровая медицина и телемедицина выделяются в качестве важных стратегических направлений развития здравоохранения и медицинских технологий, наряду с биомеханикой, превентивной медициной, медицинской генетикой. Среди приоритетных направлений развития фармацевтической промышленности указано внедрение цифровых технологий и лучших регуляторных практик на всех этапах разработки, производства и обращения лекарственных препаратов и биомаркеров[12].

Телемедицинские технологии используются и для идентификации и аутентификации участников дистанционного взаимодействия при оказании медицинской помощи с применением телемедицинских технологий в соответствии с ЕСИА [16]. Законом предусмотрено осуществление документирования информации об оказании медицинской помощи пациенту с применением телемедицинских технологий, включая внесение сведений в его медицинскую документацию. Такой документооборот осуществляется с использованием *усиленной квалифицированной электронной подписи* [6] медицинского работника. Введение в действие норм о применении телемедицинских технологий позволяет повысить качество медицины и выведет, по мнению исследователей этих вопросов, на новый уровень систему реализации лекарственных препаратов, порядок выписывания лекарственных средств и обеспечение граждан льготными лекарствами [12].

В России осуществляется создание *единого цифрового контура здравоохранения* на основе *Единой государственной информационной системы в сфере здравоохранения* (ЕГИСЗ) в соответствии с национальным проектом «Здравоохранение» и Федеральным законом от 2 декабря 2019 г. № 380-ФЗ (ред. от 18.03.2020) «О федеральном бюджете на 2020 год и на плановый период 2021 и 2022 годов», а также организация информационного взаимодействия *медицинских информационных систем* медицинских организаций частной системы здравоохранения с Единой государственной информационной системой в сфере здравоохранения (утв. Минздравом России 14.08.2020) [16].

В течение нескольких лет успешно применяются национальные стандарты (ГОСТ Р) РФ для детальной томографии на цифровых рентгеновских аппаратах, цифровых флюорографов и другие национальные стандарты[13].

Экспоненциальное развитие ряда технологий существенно меняет облик сферы здравоохранения благодаря развитию таких направлений, как синтетическая биология, 3D-печать, нанотехнологии, сопутствующая диагностика и др. В перспективе работа лечебных учреждений будет выстраиваться за счет пересмотра моделей медицинского обслуживания, внедрения цифровых технологий и искусственного интеллекта, а также комплексного развития кадровых ресурсов.

Комплексная цифровизация национальных систем здравоохранения, направленная на повышение качества здравоохранения, связана прежде всего с созданием баз электронных медицинских данных, внедрением решений в области интернет-медицины, мобильной медицины, обеспечением технической совместимости систем, использование больших массивов данных и др. Качественный уровень медуслуг может быть повышен благодаря степени персонализации услуг, эффективности взаимодействия с потребителями и качества обслуживания, предлагая пациентам цифровые решения для омниканального доступа, такие как мобильные приложения, порталы, персонализированные комплекты цифровой информации. В целях улучшения взаимодействия между поставщиками и потребителями услуг предполагается расширение использования таких цифровых инструментов, как анализ данных социальных сетей, телемедицина, виртуальная реальность [4].

Минздрав России расширяет использование робототехники в медицине. Так, к числу медицинских инструментов, аппаратов, приборов и прочих изделий, применяемых в медицинских целях отдельно или в сочетании между собой или вместе с другими принадлежностями, необходимыми для применения указанных изделий, Росздравнадзор[14] относит и *специальное программное обеспечение*, которое предназначено для профилактики, диагностики, лечения и медицинской реабилитации заболеваний, мониторинга состояния организма человека, проведения медицинских исследований.

В частности, программное обеспечение предназначено и используется для: (а) управления работой оборудования и мониторинга за его функционированием; (б) получения от оборудования диагностических данных, их накопления и расчета в автоматическом режиме; (в) мониторинга функций организма человека и передачи полученных данных (в том числе посредством беспроводных технологий); (г) расчета параметров подбора дозы (облучения, лекарственного средства, рентгеноконтрастного вещества и др.); (д) для обработки данных, полученных с диагностического медицинского оборудования, передачи их на системы планирования и терапии; (е) обработки медицинских изображений (включая изменение его качества, цветового разрешения и др.); (ж) для 3D-моделирования; (з) связи диагностического и лечебного оборудования; (и) для обработки цифровых изображений (в том числе с получением данных от диагностического оборудования в неизменном виде).

Искусственный интеллект с функцией машинного обучения, обработка большого массива биометриче-

[12] Digital medicine: implications for healthcare leaders / Jeff Goldsmith, Medical informatics, 2003. URL: http://book.itep.ru/depository/it_med GS_DIGITAL_MED_ 1199.pdf .

[13] ГОСТ Р 56324-2014. Национальный стандарт Российской Федерации. Изделия медицинские электрические. Аппараты рентгеновские цифровые для дентальной панорамной томографии. Технические требования для государственных закупок (утв. и введен в действие Приказом Росстандарта от 12 декабря 2014 г. № 2079-ст.).

[14] Tracie White. How digital medicine is improving patient care. URL: https://stanmed.stanford.edu/ 2018 fall/ digital-medicine-improve-patient-care.html.

ских и иных медицинских данных человека, компьютерное программирование и мониторинг процессов диагностики, лечения, терапии, хирургического и иных видов вмешательств, а также оценка и прогнозирование медицинских исследований и практики — далеко не полный перечень областей, где уверенно чувствует себя цифровая медицина. Например, широко применяются носимые человеком медицинские устройства, контролирующие состояние его здоровья и функционирование отдельных органов (сердца, легких и др.), общее состояние организма человека[15].

Использование в современной медицине искусственного интеллекта с *машинным обучением* [17] стало возможным благодаря использованию полученных больших данных, наряду с заметно увеличенной вычислительной мощностью и облачными сервисами. Для медицины это начинает оказывать влияние на *трех уровнях*:

– для клиницистов — преимущественно посредством быстрой и точной интерпретации изображений;

– для систем здравоохранения — за счет улучшения рабочего процесса и возможности сокращения медицинских ошибок;

– для пациентов — позволяя им обрабатывать свои собственные данные для укрепления здоровья.

Несмотря на имеющиеся пока проблемы в применении цифровых технологий, в том числе предвзятость, конфиденциальность и безопасность, а также отсутствие прозрачности, общий положительный эффект несомненен [20].

Большинство компьютерных алгоритмов в медицине, как отмечают исследователи[16], являются *«экспертными системами»* [14], т. е. набором правил, кодирующих знания по заданной тематике, которые применяются для получения выводов о конкретных клинических сценариях, таких как обнаружение лекарственных взаимодействий или оценка целесообразности получения рентгенологической визуализации. Экспертные системы работают так, как это сделал бы идеальный студент-медик: они берут общие принципы медицины и применяют их к новым пациентам. Искусственный интеллект на базе машинного обучения подходит к проблемам как врач: изучая правила из большого массива данных. Начиная с наблюдений на уровне пациента, алгоритмы просеивают огромное количество переменных, ища комбинации, которые надежно предсказывают результаты. В некотором смысле этот процесс аналогичен традиционным регрессионным моделям: существует результат, ковариантны и статистическая функция, связывающая их [9]. Эта способность позволяет использовать новые виды данных, объем или сложность которых ранее сделали бы их анализ невообразимым.

Используя значительные достижения в вычислительной мощности, цифровые пиксельные матрицы, лежащие в основе рентгенограмм, становятся миллионами индивидуальных переменных. Затем алгоритмы приступают к работе, объединяя пиксели в линии и формы и в конечном итоге изучая контуры линий переломов, паренхиматозных помутнений и многое другое. Даже традиционные данные по *страховым случаям* могут обрести новую жизнь: диагностические коды прослеживают сложную динамическую картину истории болезни пациентов, гораздо более богатую, чем статические переменные для сосуществующих состояний, используемые в стандартных статистических моделях. Однако алгоритмы могут «подгонять» предсказания к ложным корреляциям в данных, что может давать неустойчивые оценки, повлиять на точности модели.

Другим ключевым вопросом является количество и качество входных данных. Алгоритмам *машинного обучения* [16] для достижения приемлемого уровня производительности часто требуются миллионы наблюдений. Компании тратят огромные ресурсы на сбор высококачественных, непредвзятых данных для обеспечения своих алгоритмов, а существующие данные в электронных медицинских картах или базах данных претензий нуждаются в тщательном хранении и обработке, прежде чем их можно будет использовать. Вместе с тем машинное обучение стало повсеместным и незаменимым для решения сложных задач в большинстве наук. В астрономии алгоритмы просеивают миллионы изображений с телескопов, чтобы классифицировать галактики и найти сверхновые. В биомедицине машинное обучение может предсказывать структуру и функции белка по генетическим последовательностям и определять оптимальные диеты [14, 18] по клиническим и микробиологическим профилям пациентов. Те же самые методы откроют огромные новые возможности в медицине. Поразительный пример: алгоритмы могут считывать кортикальную активность непосредственно из головного мозга, передавая сигналы от моторной коры парализованного человека к мышцам рук и восстанавливая моторный контроль. Эти достижения были бы невозможны без машинного обучения обработке физиологических данных в реальном времени с высоким разрешением.

Искусственный интеллект с машинным обучением имеет ряд неоспоримых преимуществ в цифровой медицине, что подтвердили ряд проведенных исследований[17]. *Во-первых*, машинное обучение значительно улучшает прогноз и предиктивную аналитику данных для получения модели процесса или физического результата. Современные прогностические мо-

[15] Цифровая медицина — ключевое направление развития // Международный форум по цифровому здравоохранению (22 апреля 2019 г., Москва). URL: https://www.sechenov.ru/ pressroom/ news/ tsifrovaya-meditsina-klyuchevoe-napravlenie-razvitiya/?sphrase_id=1137566.

[16] Obermeyer Z., M. Phil, Ezekiel J. Emanuel. Predicting the Future — Big Data, Machine Learning, and Clinical Medicine. URL: https://www.ncbi.nlm.nih.gov/.

[17] Bouton C. E., Shaikhouni A., Annetta N. V., et al. Restoring cortical control of functional movement in a human with quadriplegia // Nature. 2016; Gilbert F. J., Astley S. M., Gillan M. G. C., et al. Single reading with computer-aided detection for screening mammography // N. Engl. J. Med. 2008. Vol. 359. P. 1675–1684.

дели в медицине значительно облегчают диагностику и лечение заболеваний и их профилактику. *Во-вторых*, машинное обучение вытеснит большую часть работы рентгенологов и патологоанатомов. Эти врачи сосредоточены в основном на интерпретации оцифрованных изображений, которые могут быть легко переданы непосредственно алгоритмам. Массивные наборы данных визуализации в сочетании с последними достижениями в области компьютерного зрения приведут к быстрому повышению производительности, и точность машин скоро превысит человеческую. *В-третьих*, машинное обучение повысит точность диагностики. Алгоритмы вскоре будут генерировать дифференциальные диагнозы, предлагать высокоэффективные тесты и уменьшать чрезмерное использование тестирования.

В соответствии со ст. 34 Федерального закона № 323-ФЗ предусматривается оказание высокотехнологической медицинской помощи, включающей в себя применение новых сложных и уникальных методов лечения, а также ресурсоемких методов лечения с научно доказанной эффективностью, к которым наряду с клеточными технологиями, роботизированной техникой и *информационными технологиями* (ИТ) отнесены и методы генной инженерии. В то же время, ст. 51 Семейного кодекса РФ предусматривает применение метода искусственного оплодотворения или имплантации эмбриона для его вынашивания суррогатной матерью и, таким образом, создает сложную юридическую конструкцию суррогатного материнства и родительских прав генетических родителей, которая имеет много правовых и этических аспектов[18].

Новые элементы цифровой медицины

Цифровизация традиционной медицины привела к появлению новой области медицины — *цифровой терапии* (*digital therapeutics*), базирующейся на использовании цифровых технологий для улучшения терапии при лечении пациентов. Цифровая терапия ассоциируется в основном с онлайн-инструментами управления здоровьем и автономными медицинскими приложениями, как правило, без применения рецептурных лекарств[19].

Задачами современного здравоохранения, как отмечается в прогнозном Обзоре компании *Deloitte* 2018 года[20], становятся обеспечение качества, результативности и ценности медицинских услуг. В настоящее время участники отрасли по всему миру разрабатывают инновационные, экономически рентабельные, клиентоцентричные модели обслуживания на базе современных технологий, причем как в медицинских учреждениях, так и за их пределами на основе принципов *обеспечения высококачественного, экономчного и "умного" здравоохранения*. Происходит переориентация с объема медицинских услуг на их ценность для потребителя. Для этого проводятся программы по повышению операционной эффективности, внедрению современных технологий, управлению здоровьем населения, поощрению здорового образа жизни и контролю за социальными детерминантами здоровья. Помимо этого, организации отрасли изучают новые источники получения доходов, включая максимальное использование возможностей *интеллектуальной собственности*.

Политика и регулирование в области здравоохранения по всему миру преследуют схожие цели: обеспечение качества обслуживания и безопасности пациентов, борьба с мошенничеством и киберугрозами. Цифровые решения в области здравоохранения, призванные повысить точность диагностики заболеваний и персонализировать средства их терапии, создают сложности, связанные с *защитой данных*. В настоящее время наиболее актуальны с точки зрения управления данными и обеспечения их безопасности такие направления, как когнитивные вычисления, совместимые облачные системы электронных медицинских записей и Интернет вещей (*IoT*). В центре внимания по-прежнему находятся кибербезопасность и управление рисками, связанными с личными и медицинскими данными пациентов. Экспоненциальное развитие ряда технологий существенно меняет облик сферы здравоохранения благодаря развитию таких направлений, как синтетическая биология, 3D-печать, нанотехнологии, сопутствующая диагностика и др. В перспективе работа лечебных учреждений будет выстраиваться за счет пересмотра моделей медицинского обслуживания, внедрения цифровых технологий и искусственного интеллекта, а также комплексного развития кадровых ресурсов.

Влияние пандемии *Covid*-19 придало новый импульс в развитии законодательства цифрового здравоохранения во всем мире. Многие развитые страны, включая США, Великобританию, Италию, Германию, уже создают систему цифрового здравоохранения и медицины. Так, Германия продвигает цифровую трансформацию сектора здравоохранения под влиянием пандемии *Covid*-19 и общей необходимостью реформ. В 2019 г. принят Закон о цифровой помощи (*Digitale-Versorgung-Gesetz, DVG*)[21], а в 2020 г. опубликован Регламент приложений для здоровья (*Digitale-Gesundheitsanwendungen-Verordnung* или *DiGAV*),

[18] Федеральный закон от 29 июля 2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» // СЗ РФ. — 2017. — № 31 (Часть I). — Ст. 4791.

[19] Распоряжение Правительства РФ от 6 июня 2020 г. № 1512-р «Об утверждении Сводной стратегии развития обрабатывающей промышленности Российской Федерации до 2024 года и на период до 2035 года» // СЗ РФ. — 2020. — № 24. — Ст. 3843.

[20] ГОСТ Р 56324-2014. Национальный стандарт Российской Федерации. Изделия медицинские электрические. Аппараты рентгеновские цифровые для дентальной панорамной томографии. Технические требования для государственных закупок (утв. и введен в действие Приказом Росстандарта от 12 декабря 2014 г. № 2079-ст.).

[21] Natarajan A., Su H., Heneghan C. Assessment of physiological signs associated with COVID-19 measured using wearable devices // npj Digital Medicine (2020). URL: https://www.nature.com/ articles/s41746-020-00363-7.

который позволяет использовать соответствующие сертифицированные мобильные приложения цифрового здоровья с централизованным банком данных. Электронное и мобильное здоровье занимают приоритетное место в повестке дня. Недавно опубликованные законы упростят для врачей проведение онлайн-видео-консультаций, возместят пациентам расходы за использованием предписанных цифровых приложений для здоровья и гарантируют, что все заинтересованные стороны будут иметь доступ к безопасной сети передачи данных о здравоохранении для лечения.

Еще одним и столь необходимым шагом к цифровой трансформации сектора здравоохранения в Германии является отказ от бумажных рецептов. Медицинские услуги, вспомогательные средства или уход на дому теперь можно назначать в электронном виде. Кроме того, в Германии утверждена специальная инвестиционная программа, принятая в соответствии с Законом о будущем больниц (*Krankenhauszukunftsgesetz, KHZG*), в целях улучшения цифровой инфраструктуры больниц, особенно в том, что касается ИТ и кибербезопасности. Финансирование доступно для инвестиций в современные возможности для оказания неотложной помощи и цифровую инфраструктуру, включая порталы для пациентов, электронную документацию услуг по уходу и лечению, цифровое управление лекарствами, меры безопасности ИТ и межотраслевые телемедицинские сетевые структуры. Огромный потенциал, открываемый новыми законами, особенно актуален для поставщиков медицинских приложений, отпускаемых только по рецепту, а также телемедицинского программного обеспечения и оборудования.

Вместе с тем в основе цифровых моделей медицины, решений и функций лежат персональные (включая биометрические) данные пациентов. Такие данные должны обрабатываться с максимальной степенью соответствия действующему *информационному законодательству* о персональных данных [6, 10], которые являются одними из самых ценных активов компании и требуют надлежащей защиты и регулирования оборота.

Под эгидой Всемирной организации здравоохранения работает Международный форум регуляторов медицинского оборудования[22], который представляет собой группу регулирующих органов по медицинскому оборудованию со всего мира, которые добровольно объединились, чтобы согласовать нормативные требования к медицинской продукции, которые различаются от страны к стране. В России — это Минздрав РФ, в США — Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США и др.

В то же время применение цифровых технологий в медицине создает и новые риски и угрозы, которые проявляются в новых видах врачебных ошибок при обработке и интерпретации медицинских данных при использовании искусственного интеллекта и машинного обучения или применении телемедицинских технологий; умышленном искажении собранных данных для получения страховых выплат; неквалифицированной врачебной помощи в персональной медицине и оказании медуслуг, причинении вреда мошенническими действиями с персональными и биометрическими данными пациентов, причинении вреда в результате ошибки при оказании телемедицинских услуг или программного сбоя робототехнического умного медицинского устройства или оборудования [1, 2].

Заключение

Цифровое здравоохранение *(Digital Health)* — это термин, который охватывает сферу здравоохранения, предоставляемого или улучшаемого с помощью цифровых технологий, начиная от теледиагностики и телемедицины, онлайн-платформ и носимых медицинских устройств до мобильного программного обеспечения и приложений, машинного обучения и искусственного интеллекта, которые предназначены для оказания медицинской помощи и услуг в системе здравоохранения и социального обеспечения. Цифровые технологии здравоохранения *(digital health technologies)* готовы к использованию автономно или в сочетании с традиционными медицинскими продуктами и услугами, такими как медицинские приборы или диагностические тесты.

Цифровая медицина *(digital medicine)* в современном понимании представляет собой область здравоохранения, традиционной медицины, которая связана с использованием передовых технологий и технических решений в качестве инструментов осуществления медицинской деятельности и оказания услуг в сфере здравоохранения и социальной помощи. Применение современных цифровых медицинских средств определяется использованием высокотехнологичного оборудования и программного обеспечения, искусственного интеллекта, современных методов тестирования и диагностики, терапии и лечения, которые направлены на расширение возможностей медицины, включая лечение, восстановление, профилактику заболеваний и укрепление здоровья отдельных пациентов и различных групп населения. Цифровая медицина охватывает устройства и приложения, помогающие вести постоянный мониторинг показателей жизнедеятельности организма человека и в целом подразумевает использование информационных и коммуникационных технологий с целью решения проблем со здоровьем пациентов, включая аппаратные технологии *Digital health* и программные решения и услуги.

Цифровые медицинские продукты могут использоваться независимо или совместно с фармацевтическими препаратами, биологическими препаратами, устройствами или другим медицинским оборудованием и материалами для оптимизации ухода за пациен-

[22] Obermeyer Z., M. Phil, Ezekiel J. Emanuel. Predicting the Future — Big Data, Machine Learning, and Clinical Medicine. URL: https://www.ncbi.nlm.nih.gov/.

тами и улучшения их здоровья. Цифровая медицина предоставляет пациентам и поставщикам медицинских услуг современные интеллектуальные и доступные инструменты для решения широкого спектра проблем с помощью высококачественных, безопасных и эффективных измерений и основанных на данных медицинских манипуляций и вмешательств. Как дисциплина, цифровая медицина включает в себя широкий профессиональный опыт и профессиональную ответственность в отношении использования цифровых инструментов. Цифровая медицина нацелена на широкое применение цифровых технологий.

Как показывает практика расширяющегося применения цифровых технологий в здравоохранении и медицине, процесс цифровизации этой области деятельности требует разработки нового массива законодательства, в первую очередь информационно-правового (на основе новой теории информационного права [6, 7]), создания специальной системы стандартов и специального программного обеспечения, а также установления особого порядка обработки и использования фактических медицинских и биометрических данных для их реализации в цифровых медицинских технологиях.

Литература

1. Базина О. О., Сименюра С. С. Телемедицина: достоинства, недостатки, реалии (правовой анализ и практическое применение) // Медицинское право. 2020. № 3. С. 32–38.
2. Грачева Ю. В., Коробеев А. И., Маликов С. В., Чучаев А. И. Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения // Lex russica. 2020. № 1. С. 145–159.
3. Карцхия А. А. Новые элементы национальной безопасности: национальный и международный аспект // Вопросы кибербезопасности. 2020. № 6(40). С.72 — 82. DOI: 10.21681/2311-3456-2020-06-72-82.
4. Карцхия А. А. Правовое регулирование и возможности современных биотехнологий // ИС. Промышленная собственность. 2020. № 8. С. 33–46.
5. Карпов О. Э., Субботин С. А., Шишканов Д. В., Замятин М. Н. Цифровое здравоохранение. Необходимость и предпосылки // Врач и информационные технологии. 2017. № 3. С. 6–22.
6. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере: Монография. М.: РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
7. Ловцов Д. А. Теория информационного права: базисные аспекты // Государство и право. 2011. — № 11. — С. 43–51.
8. Ловцов Д. А. Информационная безопасность автоматизированных блокчейн-систем: угрозы и способы повышения // Тр. II Междунар. науч.-прак. конф. «Трансформация национальной социально-экономической системы России» (22 ноября 2019 г.) / РГУП. Москва: РГУП, 2020. С. 464–473. ISBN 978-5-93916-823-6.
9. 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. DOI: 10.21681/1994-1404-2017-1-28-36.
10. Ловцов Д. А., Федичев А. В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. № 2. С. 35–54. DOI: 10.21681/1994-1404-2017-2-35-54.
11. Морозова Ю. А. Цифровизация как глобальный, страновой и отраслевой процесс в повышении результативности и эффективности здравоохранения и медицины // Интеллект. Инновации. Инвестиции. 2019. № 4. С. 44–53.
12. Муслимов М. И. Цифровое здравоохранение как фактор революционных преобразований в отрасли // Современные проблемы здравоохранения и медицинской статистики. 2018. № 3. С. 63–74.
13. Право граждан на лекарственное обеспечение : монография / Н. В. Путило, Н. С. Волкова и др. М.: ИЗиСП, «Контракт», 2017. 340 с.
14. Скворцова М. А., Вишневская Ю. А., Писарев А. В. Проектирование экспертных информационных систем в медицине: правовые и функциональные аспекты // Правовая информатика. 2020. № 2. С. 71–81. DOI: 10.21681/1994-1404-2020-2-71-81.
15. Федосеев С. В. Применение современных технологий больших данных в правовой сфере // Правовая информатика. 2018. № 4. С. 50–58. DOI: 10.21681/1994-1404-2018-4-50-58.
16. Черных А. М. Основные направления интеграции федеральных государственных информационных систем и пространственных данных // Правовая информатика. 2018. № 2. С. 47–56. DOI: 10.21681/1994-1404-2018-2-47-56.
17. Emmert-Streib F., Dehmer M. A. Machine learning perspective on Personalized Medicine: an automized, comprehensive knowledge base with ontology for pattern recognition // Machine Learning and Knowledge Extraction. 2019. T. 1. No 1. P. 149–156.
18. Meshalkin V. P., Ivashkin Y. A., Nikitina M. A. Computer multi-agent model of chemico-physiological processes in the human gastrointestinal tract as a living biochemical system // Doklady Akademii nauk. 2019. T. 484. — No 3. P. 303—306.

19. Vishnevskaya J. A., Baykov Y. D., Skvortsova M. Study the Possibility of Creating Self-Diagnosis and First Aid System // 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2019. P. 1897–1901.
20. Topol E. J. High-performance medicine: the convergence of human and artificial intelligence // Nature Medicine. 2019. No 25. P. 44–56. DOI: org/10.1038/s41591-018-0300-7.

Рецензенты: ***Азаров Павел Викторович,*** *кандидат медицинских наук, заведующий отделением ГКБ №52, Москва, Россия.*
E-mail: azarovp@mail.ru

Захарцев Сергей Иванович, *доктор юридических наук, профессор, академик РАРАН, заведующий кафедрой Российского государственного социального университета, Россия, Москва.*
E-mail: sergeyivz@ya.ru

LEGAL INFORMATION SUPPORT FOR A DIGITAL HEALTH ECOSYSTEM

Alexandr Kartskhiya, *Dr.Sc. (Law), Associate Professor, Professor of the Department of Civil Law Disciplines, Gubkin Russian State University of Oil and Gas (National University), Moscow, Russia.*
E-mail: *arhz50@mail.ru*

Keywords: *biometric data, healthcare law, information technology, artificial intelligence, digital medicine, telemedicine, digital healthcare.*

Abstract.
The purpose of the study is to determine the features of information technologies usage of a legal regulation of digital healthcare, as well as to determine the basic conceptual apparatus and structure of modern legal mechanism of a digital healthcare ecosystem.
Research method: comparative legal analysis of the current national Russian and foreign legislation, strategic documents and international treaties and agreements on digital health and medicine, taking into account the structural and value assessment of information technologies usage in digital medicine.
Result: the study revealed some features of initial formation stage of digital health special legislation and digital medicine, that enable to come to the finding of the exceptional importance of a new direction in medicine and the prospects of digital health in modern conditions, that will require a special legislation drafting of digital healthcare.

References

1. Bazina O. O., Simeniura S. S. Telemeditcina: dostoinstva, nedostatki, realii (pravovoi` analiz i prakticheskoe primenenie) // Meditcinskoe pravo. 2020. № 3. S. 32-38.
2. Gracheva Iu. V., Korobeev A. I., Malikov S. V., Chuchaev A. I. Ugolovno-pravovy`e riski v sfere tcifrovy`kh tekhnologii`: problemy` i predlozheniia // Lex russica. 2020. № 1. S. 145-159.
3. Kartchiia A. A. Novy`e e`lementy` natcional`noi` bezopasnosti: natcional`ny`i` i mezhdunarodny`i` aspekt // Voprosy` kiberbezopasnosti. 2020. № 6(40). S.72-82. DOI: 10.21681/2311-3456-2020-06-72-82.
4. Kartchiia A. A. Pravovoe regulirovanie i vozmozhnosti sovremenny`kh biotekhnologii` // IS. Promy`shlennaia sobstvennost`. 2020. № 8. S. 33-46.
5. Karpov O. E.`., Subbotin S. A., Shishkanov D. V., Zamiatin M. N. Tcifrovoe zdravookhranenie. Neobhodimost` i predposy`lki // Vrach i informatcionny`e tekhnologii. 2017. № 3. S. 6-22.
6. Lovtcov D. A. Sistemologiia pravovogo regulirovaniia informatcionny`kh otnoshenii` v infosfere : monografiia. M.: RGUP, 2016. 316 s. ISBN 978-5-93916-505-1.
7. Lovtcov D. A. Teoriia informatcionnogo prava: bazisny`e aspekty` // Gosudarstvo i pravo. 2011. — № 11. — S. 43-51.
8. Lovtcov D. A. Informatcionnaia bezopasnost` avtomatizirovanny`kh blokchei`n-sistem: ugrozy` i sposoby` povy`sheniia // Tr. II Mezhdunar. nauch.-prak. konf. «Transformatciia natcional`noi` sotcial`no-e`konomicheskoi` sistemy` Rossii» (22 noiabria 2019 g.) / RGUP. Moskva: RGUP, 2020. S. 464-473. ISBN 978-5-93916-823-6.

9. Lovtcov D. A., Bogdanova M. V., Parshintceva L. S. Pakety` pricladny`kh programm dlia mnogoaspektnogo analiza sudebnoi` statisticheskoi` informatcii // Pravovaia informatika. 2017. № 1. S. 28-36. DOI: 10.21681/1994-1404-2017-1-28-36.
10. Lovtcov D. A., Fedichev A. V. Arhitektura natcional`nogo classifikatora pravovy`kh rezhimov informatcii ogranichennogo dostupa // Pravovaia informatika. 2017. № 2. S. 35-54. DOI: 10.21681/1994-1404-2017-2-35-54.
11. Morozova Iu. A. Tcifrovizatciia kak global`ny`i`, stranovoi` i otraslevoi` protcess v povy`shenii rezul`tativnosti i e`ffektivnosti zdravookhraneniia i meditciny` // Intellekt. Innovatcii. Investitcii. 2019. № 4. S. 44-53.
12. Muslimov M. I. Tcifrovoe zdravookhranenie kak faktor revoliutcionny`kh preobrazovanii` v otrasli // Sovremenny`e problemy` zdravookhraneniia i meditcinskoi` statistiki. 2018. № 3. S. 63-74.
13. Pravo grazhdan na lekarstvennoe obespechenie : monografiia / N. V. Putilo, N. S. Volkova i dr. M.: IZiSP, «Kontrakt», 2017. 340 s.
14. Skvortcova M. A., Vishnevskaia Iu. A., Pisarev A. V. Proektirovanie e`kspertny`kh informatcionny`kh sistem v meditcine: pravovy`e i funktcional`ny`e aspekty` // Pravovaia informatika. 2020. № 2. S. 71-81. DOI: 10.21681/1994-1404-2020-2-71-81.
15. Fedoseev S. V. Primenenie sovremenny`kh tekhnologii` bol`shikh danny`kh v pravovoi` sfere // Pravovaia informatika. 2018. № 4. S. 50-58. DOI: 10.21681/1994-1404-2018-4-50-58.
16. Cherny`kh A. M. Osnovny`e napravleniia integratcii federal`ny`kh gosudarstvenny`kh informatcionny`kh sistem i prostranstvenny`kh danny`kh // Pravovaia informatika. 2018. № 2. S. 47-56. DOI: 10.21681/1994-1404-2018-2-47-56.
17. Emmert-Streib F., Dehmer M. A. Machine learning perspective on Personalized Medicine: an automized, comprehensive knowledge base with ontology for pattern recognition // Machine Learning and Knowledge Extraction. 2019. T. 1. No 1. P. 149–156.
18. Meshalkin V. P., Ivashkin Y. A., Nikitina M. A. Computer multi-agent model of chemico-physiological processes in the human gastrointestinal tract as a living biochemical system // Doklady Akademii nauk. 2019. T. 484. — No 3. P. 303–306.
19. Vishnevskaya J. A., Baykov Y. D., Skvortsova M. Study the Possibility of Creating Self-Diagnosis and First Aid System // 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2019. P. 1897–1901.
20. Topol E. J. High-performance medicine: the convergence of human and artificial intelligence // Nature Medicine. 2019. No 25. P. 44–56. DOI: 10.1038/s41591-018-0300-7.

ЭФФЕКТИВНОСТЬ ИНФОРМАЦИОННОГО ОБМЕНА В МУЛЬТИСЕРВИСНОЙ РАДИОСЕТИ С ВЫДЕЛЕНИЕМ КАНАЛОВ ПО ТРЕБОВАНИЮ

Шиманов С. Н., Крикунов А. А.*

***Ключевые слова**: мультисервисная радиосеть, сеть радиосвязи, многопотоковая модель, предоставление каналов по требованию, неоднородный трафик, двухфазное обслуживание трафика, случайный множественный доступ, транкинговая система связи, нестационарная абонентская нагрузка, динамическое распределение канального ресурса, оперативность информационного обмена.*

Аннотация.

Цель работы: совершенствование научно-методического аппарата для оценки и оптимизации характеристик мультисервисных сетей радиосвязи в условиях динамики абонентского трафика и доступного канального ресурса.

Методы: методы теории телетрафика, методы аналитического и имитационного моделирования, теории вероятностей и теории марковских процессов.

Результаты: разработана комплексная математическая модель обслуживания абонентского трафика в мультисервисной радиосети с предоставлением каналов по требованию в условиях конечного числа абонентов и малого канального ресурса; полученная модель позволяет учесть взаимную зависимость длительностей различных фаз обслуживания: этапа отправки запроса по каналу случайного доступа в адрес главной станции и этапа непосредственной передачи пользовательского трафика согласно принятому алгоритму обслуживания; показано, что существует оптимальное распределение канального ресурса между служебными и рабочими каналами, которое зависит от текущей нагрузки и доступной канальной емкости сети радиосвязи.

DOI::10.21681/1994-1404-1-24-35

Введение

Современные сети радиосвязи в составе крупномасштабных автоматизированных систем типа ГАС РФ «Правосудие» [1, 9] являются, как правило, мультисервисными, т. е. ориентированы на интегральное обслуживание различных видов абонентского трафика с использованием единого *канального ресурса* (КР) [2, 3]. Как следствие, на этапе проектирования таких радиосетей возникает необходимость эффективно решать *задачу распределения* информационного ресурса сети связи между ее абонентами в условиях совместного обслуживания сервисов (трафика) реального времени (ТРВ) и трафика данных (ТД), допускающего некоторую задержку при передаче. В условиях ограниченного КР сети радиосвязи его распределение между абонентами чаще всего организуется на основе процедуры предоставления каналов по требованию (ПКТ). Такой подход в настоящее время успешно применяется в подсистемах спутниковой связи, а также в мобильной сотовой связи, транкинговых системах связи и позволяет обеспечить обслуживание абонентского трафика с приемлемым качеством [5, 11, 15, 16].

Как правило, в таких системах общий КР жестко разделен между *служебными каналами* (СК), которые предназначены для организации процедуры обслуживания абонентов, и рабочими каналами, предназначенными непосредственно для передачи абонентского трафика. Общее время обслуживания трафика для систем ПКТ складывается из двух составляющих: времени передачи требования на предоставление КР по СК и времени обработки требования, принятого на обслуживание

* ***Шиманов Сергей Николаевич,*** *доктор технических наук, профессор, профессор кафедры «Автоматизированных систем боевого управления» филиала Военной академии РВСН имени Петра Великого, Московская область, г. Серпухов, Российская Федерация.*

E-mail: 41kaf_rabota@mail.ru

Крикунов Алексей Александрович, *кандидат технических наук, докторант филиала Военной академии РВСН имени Петра Великого, Московская область, г. Серпухов, Российская Федерация.*

E-mail: 41kaf_rabota@mail.ru

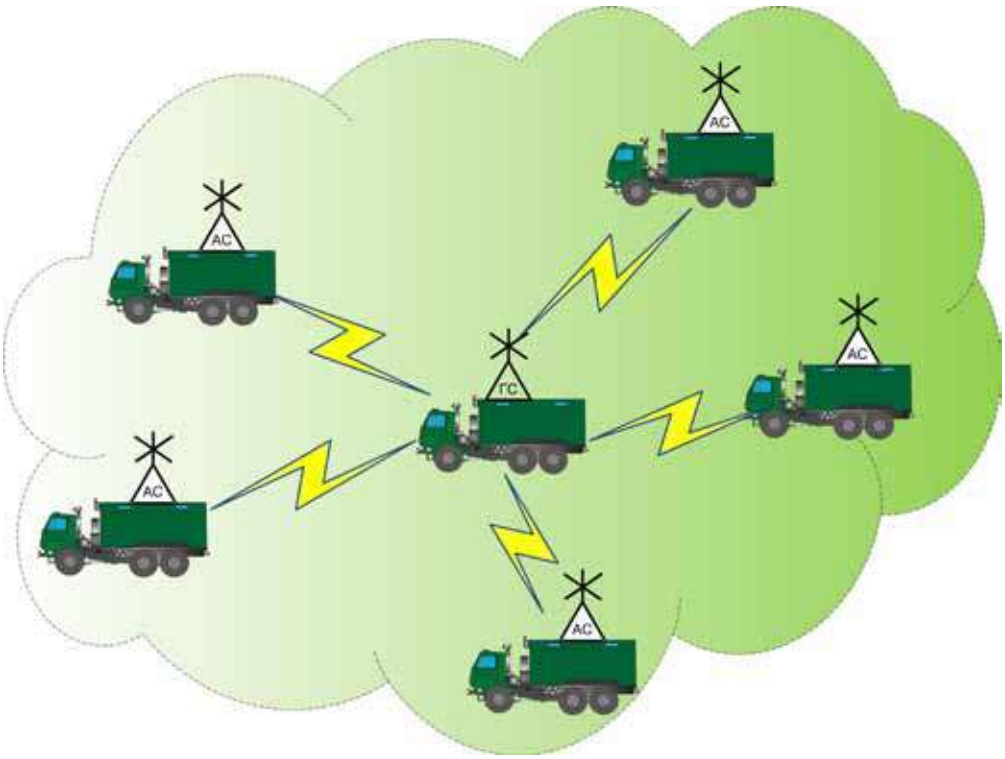


Рис. 1. Структура сети радиосвязи с предоставлением каналов по требованию

(ожидание в очереди плюс непосредственная передача трафика). Как известно, применение *динамического* способа распределения КР позволяет значительно повысить эффективность его использования [2, 11, 13], в то же время требуется решить ряд дополнительных проблем на этапе проектирования и эксплуатации таких радиосетей. В условиях малого количества каналов, доступных для распределения, и относительно небольшого числа абонентов возникает достаточно сильная корреляция между характеристиками качества обеих фаз обслуживания трафика. Велика вероятность простаивания СК при перегрузке рабочих каналов (абоненты находятся на обслуживании или в очереди, ожидая начала обслуживания, и не генерируют вызывной трафик) либо обратная ситуация с простаиванием рабочих каналов в условиях блокировки СК [7]. Таким образом, особенно остро стоит *задача обеспечения эффективности* использования каждой единицы КР. Кроме того, абонентский трафик, как правило, не является стационарным, а объем доступного КР радиосети может изменяться в зависимости от условий прохождения радиосигналов. С учетом этих особенностей, для поддержания нормального режима функционирования радиосети с ПКТ в условиях динамики трафика и доступного КР необходимо соответствующим образом перераспределять КР между служебными и рабочими каналами в зависимости от текущего состояния сети радиосвязи. Для решения этой задачи требуется прежде всего разработать математический аппарат, позволяющий оценить необходимые показатели эффективности и качества информационного обмена.

Математическое моделирование радиосети с предоставлением каналов по требованию

Рассмотрим радиосеть (рис. 1), в которой выделение КР осуществляется централизовано главной станцией (ГС) по запросам абонентских станций (АС) с использованием служебного канала. В информационном потоке можно выделить трафик реального времени, требующий фиксированной скорости передачи (телефонная связь) и трафик передачи данных (файловый обмен), допускающий задержку. Трафик реального времени имеет преимущество в занятии и использовании КР [10, 14].

Для такой системы с динамическим резервированием оперативность обслуживания абонентов характеризуется среднем временем $\overline{T}_{обсл.общ.}$ обслуживания заявки на выделение КР, которое складывается из среднего времени $\overline{T}_{СК}$ задержки в СК и среднего времени $\overline{T}_{обр}$ обработки заявки, принятой на обслуживание. Соответственно, общий КР системы разделен на две части:

первая – ресурс, необходимый для функционирования СК;

вторая – КР, динамически выделяемый по требованию на обслуживание абонентского трафика.

Очевидно, что *оперативность* обслуживания в каждой отдельной составляющей системы будет повышаться с увеличением соответствующего объема КР. Следовательно, с учетом ограниченности КР возникает задача оптимального его разделения с целью минимизации общего времени обслуживания заявки:

$$\overline{T}_{обсл.общ} = \overline{T}_{СК} + \overline{T}_{обр}. \quad (1)$$

Для решения этой задачи необходимо рассмотреть и проанализировать две подсистемы: служебный канал и непосредственно систему динамического выделения КР (подсистему распределения рабочих каналов (ПРРК)) по требованию.

Для построения математической модели второй подсистемы примем следующие *исходные данные*. В системе имеется два различных потока заявок на обслуживание, соответствующих различным видам трафика (ТРВ и ТД) и образованных конечным числом абонентов N_1 и N_2 соответственно. Поступление заявок этих потоков в СК происходит через интервалы времени, имеющие показательное распределение с соответствующими параметрами λ_1 и λ_2, которые зависят от состояния сети. Пусть $V_{об}$ — скорость передачи информации мультисервисной линии, выраженная в единицах канального ресурса (к.е.); M — число к.е., выделенное для работы СК; $V = V_{îá} - M$ — объем КР, предназначенный для непосредственного обслуживания принятых заявок; b_1 — число единиц канального ресурса, необходимого для обслуживания одной заявки первого потока (трафика реального времени), причем $b_1 > 1$; $\tau_1 = \frac{1}{\mu_1}$ — среднее время для обслуживания этой заявки (длительность обслуживания также распределена экспоненциально) [8, 13].

Если для обслуживания поступившей заявки нет необходимого канального ресурса, заявка становится в очередь. Соответственно, $l_1 \le N_1$, $l_2 \le N_2$ — длина очереди для заявок каждого потока; $i_1 \le N_1$, $i_2 \le N_2$ — количество заявок, находящихся на обслуживании.

Преимущества трафика реального времени (ТРВ) над трафиком в занятии и использовании канального ресурса заключаются:

– в снижении скорости передачи данных с ростом нагрузки на сеть;

– в первоочередном обслуживании заявок первого потока, находящихся в очереди.

Второй пункт означает, что освободившийся канальный ресурс при условии его достаточности будет выделен находящейся в очереди заявке на передачу трафика реального времени, независимо от относительного времени поступления требований двух потоков.

Положим, что заявки на передачу трафика реального времени являются «нетерпеливыми», т.е. покидают очередь, если время ожидания начала обслуживания превысит некоторое заданное. Будем предполагать, что каждая поступившая заявка первого потока может ожидать начала обслуживания не более случайного времени, распределенного по показательному закону с параметром σ.

Механизм динамически изменяемой скорости передачи реализуется путем выделения соответствующему трафику так называемого *макроканала*, пропускная способность которого изменяется в зависимости от текущей загрузки канального ресурса (например, в соответствии с алгоритмом двоичного изменения пропускной способности [13, 14]). Будем считать минимальную скорость макроканала $g_0 = 1$ к.е., $g = \overline{1,2...V}$. Время обслуживания одной заявки второго потока распределено по показательному закону и при минимальной пропускной способности $\tau_{02} = \frac{1}{\mu_{02}}$. Следовательно, $\mu_2 = g \cdot \mu_{02}$. Обозначим $w = i_1 b_1$ — число канальных единиц, занятых обслуживанием трафика реального времени; $f = V - w$ – оставшийся канальный ресурс. В общем случае средняя интенсивность $\mu_2 = \mu_2(f, i_2)$ обслуживания для потока заявок однозначно определяется для каждого состояния сети.

Состояние модели задается вектором (i_1, l_1, i_2, l_2), совокупность таких векторов образует пространство состояний модели S. Вероятности $P(i_1, l_1, i_2, l_2)$ интерпретируются как доля времени пребывания системы в соответствующих состояниях.

Динамика изменения состояний системы описывается случайным процессом $r(t) = (i_1(t), l_1(t), i_2(t), l_2(t))$, определенном на конечном пространстве состояний S; $U_1 \subset S$ – множество состояний, в которых заявка первого потока встает в очередь на обслуживание $(w + i_2 + b_1 > V)$. Аналогично $U_2 \subset S, (w + i_2 + 1 > V)$.

Если поступление заявок от каждого абонента подчиняется закону Пуассона с интенсивностью γ_1, γ_2 для соответствующего потока, то суммарные интенсивности потоков на входе СК:

$$\begin{aligned} \lambda_1(i_1, l_1) &= N_{a1} \cdot \gamma_1 = (N_1 - i_1 - l_1)\gamma_1, \Rightarrow (i_1 + l_1) \le N_1 \\ \lambda_2(i_2, l_2) &= N_{a2} \cdot \gamma_2 = (N_2 - i_2 - l_2)\gamma_1, \Rightarrow (i_2 + l_2) \le N_2 \end{aligned}, \quad (2)$$

где N_{a1}, N_{a2} — количество активных абонентов, создающих в текущем состоянии соответствующий поток заявок в СК;

$$N_{a1} = (N_1 - i_1 - l_1), \quad N_{a2} = (N_2 - i_2 - l_2). \quad (3)$$

Так как заявки на обслуживание попадают в систему через СК, интенсивности соответствующих потоков на входе модели будут отличаться от приведенных в выражениях (2, 3). Для их расчета зададим следующие параметры.

Пусть СК функционирует на основе синхронного протокола случайного множественного доступа (СМД) [2, 12, 16]. В настоящее время известно и хорошо исследовано множество таких протоколов, они получили широкое распространение и обладают лучшими характеристиками по сравнению с асинхронными. Для поддержания высокой эффективности использования канала при изменении интенсивности входного потока, в СК реализована процедура оптимального параметрического управления. Тогда относительная пропускная способность, равная средней скорости передачи по каналу, будет постоянной и максимальной для данного протокола при достаточной первичной нагрузке [6, 16, 17]. Для СК, под который выделена 1 к.е., $C = C_{оптимальное} = C_0$. Соответственно, если под СК выделено M единиц канального ресурса, $C = M \cdot C_0$.

Пусть C_1, C_2 — пропускные способности канала по соответствующему потоку. Независимо от конкретного протокола, несложно показать, что

$$C = M \cdot C_0 = C_1 + C_2 \cdot \quad (4)$$

Приняв длительность цикла передачи (временного такта) равной единице без потери общности результатов и переходя к первичной активности абонентов [5, 16], выраженной через вероятность генерации заявки в очередном кадре, получим:

$$p_1 = 1 - e^{-y_1}, p_2 = 1 - e^{-y_2}. \quad (5)$$

Основным *недостатком* существующих математических моделей протоколов СМД в условиях ограниченного множества абонентов является их резкое усложнение и увеличение вычислительных ресурсов, необходимых для расчетов, при возрастании числа входных потоков и количества абонентов, создающих эти потоки [4, 14]. Следовательно, невозможно напрямую использовать такие математические модели как составную часть *комплексной модели* исследуемой системы. В рамках решаемой задачи достаточно с допустимой погрешностью определить пропускную способность и время задержки передачи требования в СК для каждого потока.

Проведенные для различных протоколов СМД исследования показывают, что для выбранной модели входного потока при условии поддержания канала в оптимальном режиме с высокой точностью (погрешность не более 5%) выполняется соотношение:

$$\frac{C_1}{C_2} = \frac{p_1 \cdot N_{a1}}{p_2 \cdot N_{a2}}. \quad (6)$$

Будем полагать, что при падении первичной нагрузки в служебном канале ниже оптимального (максимального) значения пропускной способности, время задержки будет составлять приблизительно один такт (непосредственно на передачу), а пропускная способность СК будет примерно равна первичной нагрузке в нем. Тогда с учетом (4–6) получим:

$$\left.\begin{aligned} C_1 &= M \cdot C_0 \cdot \frac{p_1 \cdot N_{a1}}{p_1 \cdot N_{a1} + p_2 \cdot N_{a2}} \\ C_2 &= M \cdot C_0 \cdot \frac{p_2 \cdot N_{a2}}{p_1 \cdot N_{a1} + p_2 \cdot N_{a2}} \end{aligned}\right\}, \quad (7)$$

$$при \quad p_1 \cdot N_{a1} + p_2 \cdot N_{a2} > M \cdot C_0$$

$$C_1 = p_1 \cdot N_{a1}, \quad C_2 = p_2 \cdot N_{a2},$$

$$при \quad p_1 \cdot N_{a1} + p_2 \cdot N_{a2} \le M \cdot C_0$$

Значения C_1 и C_2 можно рассматривать как интенсивности входных потоков для рассматриваемой математической модели [7, 14]:

$$\lambda_{t1} = C_1, \quad \lambda_{t2} = C_2$$

Используя известные соотношения из [4, 6] с учетом (7), получим следующие выражения для времени задержки (передачи) в СК:

$$\left.\begin{aligned} T_{1CK} &= \frac{p_1 \cdot N_{a1} + p_2 \cdot N_{a2} - M \cdot C_0}{p_1 \cdot M \cdot C_0} + 1 \\ T_{2CK} &= \frac{p_1 \cdot N_{a1} + p_2 \cdot N_{a2} - M \cdot C_0}{p_2 \cdot M \cdot C_0} + 1 \end{aligned}\right\}, \quad (8)$$

$$при \quad p_1 \cdot N_{a1} + p_2 \cdot N_{a2} > M \cdot C_0$$

$$T_{1CK} = T_{2CK} = T_{CK} = 1, \quad при \quad p_1 \cdot N_{a1} + p_2 \cdot N_{a2} \le M \cdot C_0$$

Среднее время передачи требования на предоставление КР по СК находится как математическое ожидание по всем состояниям системы:

$$\left.\begin{aligned} \overline{T}_{1CK} &= \sum_{(i_1(t),l_1(t),i_2(t),l_2(t))\in S} p(i_1(t),l_1(t),i_2(t),l_2(t)) \cdot T_{1CK} \\ \overline{T}_{2CK} &= \sum_{(i_1(t),l_1(t),i_2(t),l_2(t))\in S} p(i_1(t),l_1(t),i_2(t),l_2(t)) \cdot T_{2CK} \end{aligned}\right. \quad (9)$$

Качество обслуживания трафика реального времени оценивается по следующим показателям [8, 10, 13, 14]:

– среднее число заявок первого потока, находящихся на обслуживании

$$I_1 = \sum_{(i_1(t),l_1(t),i_2(t),l_2(t))\in S} p(i_1(t),l_1(t),i_2(t),l_2(t)) \cdot i_1; \quad (10)$$

– средний объем канального ресурса, занятый обслуживанием заявок первого потока

$$m_1 = I_1 \cdot b_1; \quad (11)$$

– средняя длина очереди

$$L_1 = \sum_{(i_1(t),l_1(t),i_2(t),l_2(t))\in S} p(i_1(t),l_1(t),i_2(t),l_2(t)) \cdot l_1; \quad (12)$$

– среднее время обработки (нахождения в системе) заявки первого потока (определяется по формуле Литтла)

$$\overline{T}_{1îáð} = \frac{I_1 + L_1}{\overline{\lambda}_{t1}}; \quad (13)$$

где $\overline{\lambda}_{t1}$ — средняя интенсивность заявок первого потока,

$$\overline{\lambda_{t1}} = \sum_{(i_1(t),l_1(t),i_2(t),l_2(t))\in S} p(i_1(t),l_1(t),i_2(t),l_2(t)) \cdot \lambda_{t1}; \quad (14)$$

– доля заявок первого потока, потерянная вследствие неудачного завершения времени ожидания,

$$\pi_\sigma = \frac{\sigma}{\overline{\lambda}_{t1}} \cdot \sum_{(i_1(t),l_1(t),i_2(t),l_2(t))\in S} p(i_1(t),l_1(t),i_2(t)) \cdot \quad (15)$$

Для трафика данных, помимо показателей (10–13) дополнительно введем b_2 — среднее число к. е., занятых обслуживанием заявок второго потока,

$$\overline{b_2} = \frac{\sum_{(i_1(t),l_1(t),i_2(t),l_2(t))\in S} p(i_1(t),l_1(t),i_2(t),l_2(t)) \cdot \mu_2(i_2, f)}{I_2 \cdot \mu_{02}} \quad (16)$$

Объединив выражения (10–14, 8, 9), получим:

$$\overline{T}_{1\text{îáð}} = \frac{\sum\limits_{(i_1,l_1,i_2,l_2)\in S} P(i_1,l_1,i_2,l_2)\cdot i_1 + \sum\limits_{(i_1,l_1,i_2,l_2)\in S} P(i_1,l_1,i_2,l_2)\cdot l_1}{\sum\limits_{(i_1,l_1,i_2,l_2)\in S} P(i_1,l_1,i_2,l_2)\cdot\left(\frac{M\cdot C_0}{t_c}\cdot\frac{p_1\cdot(N_1-i_1-l_1)}{p_1\cdot(N_1-i_1-l_1)+p_2\cdot(N_2-i_2-l_2)}\right)}$$

$$\overline{T}_{2\text{îáð}} = \frac{\sum\limits_{(i_1,l_1,i_2,l_2)\in S} P(i_1,l_1,i_2,l_2)\cdot i_2 + \sum\limits_{(i_1,l_1,i_2,l_2)\in S} P(i_1,l_1,i_2,l_2)\cdot l_2}{\sum\limits_{(i_1,l_1,i_2,l_2)\in S} P(i_1,l_1,i_2,l_2)\cdot\left(\frac{M\cdot C_0}{t_c}\cdot\frac{p_2\cdot(N_2-i_2-l_2)}{p_1\cdot(N_1-i_1-l_1)+p_2\cdot(N_2-i_2-l_2)}\right)} \qquad (17)$$

Система уравнений равновесия

Для расчета введенных показателей эффективности и качества необходимо составить и решить систему уравнений равновесия. Существование *стационарного* режима обеспечивается заданными ограничениями. В рассматриваемой модели из состояния (i_1,l_1,i_2,l_2) возможны следующие переходы $r(t)$:

Из состояния (i_1,l_1,i_2,l_2) (рис. 2):

В состояние $(i_1-1,l_1,i_2,l_2) \xleftarrow[(l_1=0,l_2=0)]{\mu_1\cdot i_1}$ переход осуществляется по завершении обслуживания заявки ТРВ при отсутствии в очереди заявок других потоков.

В состояние $(i_1,l_1-1,i_2,l_2) \xleftarrow[(l_1\neq 0)]{(\mu_1\cdot i_1+\sigma\cdot l_1)}$ переход осуществляется или при успешном завершении обслуживания заявки ТРВ (при этом на ее место встает очередная заявка из очереди ТРВ), или при отказе от обслуживания заявки соответствующего потока, находящейся в очереди, вследствие превышения интервала ожидания.

В состояние $(i_1,l_1+1,i_2,l_2) \xleftarrow[(w+i_2+b_1>V)]{\lambda_{t1}(i_1,l_1)}$ переход осуществляется при поступлении очередной заявки ТРВ и отсутствии достаточного свободного КР для ее обслуживания.

В состояние $(i_1+1,l_1,i_2,l_2) \xleftarrow[(w+i_2+b_1\leq V)]{\lambda_{t1}(i_1,l_1)}$ переход осуществляется при поступлении очередной заявки ТРВ и наличии достаточного свободного КР для ее обслуживания.

В состояние $(i_1,l_1,i_2+1,l_2) \xleftarrow[(w+i_2+1\leq V)]{\lambda_{t2}(i_2,l_2)}$ переход осуществляется при поступлении очередной заявки ТД и наличии достаточного свободного КР для ее обслуживания.

В состояние $(i_1,l_1,i_2,l_2+1) \xleftarrow[(w+i_2+1>V)]{\lambda_{t2}(i_2,l_2)}$ переход осуществляется при поступлении очередной заявки ТД и отсутствии достаточного свободного КР для ее обслуживания.

В состояние $(i_1,l_1,i_2-1,l_2) \xleftarrow[((l_1=0)or(w+i_2+b_1-1>V),l_2=0)]{\mu_2(i_2,f)}$ переход осуществляется при завершении обслуживания заявки ТД и пустой очереди соответствующего потока, при этом очередь заявок ТРВ тоже нулевая либо свободного КР недостаточно, чтобы начать обслуживание очередной заявки первого потока.

В состояние $(i_1,l_1,i_2,l_2-1) \xleftarrow[(l_2\neq 0),(w+i_2+b_1-1>V)or(l_1=0)]{\mu_2(i_2,f)}$ переход осуществляется при завершении обслуживания заявки ТД (при этом на ее место встает новая из очереди ТД), при условии, что освободившийся КР не может быть выделен очередной заявке ТРВ.

В состояние $(i_1+1,l_1-1,i_2-1,l_2) \xleftarrow[(w+i_2+b_1-1=V,l_1\neq 0)]{\mu_2(i_2,f)}$ переход осуществляется при завершении при завершении обслуживания заявки ТД и принятии на обслуживание очередной заявки ТРВ, имеющей приоритет, при условии достаточности КР.

В состояние $(i_1-1,l_1,i_2+a,l_2-a) \xleftarrow[a=\min(b_1,l_2)]{\mu_1\cdot i_1}$ $(l_1=0,l_2\neq 0)$ переход осуществляется при завершении обслуживания заявки ТРВ и пустой очереди соответствующего потока, при этом в зависимости от длины очереди ТД на обслуживание будет принято от 1 до b_1 заявок второго потока.

В состояние (i_1,l_1,i_2,l_2) (рис. 3):

Из состояния $(i_1-1,l_1,i_2,l_2) \xrightarrow[(w+i_2+b_1\leq V)]{\lambda_{t1}(i_1-1,l_1)}$ переход осуществляется при поступлении очередной заявки ТРВ и наличии достаточного свободного КР для ее обслуживания.

Из состояния $(i_1,l_1-1,i_2,l_2) \xrightarrow[(w+i_2+b_1>V)]{\lambda_{t1}(i_1-1,l_1)}$ переход осуществляется при поступлении очередной заявки ТРВ и отсутствии достаточного свободного КР для ее обслуживания.

Из состояния $(i_1,l_1+1,i_2,l_2) \xrightarrow[(l_1\neq 0)]{(\mu_1\cdot i_1+\sigma\cdot(l_1+1))}$ переход осуществляется или при успешном завершении обслуживания заявки ТРВ (при этом на ее место встает очередная заявка из очереди ТРВ), или при отказе от обслуживания заявки соответствующего потока, находящейся в очереди, вследствие превышения интервала ожидания.

Из состояния $(i_1+1,l_1,i_2,l_2) \xrightarrow[(l_1=0,l_2=0)]{\mu_1\cdot(i_1+1)}$ переход осуществляется по завершении обслуживания заявки ТРВ при отсутствии в очереди заявок других потоков.

Из состояния

$(i_1,l_1,i_2+1,l_2) \xrightarrow[((l_1=0)or(w+i_2+b_1>V),l_2=0)]{\mu_2(i_2+1,f)}$ переход осуществляется при завершении обслуживания заявки ТД и пустой очереди соответствующего потока, при этом очередь заявок ТРВ тоже нулевая либо свободного КР недостаточно, чтобы начать обслуживание очередной заявки первого потока.

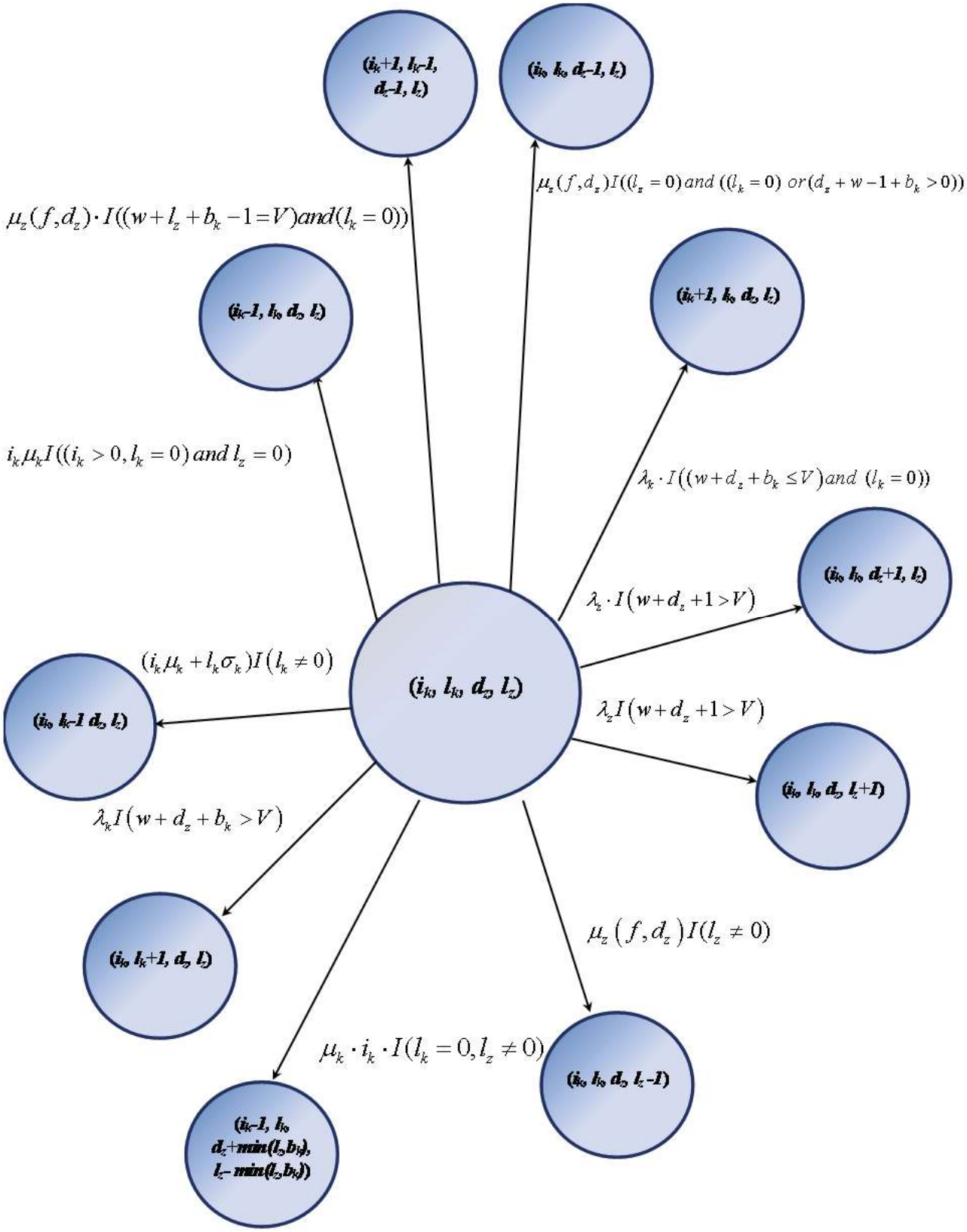


Рис. 2. Возможные переходы системы из текущего состояния

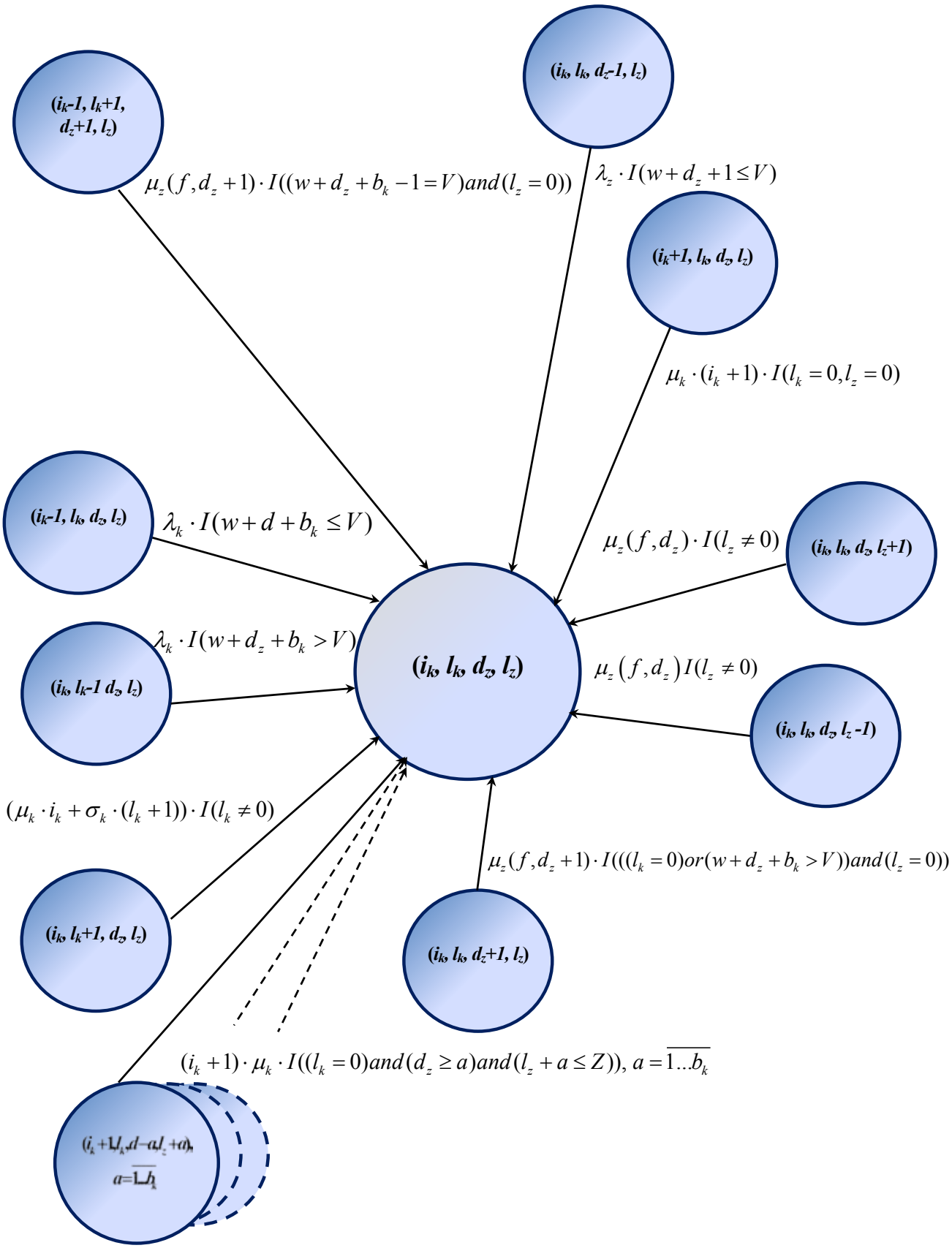


Рис. 3. Возможные переходы системы в текущее состояние

Из состояния $(i_1, l_1, i_2, l_2 + 1) \xrightarrow[((w+i_2+b_1-1>V) or (l_1=0), l_2 \neq 0)]{\mu_2(i_2, f)}$ переход осуществляется при завершении обслуживания заявки ТД (при этом на ее место встает новая из очереди ТД), при условии, что освободившийся КР не может быть выделен очередной заявке ТРВ.

Из состояния $(i_1, l_1, i_2 - 1, l_2) \xrightarrow[(w+i_2 \leq V)]{\lambda_{t2}(i_2-1, l_2)}$ переход осуществляется при поступлении очередной заявки ТД и наличии достаточного свободного КР для ее обслуживания.

Из состояния $(i_1, l_1, i_2, l_2 - 1) \xrightarrow[(w+i_2+1>V)]{\lambda_{t2}(i_2, l_2-1)}$ переход осуществляется при поступлении очередной заявки ТД и отсутствии достаточного свободного КР для ее обслуживания.

Из состояния $(i_1 - 1, l_1 + 1, i_2 + 1) \xrightarrow[(w+i_2+b_1=V, l_1 \neq 0)]{\mu_2(i_2+1, f)}$ переход осуществляется при завершении при завершении обслуживания заявки ТД и принятии на обслуживание очередной заявки ТРВ, имеющей приоритет, при условии достаточности КР.

Из состояний $(i_1 + 1, \underset{a=\overline{1 \ldots b_1}}{i_2 - a}, l_2 + a) \xrightarrow[(l_1=0, i_2 \geq a, l_2 + a \leq N_2)]{(i_1+1) \cdot \mu_1}$ переход осуществляется при завершении обслуживания заявки ТРВ и пустой очереди соответствующего потока, при этом в зависимости от длины очереди ТД на обслуживание будет принято от 1 до b_1 заявок второго потока.

Заметим, что при $l_2 \neq 0$ пропускная способность всех макроканалов, выделенных ТД, *минимальна*, т.е. для всех обслуживаемых заявок второго потока $b_2 = g_2 = 1$.

Чтобы в записи системы уравнений равновесия упростить вид состояний, из которых совершается переход, оставим в их обозначении только те компоненты, которые при этом изменяются. Система уравнений формируется путем последовательного перебора всех возможных состояний, для которых предварительно необходимо провести общую нумерацию:

$$
\begin{aligned}
&P(i_1, l_1, i_2, l_2) \cdot \{\lambda_{t1}(i_1, l_1) \cdot I(w + i_2 + b_1 \leq V) + \lambda_1(i_1, l_1) \cdot I(w + i_2 + b_1 > V) + \\
&+ \lambda_{t2}(i_2, l_2) \cdot I(w + i_2 + 1 \leq V) + \lambda_{t2}(i_2, l_2) \cdot I(w + i_2 + 1 > V) + \mu_1 \cdot i_1 \cdot I(l_1 = 0, l_2 = 0) + \\
&+ (\mu_1 \cdot i_1 + \sigma \cdot l_1) \cdot I(l_1 \neq 0) + \mu_2(i_2, f) \cdot I((l_1 = 0) or (w + i_2 + b_1 - 1 > V), l_2 = 0) + \\
&+ \mu_2(i_2, f) \cdot I(l_1 \neq 0) + \mu_1 \cdot i_1 \cdot I(l_1 = 0, l_2 \neq 0) + \mu_2(i_2, f) \cdot I(w + i_2 + b_1 - 1 = V, l_2 = 0) \ \} = \\
&= \{P(i_1 - 1) \cdot \lambda_{t1}(i_1 - 1, l_1) \cdot I(w + i_2 + b_1 \leq V) + P(l_1 - 1) \cdot \lambda_{t1}(i_1 - 1, l_1) \cdot I(w + i_2 + b_1 > V) + \\
&+ P(i_2 - 1) \cdot \lambda_{t2}(i_2 - 1, l_2) \cdot I(w + i_2 + 1 \leq V) + P(l_2 - 1) \cdot \lambda_{t2}(i_2, l_2 - 1) \cdot I(w + i_2 + 1 > V) + \\
&+ P(i_1 + 1) \cdot \mu_1 \cdot (i_1 + 1) \cdot I(l_1 = 0, l_2 = 0) + P(l_1 + 1) \cdot (\mu_1 \cdot i_1 + \sigma \cdot (l_1 + 1)) \cdot I(l_1 \neq 0) + \\
&+ P(i_2 + 1) \cdot \mu_2(i_2 + 1, f) \cdot I((l_1 = 0) or (w + i_2 + b_1 > V), l_2 = 0) + \\
&+ P(l_2 + 1) \cdot \mu_2(i_2, f) \cdot I(l_2 \neq 0) + P(i_1 - 1, l_1 + 1, i_2 + 1) \cdot \mu_2(i_2 + 1, f) \cdot I(w + i_2 + b_1 - 1 = V, l_2 = 0) + \\
&+ \sum_{a=\overline{1 \ldots b_1}} P(i_1 + 1, i_2 - a, l_2 + a) \cdot (i_1 + 1) \cdot \mu_1 \cdot I(l_1 = 0, i_2 \geq a, l_2 + a \leq N_2)\}, \quad (i_1(t), l_1(t), i_2(t), l_2(t)) \in S.
\end{aligned}
\tag{17}
$$

Здесь $I(\cdot)$ — индикаторная функция, значение которой равно «1» при выполнении условия в скобках или «0» — в противном случае. Для значений $P(i_1, l_1, i_2, l_2)$ выполняется условие нормировки.

Эксперимент

В общем случае решение системы уравнений (17) может быть получено с помощью стандартных программных средств для ЭВМ численными методами [13]. Общее время обслуживания рассчитывается по выражению (1).

На рис. 4 и 5 приведены типовые графики зависимостей $\overline{T}_{обсл.общ.}$, $\overline{T}_{СК}$, $\overline{T}_{обр}$ от M для первого и второго потока заявок соответственно.

Ввиду сложности вывода точных аналитических зависимостей приведенные выше графики можно получить только путем последовательного решения системы (17) для различных значений M. Из графиков видно, что функции $\overline{T}_{обсл.общ.}$ для обоих потоков имеют минимум в одной и той же точке, который может быть найден численными методами. Таким образом, существует решение рассматриваемой оптимизационной задачи по поиску оптимального распределения канального ресурса между служебными и рабочими каналами.

Как отмечалось выше, в процессе функционирования сети радиосвязи структура и характер абонентского трафика не являются стационарными, в частности, возможны значительные колебания интенсивности первичной нагрузки, кроме того, может меняться доступный объем распределяемого канального ресурса. На рис. 6 и 7 приводятся результаты исследования влияния указанных факторов на положение точки минимума функции $\overline{T}_{обсл.общ.}(M)$ для ТРВ, т.е. значения $\overline{T}_{обсл.общ.}$ и $M_{СК}^{опт}$.

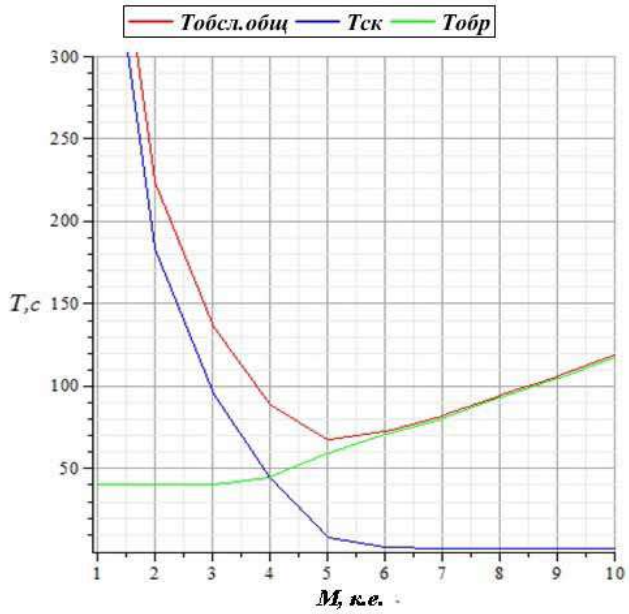


Рис. 4. Графики зависимостей времени обслуживания заявок трафика реального времени от величины КР, выделенного под СК

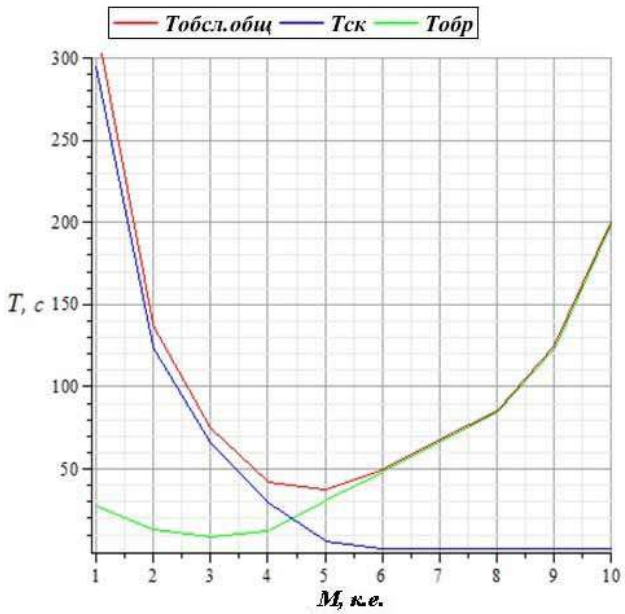


Рис. 5. Графики зависимостей времени обслуживания заявок трафика данных от величины КР, выделенного под СК

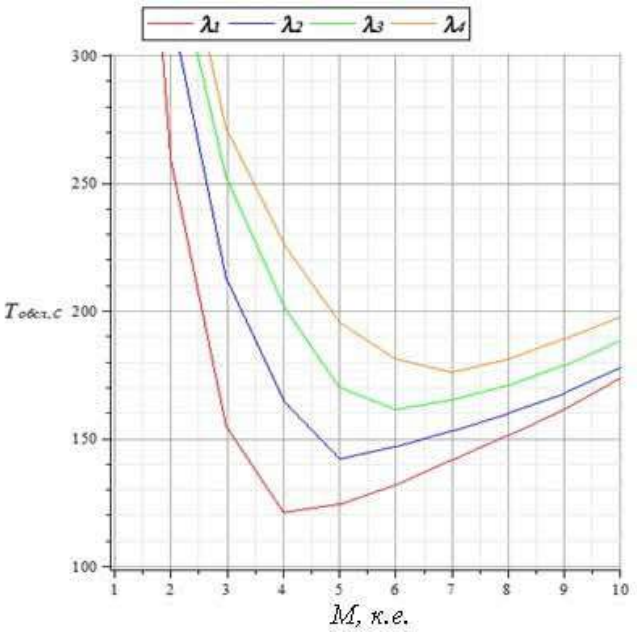


Рис. 6. Графики зависимости среднего времени обслуживания трафика реального времени от величины КР, выделенного под СК при различной первичной нагрузке

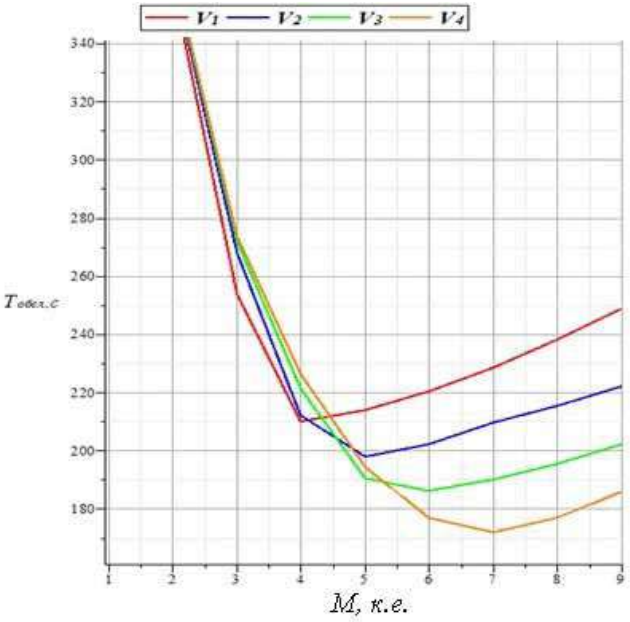


Рис. 7. Графики зависимости среднего времени обслуживания трафика реального времени от величины КР, выделенного под СК при различном объеме доступного КР

С ростом первичной нагрузки значение $M_{CK}^{опт}$, соответствующее оптимальному времени обслуживания абонентского трафика, также увеличивается — точка минимума смещается вправо. Очевидно, что при большей первичной нагрузке требуется более высокая пропускная способность СК, при этом $T_{обсл.общ.}^{опт}$ возрастает. Увеличение доступного КР сопровождается, *во-первых*, смещением точки минимума вправо, а *во-вторых*, уменьшением значения $T_{обсл.общ.}^{опт}$.

Заключение

Для решения задачи оценки эффективности и качества информационного обмена в мультисервисной радиосети с предоставлением каналов по требованию разработана комплексная математическая модель, которая является объединением математических моделей двух подсистем: широковещательного служебного канала с тактированным случайным множественным доступом и подсистемы распределения рабочих каналов. Математическая модель служебного канала задает входную нагрузку для второй модели, текущее состояние которой, в свою очередь, оказывает воздействие на входную нагрузку в служебном канале. Так учитывается взаимное влияние двух фаз обслуживания абонентского трафика в сети радиосвязи.

На основе анализа большого числа результатов аналитического и имитационного моделирования были получены достаточно простые выражения, позволяющие в пределах погрешности 5–10% оценить пропускную способность и среднее время передачи для широкого набора протоколов синхронного случайного множественного доступа по каждой из групп разнородных абонентов, что обеспечило относительную простоту разработанной модели.

В качестве основы для построения аналитической модели подсистемы распределения рабочих каналов была использована *многопотоковая модель мультисервисной линии связи* с динамически изменяемой скоростью передачи данных, которая обеспечивает эффективное использование канального ресурса радиосети. Требуемые показатели определяются путем численного решения системы уравнений равновесия, для которой составлены правила автоматизированного синтеза. Следует заметить, что предложенный подход к комплексному математическому описанию двухфазного обслуживания трафика позволяет легко изменить выбранную модель мультисервисной линии связи в соответствии со спецификой рассматриваемой радиосети.

Разработанный математический аппарат позволяет, в частности, рассчитать заданные показатели оперативности информационного обмена. Анализ результатов моделирования показал, что в радиосети с предоставлением каналов по требованию для фиксированных значений входных параметров существует оптимальное разделение общего ограниченного канального ресурса между служебными и рабочими каналами, при котором достигается *минимум среднего времени обслуживания* абонентского трафика. Длительность проведения необходимых расчетов на современных ЭВМ дает возможность напрямую использовать полученную модель при организации оперативного управления параметрами радиосети.

При изменении входной нагрузки и общего объема доступного канального ресурса радиосети требуемое количество служебных каналов, соответствующее оптимальному общему времени обслуживания абонентского трафика, также меняется. Следовательно, в условиях нестационарности первичной нагрузки и объема канального ресурса необходимо осуществлять динамическое перераспределение канального ресурса между служебными и рабочими каналами для поддержания оптимальной оперативности информационного обмена.

Литература

1. Андреев Г. И., Летунов В. В., Андреева Д. В. Эффективная спутниковая телесигнализация в подсистеме безопасности ГАС РФ «Правосудие» // Правовая информатика. 2017. № 1. С. 23–27. DOI: 10.21681/1994-1404-2017-1-23-27.
2. Григорьев, В. А., Лагутенко О. И., Распаев Ю. А. Сети и системы радиодоступа. М.: Эко-Трендз, 2005. – 384 с.
3. Деарт В. Ю. Мультисервисные сети связи. Транспортные сети и сети доступа. М.: Инсвязьиздат, 2007. – 166 с.
4. Ковальков Д. А., Крикунов А. А., Гаврилин Е. А., Ломов П. С. Расчет характеристик протокола случайного множественного доступа в широковещательной радиосети в условиях различного приоритета обслуживаемых абонентов // Труды Всеросс. конф. (с междунар. участием) «Радиоэлектронные устройства и системы для инфокоммуникационных технологий – РЭУС-2019» (29–31 мая 2019 г.). Сер. «Научные конференции, посвященные дню Радио». М.: Моск. НТОРЭС им. А. С. Попова, 2019. С. 195–200.
5. Крикунов А. А., Ковальков Д. А. Расчёт показателей качества обслуживания в радиосети декаметрового диапазона на основе многопотоковой модели с конечным числом абонентов и повтором заблокированных заявок // Радиотехнические и телекоммуникационные системы. – 2011. № 3. С. 72–76.
6. Крикунов А. А., Ковальков Д. А., Гаврилин Е. А. Оптимизация параметров протокола доступа в пакетной радиосети с интеграцией служб // Труды Междунар. симп-ма «Надежность и качество» / Пензенский гос. ун-т. Том 1. Пенза: ПГУ, 2017. С. 91–94. ISS. 2220-6418.
7. Крикунов А. А., Лапшин В. Ю., Ковальков Д. А., Шиманов С. Н. Оптимизация длительности обслуживания трафика в мультисервисной радиосети с динамическим выделением каналов по требованию // Известия института инженерной физики. 2012. № 3 (25). С. 49–53.
8. Крылов В. В. Теория телетрафика и ее приложения. СПб.: БХВ-Санкт-Петербург, 2005. 288 с.

9. Ловцов Д. А., Лобан А. В. Развитие информационно-телеметрического обеспечения наземно-космической связи в ГАС РФ «Правосудие» // Правовая информатика. 2019. № 1. С. 29–35. DOI:: 10.21681/1994-1404-2019-1-29-35.
10. Наумов В. А., Самуйлов К. Е., Яркина Н. В. Теория телетрафика мультисервисных сетей связи. М.: Изд-во РУДН, 2007. 191 с.
11. Овчинников А. М. Открытые стандарты цифровой транкинговой радиосвязи: серия изданий «Связь и бизнес». М.: МЦНТИ, «Мобильные коммуникации», 2000. 166 с.
12. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр. М.: Изд. дом «Вильямс», 2004. 1104 с.
13. Степанов С. Н. Основы телетрафика мультисервисных сетей. М.: Эко-Трендз, 2010. 392 с.
14. Степанов С. Н. Теория телетрафика: концепции, модели, приложения. М.: Горячая линия-Телеком, 2015. 867 с.
15. Сухов А. В. Оценка информационного ресурса радионавигационных станций в условиях помех от средств мобильной связи // Правовая информатика. 2019. № 1. С. 36–45. DOI: 10.21681/1994-1404-2019-1-36-45.
16. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 960 с.
17. Шиманов С. Н., Ковальков Д. А., Крикунов, А. А. Оценка интенсивности абонентской нагрузки в широковещательной радиосети // Всеросс. конф. «Современные технологии обработки сигналов» (СТОС-2019). Сер. науч. всеросс. конф-ции / РНТОРЭС им. А.С. Попова. Вып. VII. М.: «БРИС-М», 2019.С. 52–57. ISBN 978-5-905278-39-6.

Рецензент: ***Сухов Андрей Владимирович,*** *доктор технических наук, профессор, старший научный сотрудник научно-производственного объединения «Специальная техника и связь», Российская Федерация, г. Москва.*
E-mail: avs57@mail.ru

EFFICIENCY OF INFORMATION EXCHANGE IN A MULTI-SERVICE RADIO NETWORK WITH ON-DEMAND CHANNEL ALLOCATION

Sergey Shimanov, *Dr. Sc. (Technology), Professor, Professor of the Department of Automated Combat Control Systems of the branch of the Military Academy of the Peter the Great Strategic Missile Forces, Moscow Region, Serpukhov, Russian Federation.*
E-mail: *41kaf_rabota@mail.ru*

Alexey Krikunov, *Ph.D. (Technology), Doctoral student of the branch of the Military Academy of the Peter the Great Strategic Missile Forces, Moscow Region, Serpukhov, Russian Federation.*
E-mail: *41kaf_rabota@mail.ru*

Keywords: *multiservice radio network, radio communication network, multithreaded model, provision of channels on demand, heterogeneous traffic, two-phase traffic service, random multiple access, trunked communication system, non-stationary subscriber load, dynamic distribution of the channel resource, efficiency of information exchange.*

Abstract.

Purpose of the article: is to improve the scientific and methodological apparatus for evaluating and optimizing the characteristics of multiservice radio communication networks in the context of the dynamics of subscriber traffic and available channel resource.

Methods used: methods of the theory of teletraffic, methods of analytical and simulation modeling, probability theory and the theory of Markov processes.

Results: a complex mathematical model for servicing subscriber traffic in a multiservice radio network with on-demand channel allocation in conditions of a finite number of subscribers and a small channel resource is developed; the resulting model allows us to take into account the mutual dependence of the durations of various service phases: the stage of sending a request via a random access channel to the main station and the stage of direct transmission of user traffic according to the accepted service algorithm; It is shown that there is an optimal distribution of the channel resource between the service and working channels, which depends on the current load and the available channel capacity of the radio network.

References

1. Andreev G. I., Letunov V. V., Andreeva D. V. E`ffektivnaia sputneykovaia tele-signalizatciia v podsisteme bezopasnosti GAS RF «Pravosudie» // Pravovaia informatika. 2017. № 1. S. 23-27. DOI: 10.21681/1994-1404-2017-1-23-27.
2. Grigor`ev, V. A., Lagutenko O. I., Raspaev Iu. A. Seti i sistemy` radiodostu-pa. M.: E`ko-Trendz, 2005. 384 s.
3. Deart V. Iu. Mul`tiservisny`e seti sviazi. Transportny`e seti i seti dostupa. M.: Insviaz`izdat, 2007. 166 s.
4. Koval`kov D. A., Krikunov A. A., Gavrilin E. A., Lomov P. S. Raschet harakteristik protokola sluchai`nogo mnozhestvennogo dostupa v shirokoveshchatel`noi` radioseti v usloviiakh razlichnogo prioriteta obsluzhivaemy`kh abonentov // Trudy` Vseross. konf. (s mezhdunar. uchastiem) «Radioe`lektronny`e ustroi`stva i sistemy` dlia infokommunikatcionny`kh tekhnologii`– RE`US-2019» (29–31 maia 2019 g.). Ser. «Nauchny`e konferentcii, posviashchenny`e dniu Radio». M.:Mosk. NTORE`S im. A. S. Popova, 2019. S. 195-200.
5. Krikunov A. A., Koval`kov D. A. Raschyot pokazatelei` kachestva obsluzhivaniia v radioseti dekametrovogo diapazona na osnove mnogopotokovoi` modeli s konechny`m chislom abonentov i povtorom zablokirovanny`kh zaiavok // Radiotekhnicheskie i telekommunikatcionny`e sistemy`. 2011. № 3. S. 72-76.
6. Krikunov A. A., Koval`kov D. A., Gavrilin E. A. Optimizatciia parametrov protokola dostupa v paketnoi` radioseti s integratciei` sluzhb // Trudy` Mezhdunar. simp-ma «Nadezhnost` i kachestvo» / Penzenskii` gos. un-t. Tom 1. Penza: PGU, 2017. S. 91-94. ISS. 2220-6418.
7. Krikunov A. A., Lapshin V. Iu., Koval`kov D. A., Shimanov S. N. Optimizatciia dlitel`nosti obsluzhivaniia trafika v mul`tiservisnoi` radioseti s dinamicheskim vy`deleniem kanalov po trebovaniiu // Izvestiia instituta inzhenernoi` fiziki. 2012. № 3 (25). S. 49-53.
8. Kry`lov V. V. Teoriia teletrafika i ee prilozheniia. SPb.: BKHV-Sankt-Peterburg, 2005. 288 s.
9. Lovtcov D. A., Loban A. V. Razvitie informatcionno-telemetricheskogo obespecheniia nazemno-kosmicheskoi` sviazi v GAS RF «Pravosudie» // Pravovaia informatika. 2019. № 1. S. 29-35. DOI: 10.21681/1994-1404-2019-1-29-35.
10. Naumov V. A., Samui`lov K. E., Iarkina N. V. Teoriia teletrafika mul`tiservisny`kh setei` sviazi. M.: Izd-vo RUDN, 2007. 191 s.
11. Ovchinnikov A. M. Otkry`ty`e standarty` tcifrovoi` trankingovoi` radiosviazi: seriia izdanii` «Sviaz` i biznes». – M.: MTCNTI, «Mobil`ny`e kommunikatcii», 2000. 166 s.
12. Scliar B. Tcifrovaia sviaz`. Teoreticheskie osnovy` i prakticheskoe primenenie. Izd. 2-e, ispr. M.: Izd. dom «Vil`iams», 2004.1104 s.
13. Stepanov S. N. Osnovy` teletrafika mul`tiservisny`kh setei`. M.: E`ko-Trendz, 2010. 392 s.
14. Stepanov S. N. Teoriia teletrafika: kontceptcii, modeli, prilozheniia. M.: Goriachaia liniia-Telekom, 2015. 867 s.
15. Suhov A. V. Ocenka informatcionnogo resursa radionavigatcionny`kh stantcii` v usloviiakh pomekh ot sredstv mobil`noi` sviazi // Pravovaia informatika. 2019. № 1. S. 36-45. DOI: 10.21681/1994-1404-2019-1-36-45.
16. Tanenbaum E`., Ue`zeroll D. Komp`iuterny`e seti. 5-e izd. SPb.: Peter, 2012. 960 s.
17. Shimanov S. N., Koval`kov D. A., Krikunov, A. A. Ocenka intensivnosti abonentskoi` nagruzki v shirokoveshchatel`noi` radioseti // Vseross. konf. «Sovremenny`e tekhnologii obrabotki signalov» (STOS-2019). Ser. nauch. vseross. konf-tcii / RNTORE`S im. A.S. Popova. Vy`p. VII. M.: «BRIS-M», 2019. S. 52-57. ISBN 978-5-905278-39-6.

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИИ В ЭРГАСИСТЕМАХ

Ловцов Д.А.*

***Ключевые слова**: эргасистема, защищенность информации, достоверность, конфиденциальность, сохранность, принципы обеспечения, ошибки переработки, разрушающие факторы, несанкционированный доступ и использование, способы защиты информации, математические структуры.*

Аннотация.

Цель работы: совершенствование научно-методической базы теории защищенности информации в эргасистемах.

Метод: системный анализ, прагматическая классификация и математическое моделирование основных частных задач обеспечения защищенности информации в эргасистемах.

Результаты: обоснована непротиворечивая совокупность принципов контроля и защиты информации от ошибок переработки, разрушающих факторов и несанкционированного доступа и использования; обоснована прагматическая классификация ошибок при переработке информации, разрушающих факторов, потенциальных каналов утечки информации, а также соответствующих способов защиты информации; определены математические структуры моделей задач обеспечения достоверности, конфиденциальности и сохранности информации в эргасистеме; приведены доказательства утверждений о повышении достоверности информации, о совершенной семантической скрытности и об энергетической скрытности динамической информации.

Полученные результаты являются концептуальной основой для создания соответствующего эффективного информационно-математического обеспечения контроля и защиты информации в эргасистемах.

DOI: 10.21681/1994-1404-2021-1-36-50

Введение

Эффективность и информационная безопасность эргатических систем (эргасистем) в значительной степени определяются *защищённостью* циркулирующей и перерабатываемой в них содержательной информации, для обеспечения которой создаются и совершенствуются функциональные подсистемы контроля и защиты информации (КЗИ). При этом под ***защищённостью*** информации понимается конструктивное свойство функциональной подсистемы КЗИ, характеризующее степень защищённости информационных массивов (ИМ) и заключающееся в способности не допускать случайного или целенаправленного искажения или разрушения, раскрытия или модификации ИМ в информационной базе эргасистемы[1] [6, 7].

Существующие угрозы нарушения *защищённости* (в частности, достоверности, конфиденциальности и сохранности) информации обусловливают жизненно важную необходимость создания эффективных мер контроля всевозможных угроз и защиты содержательной информации в эргасистемах от искажения при переработке, от раскрытия (утечки) и модификации при несанкционированном доступе и использовании, а также от разрушения при эксплуатации [1].

Задача обеспечения (повышения) *достоверности* (помехоустойчивости, помехозащищенности [7]) при переработке информации в эргасистеме заключается главным образом в контроле правильности ИМ, обнаружении ошибок и их исправлении на различных этапах переработки информации. Задача обеспечения *конфиденциальности* (доступности, скрытности, имитостойкости [7]) — в контроле полномочий объектов эргасистемы (операторов, программно-технических средств и ресурсов эргасистемы), контроле операций по выборке ИМ и посылке данных на хранение, в установлении правил взаимодействий и разграничении доступа операторов. Задача обеспечения *сохранности*

[1] *Ловцов Д. А.* Методы защиты информации в АСУ сложными динамическими объектами // НТИ. Сер. 2. Информ. процессы и системы. 2000. № 5. С. 29–45.

* ***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, г. Москва, Российская Федерация.*

E-mail: dal-1206@mail.ru

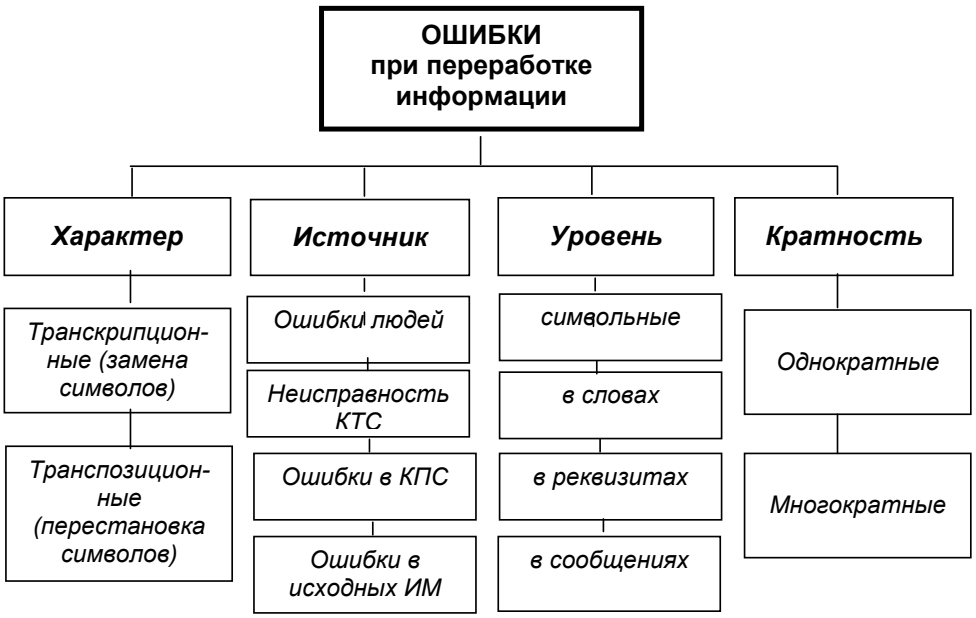


Рис. 1. Общая классификация ошибок, возникающих в эргасистеме при переработке информации

(целостности, готовности [7]) информации при эксплуатации эргасистем — в контроле правильности ИМ, обнаружении ошибок, резервировании (копировании, дублировании ИМ и их предысторий, т. е. предыдущих ИМ и массивов изменений), регенерации (перезаписи) ИМ, восстановлении ИМ во внутримашинной информационной базе по зарезервированным ИМ и ИМ из исходных документов (сообщений). Оптимальное резервирование ИМ является также одним из системных методов повышения *достоверности* информации в эргасистеме.

Совместное продуктивное решение данных сложных задач возможно на основе обоснованной непротиворечивой совокупности принципов КЗИ от ошибок переработки, от разрушающих факторов и от несанкционированного доступа и использования.

Принципы контроля и защиты информации от ошибок переработки

Исследование задачи *обеспечения достоверности информации* (ОДИ) в эргасистеме осуществляется на трех уровнях[2] [5, 14]:

синтаксическом (связан с контролем и защитой элементарных составляющих ИМ — знаков или символов);

семантическом (связан с обеспечением достоверности смыслового значения ИМ, их логичности, непротиворечивости и согласованности);

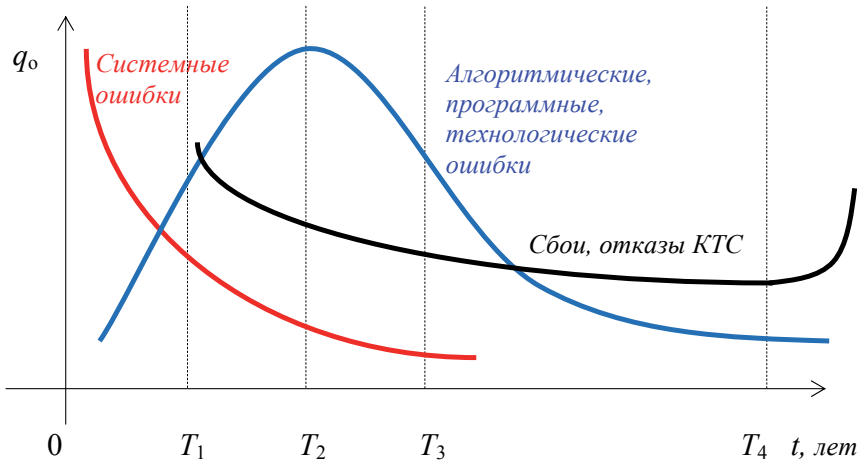
прагматическом (связан с изучением вопросов ценности информации при принятии управленческих решений, её доступности и своевременности, влияния ошибок на качество и эффективность функционирования эргасистем).

На *первом* (синтаксическом) уровне в качестве показателя достоверности можно использовать функцию $D = 1 - q_1$ (*верность* [5]) вероятности q_1 ошибки, т. е. события, состоящего в том, что *единичный* правильный (верный) символ или знак заменяется в процессе переработки информации другим, ошибочным.

На *втором* и *третьем* уровнях в качестве показателя достоверности можно использовать некоторую функцию $D(q_1)$ вероятности q_1 ошибки *единичного массива информации* (ЕМИ), т. е. события, заключающегося в том, что реальный ЕМИ (поле, запись, блок, дейтаграмма, ИМ, перфокарта, документ и др.) в информационной базе (ИБ) эргасистемы не совпадает (в пределах заданной точности) с его истинным значением.

Процесс переработки информации (реализации любой задачи в эргасистеме) можно разбить на ряд основных этапов: сбор и регистрация информации; передача исходной информации по каналам связи и первичная обработка ИМ, включая контроль обеспечения заданной достоверности; подготовка первичного документа для ввода в комплекс средств автоматизации (КСА); преобразование и перезапись данных на промежуточные документы; перезапись информации на машинный носитель; ввод информации в КСА (ЭВМ), в том числе непосредственный ввод в диалоговом человеко-машинном режиме; машинная обработка данных по алгоритмам, реализующим математические модели (решение задачи на КСА); сортировка выходных ИМ и их вывод из КСА на внешние устройства; сортировка полученных документов, их проверка и доставка получателям.

[2] *Мамиконов А. Г., Кульба В. В., Шелков А. Б.* Достоверность, защита и резервирование информации в АСУ. М. : Энергоиздат, 1986. 304 с.;
Мельников Ю. Н. Достоверность информации в сложных системах. М. : Сов. радио, 1974. 192 с.



Экспликация: T_1 — разработка проекта эргасистемы; (T_1 — T_2) — разработка эргасистемы; (T_2 — T_3) — ввод КСА в эксплуатацию; (T_3 — T_4) — гарантийная эксплуатация КСА; после T_4 — износ и старение КСА.

Рис. 2. Графики зависимости вероятности отказов на этапах жизненного цикла эргасистемы

Ошибки (*рис.* 1) могут возникать на любом из перечисленных этапов переработки информации. Ошибки персонала, операторов и пользователей средств автоматизации определяются [5]:

психофизиологическими характеристиками человека (усталостью и снижением работоспособности после определённого времени работы, неправильной интерпретацией используемых ИМ);

объективными причинами (несовершенством моделей представления информации, отсутствием должностных инструкций и нормативов, квалификацией персонала, несовершенством комплекса технических средств (КТС), неудачным расположением или неудобной конструкцией их с точки зрения эксплуатации);

субъективными причинами (небрежностью, безразличием, несознательностью, безответственностью некоторых операторов, следствием нарушения принципа материальной заинтересованности, преднамеренным искажением ИМ в корыстных целях, отсутствием должного контроля со стороны руководства за качеством выполняемых операций, плохой организацией труда и др.).

Ошибки, возникающие в процессе переработки информации на КСА, связаны [1] с помехами, сбоями и отказами КТС, ошибками в комплексах программных средств (КПС), недостаточной точностью или ошибками в исходных данных, округлением исходных, промежуточных и выходных данных, неадекватностью реализованных математических моделей реальным процессам, приближённым характером используемых методов решения задач на ЭВМ (что характерно в первую очередь для итерационных методов).

Неисправность КТС приводит к ошибкам, связанным с неисправностью центрального процессора КСА (ЭВМ), периферийного оборудования, несоответствием техническим нормам и условиям хранения магнитных носителей ИМ, физическим износом и старением элементов и узлов КТС и др. Вероятность q_o отказов КТС изменяется на этапах его жизненного цикла (*рис.* 2).

Ошибки в комплексах алгоритмов и программ обычно классифицируют на[3] [5] (см. *рис.* 2):

системные, обусловленные неправильным пониманием требований автоматизируемой задачи эргасистемы и условий её реализации;

алгоритмические, связанные с некорректной формулировкой и программной реализацией алгоритмов;

программные, возникающие вследствие описок при программировании на ЭВМ, ошибок при кодировании информационных символов, ошибок в логике машинной программы и др.;

технологические, возникающие в процессе подготовки программной документации и перевода её во внутримашинную информационную базу эргасистемы.

Обеспечение достоверности переработки информации в функционирующей эргасистеме состоит в определении пунктов логической обработки и контроля ИМ. На основе анализа различных структур переработки информации можно выделить несколько типовых структур.

В стандартном *типовом модуле переработки* (ТМП) цикл переработки информации распадается (*рис.* 3) на непосредственно логическую (математическую) обработку, контроль и исправление ошибок [5, 8]. На некоторых этапах переработки информации операции (фазы) контроля и исправления недостоверных ЕМИ могут отсутствовать либо осуществляться для группы

[3] *Ловцов Д. А.* Контроль и защита информации в АСУ. В 2-х кн. Кн. 1. Вопросы теории и применения. М. : ВА им. Петра Великого, 1991. 172 с. Кн. 2. Моделирование и разработки. М. : ВА им. Петра Великого, 1997. 252 с.

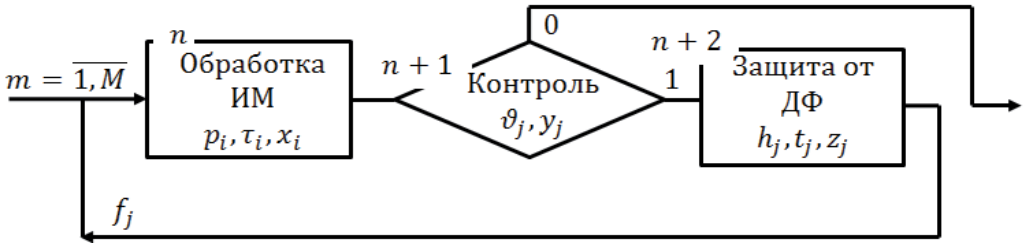


Рис. 3. Вариант разметки ТМП для задачи ОДИ

из нескольких этапов, на каждом из которых, в свою очередь, осуществляется локальный контроль и исправление ошибок. После исправления ошибочных ЕМИ они вновь обрабатываются с последующим контролем и исправлением. Фазы контроля и исправления ошибок могут повторяться *случайное* число раз.

В общем виде вероятность D достоверной переработки ЕМИ в эргасистеме определяется структурными параметрами $<G,\ p_i,\ f_j,\ I,\ J>$ технологического процесса переработки информации (ТППИ) и техническими параметрами $<\tau_i,\ x_i,\ \vartheta_j,\ y_j,\ t_j,\ z_j>$ алгоритмов (устройств) обработки на каждом этапе переработки информации:

$$D = 1 - Q = D\{S_1, \nu_m, C^0, T^0, M\}, \quad m=1,\ldots,M, \qquad (1)$$

где $S_1 = <G,\ p_i = 1 - q_i,\ f_j = 1 - e_j,\ \tau_i,\ x_i,\ \vartheta_j,\ y_j,\ t_j,\ z_j>,\ i = 1,\ldots,I;\ j = 1,\ldots,J$ — структура переработки информации; ν_m — значение случайной величины — количества циклов обработки m-го ЕМИ; C^0 — заданный материальный ресурс на обработку, контроль и исправление ошибочного ЕМИ; T^0 — директивное время переработки информации; $Q,\ M$ — вероятность искажения и величина массива перерабатываемой информации соответственно.

В эргасистеме, как правило, добиваться теоретически максимальной достоверности переработки информации нецелесообразно из-за резкого повышения сложности эргасистемы, стоимости её разработки, внедрения и эксплуатации; достаточно обеспечить требуемый (допустимый) уровень достоверности D. В реальных эргасистемах требуемая достоверность устанавливается с учётом последствий, к которым могут привести возникшие ошибки, и тех затрат (материальных, временных, интеллектуальных и др.), которые необходимы для их предотвращения (табл. 1).

Вместе с тем КТС эргасистемы часто не обеспечивает требуемого уровня достоверности переработки ИМ. Например, существующие каналы связи в эргасистеме обеспечивают (в условиях помех типа «белый шум» и с учётом различных значений удельного расхода β^2 энергии сигнала-переносчика ИМ и методов телеграфии: амплитудной — АТ, частотной — ЧТ, фазовой — ФТ, относительной фазовой — ОФТ) обмен информацией с вероятностью искажения 1 бит (рис. 4):

$q_1 \geq (10^{-1} \ldots 10^{-2})$ — радиоканал;
$q_1 \geq (10^{-3} \ldots 10^{-4})$ — радиорелейный канал;

Таблица 1

Вероятность ошибки и уровень затрат на ОДИ для некоторых классов задач эргасистемы

Класс задач эргасистемы	Допустимая вероятность q_1 искажения ЕМИ (ошибки)	Временные и материальные затраты, %				
		Время t_1 на техн. проектирование	Время t_2 на программирование	Время t_3 работы программы	Объем C_1 памяти	Стоимость C_1 КТС и др.
Оперативное планирование	10^{-4}	100	100	100	100	100
Технико-экономическое планирование	10^{-5}					
Статистический учет	10^{-5}					
Бухгалтерский учет	10^{-6}					
Обработка контрольно-измерительной информации от СДО	10^{-8}	150	150	160	170	150–200
Выработка управляющих воздействий на СДО	10^{-9}					

$q_1 \geq (10^{-4} \ \ldots \ 10^{-5})$ — проводной канал.

Поэтому для достижения *требуемой* $(q_1 \leq 10^{-6} \ldots 10^{-9})$ или *максимальной* достоверности переработки информации в эргасистеме используются специальные средства, методы и их комбинации, в том числе *каналы передачи данных* (см. рис. 4), содержащие устройства повышения достоверности (защиты от ошибок переработки).

В принятых обозначениях математическую *постановку задачи обеспечения достоверности* информации как задачи поиска оптимальной структуры $S_1^* \in \Delta_1$ переработки информации, минимизирующей суммарное (на обработку, контроль и исправления ошибок) время T и/или материальные затраты C на переработку информации, при ограничении на достоверность D перерабатываемых ИМ и при условии независимости вероятностей искажения q_i и обнаружения f_j ошибок информационных элементов можно записать в виде:

$$K_1: D(S_1^*, M, \tau_i, x_i, \vartheta_j, y_j, t_j, z_j, \nu_m) \geq D^0 \qquad (2)$$
$$T(S_1^*, M, \tau_i, \vartheta_j, t_j, \nu_m) = \min_{\{S1\}},$$
$$C(S_1^*, M, x_i, y_j, z_j, \nu_m) = \min_{\{S1\}},$$

где $\{S_1\} = \Delta_1$ — множество допустимых структур $S_1 = <p_i, f_j, I, J>$ переработки информации; D^0 — заданное значение вероятности достоверной переработки ЕМИ в эргасистеме.

Для стандартного ТМП (см. рис. 3) при $I = J = 1$ и заданных $p, f, \tau, \vartheta, t, x, y, z, C^0, T^0$ единственным параметром оптимизации процесса обработки ИМ является количество циклов ν_m, $m = 1, \ldots, M$ проверки и исправления ошибочной информации.

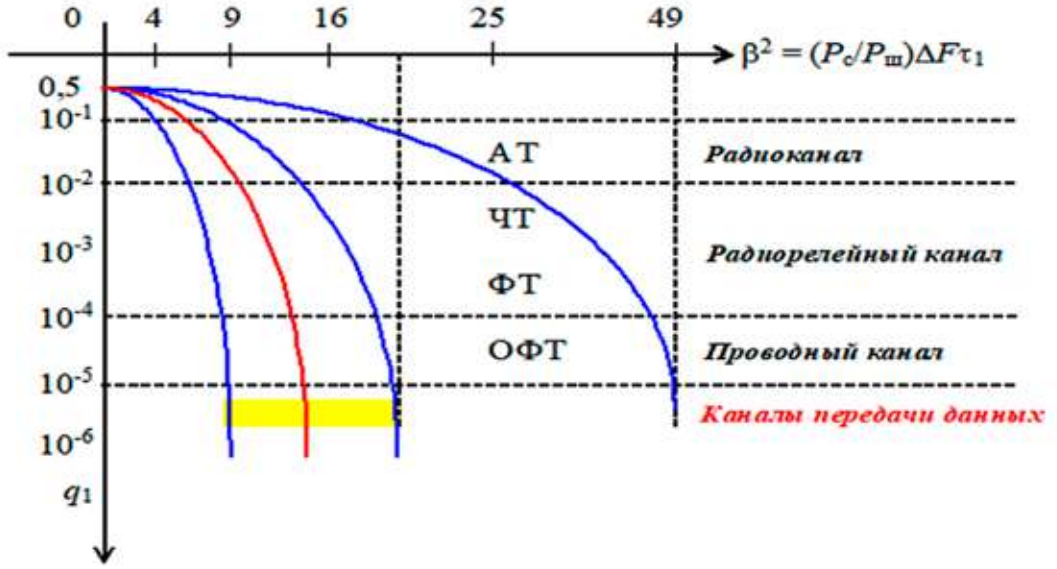


Рис. 4. Зависимость удельного расхода энергии сигнала-переносчика ИМ и вероятности искажения символа

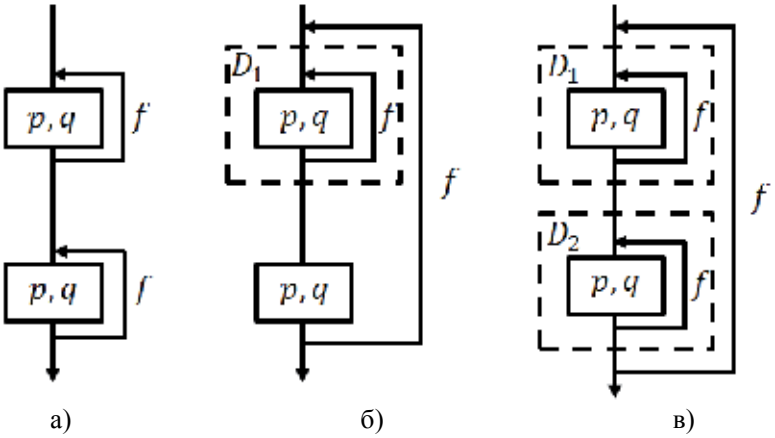
Производными стандартного ТМП являются последовательная структура переработки информации, последовательная структура при N-кратной переработке информации, последовательная структура при N-кратной переработке информации с общим контролем (общей обратной связью), циклическая и последовательно-циклическая структуры, сеть переработки информации[4]. *Сетевую* структуру переработки информации можно представить в виде графа, множество дуг которого образует стандартные ТМП и сложные циклы, а множество вершин совпадает с начальными и (или) конечными точками сложных циклов и стандартных ТМП.

***Утверждение* 1.** Достоверность информации в эргасистеме с последовательной структурой ТППИ и контролем в каждом узле по принципу обратной связи повышается, если концы обратной связи перенести к началу информационной цепи технологических операций[5].

Доказательство. Возможны три различных варианта (рис. 5, а, б, в) минимальных структурных фрагментов, из которых, собственно, и составляется структура (сеть) ТППИ в целом: (а) последовательное соединение двух ТМП, (б) последовательное соединение двух ТМП с общей обратной связью и без обратной связи для второго модуля, (в) последовательное соединение двух ТМП с общей обратной связью. Для простоты символ «решение» на рис. 5 изображен в виде точки.

[4] *Ловцов Д. А.* Контроль и защита информации в АСУ. В 2-х кн. Кн. 1. Вопросы теории и применения. М. : ВА им. Петра Великого, 1991. 172 с. Кн. 2. Моделирование и разработки. М. : ВА им. Петра Великого, 1997. 252 с.

[5] *Ловцов Д. А., Князев А. Г.* Оптимизация структуры достоверной переработки информации // НТИ. Сер. 2. Информ. процессы и системы. 1998. № 10. С. 20–27.



а) б) в)

Рис. 5. Варианты минимальных структурных фрагментов

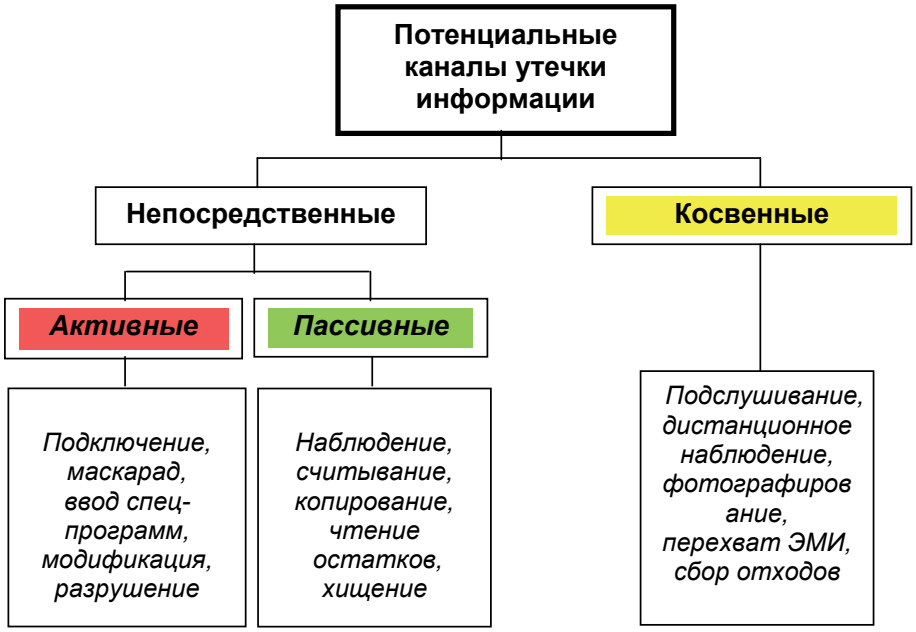


Рис. 6. Классификация каналы утечки информации

Определим для каждого из них вероятности того, что в установившемся режиме на k-м двухфазном $(i = 1,\ldots,2)$ этапе ТППИ единичный массив будет переработан без ошибок (при условии p, q, f = const):

$$D_a = D_{i=1}D_{i=2} = [p/(1 - qf)]^2 = p^2/(1 - 2qf + qf\mathbf{qf}), \quad (3)$$

$$D_б = D_1 p/[1 - (1 - D_1 p)f] = \\ = p^2/[1 - 2qf + qf(\mathbf{f + q - 1})], \quad (4)$$

$$D_1 D_2/[1 - (1 - D_1 D_2)f] = \\ = p^2/\{1 - 2qf + qf[(\mathbf{f+q-1)+f+qf-qf^2-1}]\}. \quad (5)$$

Из выражений (3) — (5) видно (выделено жирным), что поскольку $qf \geq f+q-1 \geq f+q-1+f+qf-qf^2-1$, то $D_a \leq D_б \leq D_в$, что и требовалось доказать.

Следовательно, первый структурный фрагмент является наименее приемлемым по критерию (2), но, с другой стороны, его реализация приводит к наименьшим временным и материальным затратам, поскольку $T_a < T_б < T_в$, $C_a < C_б < C_в$.

Принципы контроля и защиты информации от несанкционированного доступа и использования

Защищенность ИМ в значительной степени зависит от принятия эффективных мер по закрытию потенциальных *каналов утечки информации*, под которыми понимают[6] [9] объективно существующие способы несанкционированного использования данных, обусловленные структурно-функциональными особенностями эргасистем.

Множество существующих каналов утечки информации в эргасистеме можно разделить на три больших группы (рис. 6):

[6] *Ловцов Д. А.* Защита информации в информационно-вычислительной сети // НТИ. Сер. 3. Информ. процессы и системы. 1997. № 2. С. 7–13; Ловцов Д. А. Введение в информационную теорию АСУ: Монография. М. : ВА им. Петра Великого, 1996. 434 с.

непосредственные активные каналы, связанные с контактным несанкционированным доступом (НСД) к ресурсам эргасистемы и изменением её компонентов;

непосредственные пассивные каналы, связанные с контактным НСД к ресурсам эргасистемы, но не предусматривающие изменений компонентов системы;

косвенные каналы, позволяющие осуществить неконтактный НСД к ресурсам эргасистем.

К *первой* группе относятся, в частности, следующие основные каналы утечки информации: незаконное подключение к КТС (терминалам ввода-вывода, линиям передачи данных и др.); маскировка под зарегистрированных операторов (маскарад); несанкционированное изменение машинных программных массивов; несанкционированный ввод в программное обеспечение эргасистемы программных «закладок», специально разработанных для осуществления НСД к ИМ; злоумышленный вывод из строя подсистемы КЗИ от НСД и др.

Ко *второй* группе относятся следующие каналы: наблюдение за информационными массивами в процессе их переработки в эргасистеме; копирование ИМ, хранящихся на машинных (магнитных, оптических и др.) и немашинных (документальных) носителях; прямое хищение материальных носителей информации; преднамеренное считывание ИМ в файлах других операторов; сбор (чтение) остаточной информации на регистрах и в полях запоминающих устройств; использование служебного положения, т. е. незапланированного просмотра (ревизии) ИМ сотрудниками эргасистемы.

Каналы *третьей* группы: применение подслушивающих устройств; дистанционное наблюдение или фотографирование ИМ, представленных в визуальной (на экране дисплея, табло), графической или документальной форме; перехват, расшифровка и регистрация электромагнитного излучения (ЭМИ) КТС в процессе переработки информации (наличие большого количества переключательных цепей в составе современных ЭВМ позволяет в определенных условиях регистрировать их работу на значительном удалении как маломощного коротковолнового передатчика) с помощью специально разработанных для этой цели технических средств; сбор отходов («мусора») производства и функционирования эргасистем.

Непосредственное проникновение в информационную базу эргасистемы может осуществляться скрытно, т. е. в обход контрольных программ обеспечения конфиденциальности информации (ОКИ), а также с помощью нетрадиционных *скрытых каналов* [10, 11], реализуемых с помощью встроенных аппаратно-программных «закладок».

Наиболее характерные традиционные приёмы проникновения[7]:

использование точек входа, установленных в КСА программистами и обслуживающим персоналом, или точек, обнаруженных при проверках цепей системного контроля;

подключение к сети передачи данных специального терминала, обеспечивающего вход в информационную базу эргасистемы путем пересечения линии связи законного оператора с последующим восстановлением связи по типу ошибочного сообщения, а также в момент, когда оператор не проявляет активности, но продолжает занимать канал передачи данных;

аннулирование сигнала оператора о завершении работы с КСА и последующее продолжение работы от его имени;

неавторизованная модификация хранящейся информации, в результате чего оператор, которому эта информация принадлежит, не может получить к ней доступ.

Наибольшее распространение получили *скрытые каналы* по времени (используют временну́ю модуляцию занятости разделяемого информационно-вычислительного ресурса), каналы по памяти (используют разделяемый ресурс как промежуточный буфер при передаче данных), каналы в базах данных и знаний [4, 16] и ТППИ (используют зависимости между данными и их *функционально-технологическими преобразованиями*[8]).

Обеспечение гарантированной защиты эргасистем от НСД по скрытым каналам возможно при использовании «туннелирования» стандартных протоколов с использованием протоколов с минимальной избыточностью, не позволяющих модулировать поток пакетов. При этом пакеты стандартного протокола должны инкапсулироваться в пакеты протокола «туннелирования».

Основными *способами* ОКИ в эргасистеме являются (*рис*. 7): препятствие; контроль; управление доступом; преобразование информации.

Первый способ заключается в создании физического препятствия на пути к защищаемой информации и организации персонального автоматического (по индивидуальным токенам, жетонам, картам или ключам) и дистанционного (по специальным кодам) допуска к КСА.

Второй способ защиты заключается в организации всестороннего контроля законности операций (особенно копирования ИМ) ТППИ в эргасистеме, включая *надёжность* работы программно-математического обеспечения (ПМО), КТС и персонала; контроля законности получения доступа к ИМ каждого объекта (оператора, терминала, файла, программы или её части и др.) с целью предупреждения или обеспечения своевременной реакции на нарушение и защиты информации как от неавторизованного использования, так и от несанкционированного обслуживания системой.

Контроль доступа к информации эргасистем реализуется последовательным применением трёх способов (процедур) [3]:

[7] *Шураков В. В.* Обеспечение сохранности в системах обработки данных. М. : Финансы и статистика, 1987. 272 с.

[8] *Князев В. В., Ловцов Д. А.* Ситуационное планирование защищённой переработки информации в АСУ испытаниями сложных динамических объектов // Автоматика и телемеханика. 1998. № 9. С. 166–181.

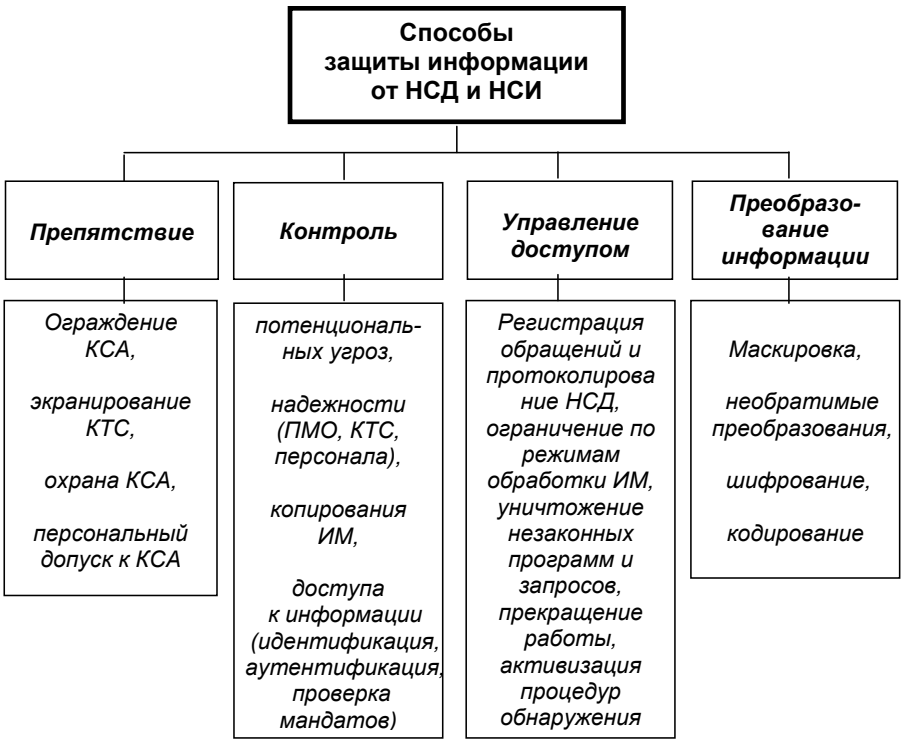


Рис. 7. Классификация способов защиты информации от несанкционированного доступа и использования

идентификации (присвоения объектам эргасистемы конкретных имён, кодов или их биометрических параметров [12] с целью последующего опознания и учёта фактов обращения, объединяемых в виде записей в так называемой «таблице авторизации», которая хранится в памяти КСА в преобразованном виде);

установления аутентичности (проверки подлинности объекта с помощью определенной информации, содержащейся в «матрице доступа» — списке операторов и запрещаемых объектов — и позволяющей убедиться в истинности обращения);

проверки полномочий (проверки информации, содержащейся в «матрице полномочий» по каждому объекту, о допустимых процедурах со стороны запрашиваемого).

Третий способ (см. рис. 7) ОКИ заключается в регулировании использования всех информационных и программно-технических ресурсов системы в пределах установленного регламента, включая ограничения на обработку ИМ, содержащих важную информацию, с уничтожением программ, сформулировавших незаконный запрос-обращение к особо важным ИМ или прекращением работы. При этом осуществляется регистрация всех (удачных и неудачных) обращений и протоколирование попыток НСД для последующего анализа и принятия мер при наличии угроз.

Четвёртый способ защиты (см. рис. 7) применяется для обеспечения необходимой скрытности информации как при переработке и хранении ИМ, так и при организации информационного обмена для получения допуска к ресурсам эргасистемы, а при передаче особо важной информации является единственным способом надежной защиты. Способ имеет четыре разновидности: маскировка; «необратимые» (плохообратимые) преобразования; шифрование; кодирование.

В случае *маскировки* защищаемые ИМ преобразуются таким образом, чтобы их содержание было доступно лишь при предъявлении некоторой специфической информации и осуществления обратных преобразований. При этом скрывается сам факт наличия информации.

В результате *«необратимых» преобразований* ИМ реформируются настолько, что для их раскрытия требуется применять специальный КТС.

Шифрование и *кодирование* позволяют скрывать содержание (смысл) ИМ при помощи, как правило, алфавитно-цифровых шифров (для донесений, отчётов и др.) и цифровых кодов (для команд, сигналов и др. коротких сообщений соответственно). При этом остается *проблемой* оценка уровня надежности и криптостойкости [15] (необратимости с точки зрения извлечения как корней, так и логарифмов) используемых стандартизованных односторонних функций зашифрования (дискретного возведения в степень в модульной арифметике) в различных криптоалгоритмах в условиях роста производительности современных вычислительных средств, приближающейся к условному порогу, равному приблизительно 10^{40} *операций в секунду* (и, возможно, более, если верить иностранным источникам, что существуют вычислительные возможности обеспечения обратимости стандартизованных функций зашифрования) [13].

Рассмотренные меры по защите ИМ предъявляют существенные *требования* к подсистеме КЗИ от несанкционированного доступа (НСД) и несанкционированного изменения (НСИ)[9]**:**

обеспечение свободного ввода данных в ИМ, к которым оператор имеет право доступа, и возможности спецификации доступа отдельных лиц к его информации с указанием типа разрешаемой работы;

обеспечение возможности выполнения процедур обновления и обработки ИМ, а также создания, модификации или исключения данных операторов в тех областях, за которые они отвечают;

информация, программное обеспечение и коммуникации должны быть защищены даже в случае серьёзных сбоев и отказов программных или технических средств;

зарегистрированный оператор должен всегда иметь доступ к своим индивидуальным ИМ;

защитный механизм КСА не должен быть разрушен даже при условии, что оператор обладает знаниями о технологии [2] его функционирования;

время реакции КСА на запросы оператора с учётом работы защитного механизма должно быть психологически приемлемым ($t \leq 20$ с);

подсистема ОКИ (в частности, подсистема авторизации, т. е. разрешения доступа) должна налагать допустимые ограничения на работу операционной системы КСА, структуру файлов, КТС и систему разделения времени;

обеспечение возможности выявления и использования минимально допустимого списка паролей, ключей и специальных команд с целью упрощения загрузки оператором при допустимых требованиях к ОКИ.

Создание подсистем КЗИ от НСД и НСИ включает три направления работ[10]: теоретические исследования; разработка средств защиты; обоснование способов использования средств защиты в эргасистеме.

В теоретическом плане основное внимание уделяется исследованию уязвимости информации в эргасистемах, выявлению и анализу каналов утечки информации, обоснованию принципов контроля и защиты информации в крупномасштабных эргасистемах и разработке методик оценки качества (надёжности) защиты. Общих методов решения проблемы ОКИ пока нет, достаточно строгие и практически значимые решения получены в настоящее время только для отдельных частных вопросов (выбор оптимальной длины пароля и оптимальной структуры ключа защиты, оценка стойкости шифрования и др.), для которых удалось сформулировать математически корректные постановки задач. Фундаментальными результатами теории ОКИ считаются *доказательства* сильной уязвимости информации в эргасистеме, возможности её защиты (с относительной надёжностью) и необходимости комбинированного использования всех способов, мер, методов, средств и мероприятий защиты.

***Утверждение* 2.** Необходимым и достаточным условием совершенной семантической скрытности динамической информации (передаваемых ИМ) в информационно-распределительной сети эргасистемы является равенство для всех переданных преобразованных информационных массивов (ПИМ) $M_{1i}, i=1,\ldots,N$ апостериорных вероятностей $p(M_{0i}|M_{1i})$ независимо от величины последних, т. е.:

$$p(M_{0i}|M_{1i}) = p(M_{0i}),\ i=1,\ldots,N, \qquad (6)$$

что эквивалентно независимости переданных ПИМ M_1 от передаваемых ИМ M_0.

Доказательство. Согласно теореме гипотез Байеса совместная вероятность передаваемых ИМ $p(M_{0i}),\ i=1,\ldots,N$, и переданных ПИМ $M_{1i},\ i=1,\ldots,N$

$$P(M_1, M_0) = P(M_0)P(M_1|M_0) = P(M_1)P(M_0|M_1).$$

Преобразуя формулу Байеса, получим:

$$-\log_2 P(M_0) - \log_2 P(M_1|M_0) =$$
$$= -\log_2 P(M_1) - \log_2 P(M_0|M_1).$$

Или, переходя к энтропии:

$$H(M_0) + H(M_1|M_0) = H(M_1) + H(M_0|M_1).$$

Тогда по «перехваченному» ПИМ M_1 соперник может получить информацию в количестве $I(M_1, M_0) = H(M_0) - H(M_0|M_1)$ *двед*. Для того чтобы обеспечить $I(M_1, M_0) = 0$, необходимо и достаточно, чтобы $H(M_0) = H(M_0|M_1)$ или, соответственно, $P(M_0) = P(M_0|M_1)$, что и требовалось доказать.

На практике для обеспечения условия (6) используются различные приёмы, в частности, так называемый способ «бегущего ключа», при котором поддерживается равенство скоростей V_{M1} передачи ПИМ M_1 и V_K передачи ключа K семантического преобразования $F(K)$ в ПИМ M_1, т. е.: $F(K)$: $M_0 \to M_2$.

***Утверждение* 3**. Необходимым и достаточным условием *энергетической* скрытности динамической информации (передаваемых ИМ) в информационно-распределительной сети эргасистемы является равенство

$$B >> (10...20), \qquad (7)$$

т. е. достаточно большая база $B = FT$ сигнала-переносчика ИМ M_0 длительностью T в полосе частот F, определяемая значением *удельного расхода* мощности $\beta^2 = (10...20)$, обеспечивающем необходимую (для каналов передачи данных) *верность* $q_1 \leq 10^{-5}$ приёма (см. рис. 4).

Доказательство. Искусственное увеличение полосы F частот согласно (7) позволяет уменьшить спектральную плотность (отношение мощности к полосе $N_с = P_с/F$ сигнала так, чтобы обеспечивалось неравенство $N_с << N_ш$, где $N_ш = P_ш/F$, и тем самым замаскировать сам факт передачи сигнала-переносчика ИМ M_0 в канале связи. При этом

$$\beta^2 = N_с/N_ш = P_с T/N_ш = P_с TF/N_ш F = (P_с/P_ш)B.$$

Отсюда: $P_с/P_ш = \beta^2/B \approx (10...20)/B$, т. е. для того чтобы обеспечить $P_с/P_ш << 1$, необходимо и до-

[9] *Шураков В. В.* Обеспечение сохранности в системах обработки данных. М. : Финансы и статистика, 1987. 272 с.

[10] *Ловцов Д. А.* Введение в информационную теорию АСУ : монография. М. : ВА им. Петра Великого, 1996. 434 с.

статочно обеспечить $B >> (10...20)$, что и требовалось доказать.

На практике для обеспечения условия (7) в качестве сигнала-переносчика используются так называемые сложные шумоподобные сигналы, обладающие большой избыточностью по полосе частот и длительности (например, с линейно-частотной модуляцией: $f_c = kt + f_0$; $F = k/T >> 1/T \rightarrow FT >> 1$), для которых T — длительность, соответствующая одному элементу $M_{1i} \in M_1$, $i=1,\ldots,N$ ПИМ, а F — полоса занимаемых частот. При использовании таких сигналов удается замаскировать их «белым» флуктуационным шумом с интенсивностью N_0 без ухудшения качества передачи сообщений (ИМ).

В разработке конкретных средств, методов и мероприятий защиты достигнуты наибольшие результаты, с помощью которых можно обеспечить требуемый уровень конфиденциальности ИМ в эргасистеме.

Отдельные разработки доведены до организации серийного выпуска или реализованы в виде общегосударственного стандарта. Например, ЭВМ, серийно выпускаемые американской фирмой IBM, содержат следующие средства защиты: схемы прерывания, позволяющие физически отделить исполнение программы оператора от исполнения управляющих процедур; блок защиты памяти, позволяющий контролировать и регулировать доступ оператора и задач к защищаемым полям памяти; специальные регистры защиты; программно-читаемые часы для регистрации времени свершения тех или иных событий и др.

В большинстве операционных систем современных ЭВМ предусматривается разграничение доступа к ИМ с помощью специальных паролей, четкое разделение ресурсов между решаемыми задачами, протоколирование информационно-вычислительного процесса и др.

Основные результаты, достигнутые в третьем направлении работ? — в обосновании способов использования методов, средств и мероприятий КЗИ от НСД и НСИ, — сводятся к следующим *выводам*:

ни один из способов, методов, мер, средств, мероприятий не является абсолютно надёжным, максимальный эффект достигается при объединении всех их в единую целостную подсистему ОКИ;

технические методы, меры и средства составляют лишь незначительную часть (около[11] 20%) подсистемы ОКИ (основную её часть составляют организационные);

подсистема ОКИ должна создаваться параллельно с эргасистемой, начиная с момента выработки общего замысла построения и проектирования последней;

выбор количества и содержания мероприятий ОКИ, а также способов их реализации осуществляется в каждом конкретном случае исходя из имеющихся средств и методов применительно к определённому КСА;

функционирование подсистемы ОКИ должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов переработки информации в эргасистеме;

необходимо осуществлять постоянный контроль функционирования подсистемы ОКИ со стороны администратора безопасности информации.

Набор $S_2 \in \Delta_2$ атрибутов доступа к ресурсам эргасистемы включает, в частности, множество $\Pi = <\Pi_1, \Pi_2, \ldots, \Pi_n>$ индивидуальных *паролей* $\Pi_i = \{x_{ij}\}$, $i=1,\ldots,n$; $j=1,\ldots,w_i$ (имён, алгоритмов, вопросов и др.) n объектов эргасистемы; множество $Э = <Э_1, Э_2, \ldots, Э_n>$ соответствующих эталонных паролей, преобразованных с целью защиты по соответствующему ключу $k \in K$ и хранящихся в специальной памяти эргасистемы; множество алфавитов $A = \{A_1(R_1), A_2(R_2), \ldots, A_L(R_L)\}$ различного размера R_l, $l=1,\ldots,L$ парольных символов $x_{ijl} \in A_l(R_l)$; определённое значение длительности цикла доступа $T = <t_и, t_x, t_о, t_п, t_з>$, включающей, в частности, время $t_и$ ввода имени объекта эргасистемы и время t_x ввода пароля, время $t_о$ отключения КСА в случае ошибочного (неверного) ввода, $t_п$ — печати сообщения об ошибке, $t_з$ — искусственной задержки начала следующей попытки; заданное значение числа f разрешённых попыток доступа.

В принятых обозначениях общую математическую постановку *задачи обеспечения конфиденциальности информации* как задачи поиска оптимального набора $S = <П, Э, K, A, T, f>$ атрибутов доступа, минимизирующего сумму $\Sigma_j c_j$ потерь от раскрытия (утечки) информации и затрат на разработку и эксплуатацию элементов КЗИ при ограничении на вероятность p_w НСД (раскрытия пароля) и на ожидаемое время $\check{T}_o$ безопасной работы, можно записать в виде:

$$\begin{aligned} &K: \Sigma_j c_j(S_2^*) = \min_{\{S2\}}, \\ &\quad p_w(S_2^*) \le p_w^0, \\ &\quad \check{T}_o(S_2^*) > \check{T}_o^0, \\ &\quad \Sigma_j c_j = c_1 + \check{c}_2 = c_1 + g(1 - p_w), \end{aligned} \tag{8}$$

где c_1 — затраты, связанные с разработкой и эксплуатацией элементов КЗИ; $\check{c}_2$ — математическое ожидание потерь, которое несёт эргасистема в результате раскрытия привилегированной информации; g — моральные и материальные потери эргасистемы от НСИ.

Решение задачи (8) возможно на основе известных методов математического программирования.

Принципы контроля и защиты информации от разрушающих факторов

Причины, вызывающие разрушение ИМ на физических магнитных носителях информации (МНИ), подразделяются на технологические и эксплуатационные, по наличию дефектов на МНИ. Технологические разрушающие факторы обусловлены показателями качества МНИ, несовершенством их производства, вследствие чего эти носители имеют заводские дефекты (повреждения магнитного слоя, надрывы кромки лент и др.).

[11] Ловцов Д. А. Введение в информационную теорию АСУ : монография. М. : ВА им. Петра Великого, 1996. 434 с.

Таблица 2

Эксплуатационные причины разрушения ИМ

Результат воздействия разрушающих факторов	Разрушающие факторы	
	Режим эксплуатации	
	Хранение ИМ на носителях	Непосредственное использование ИМ
Разрушение информационного массива	1. Ошибки персонала архивов МНИ. 2. Ошибки операторов КСА. 3. Агрессивность среды (температура, влажность, ЭМИ, помехи и др.).	1. Ошибки оператора КСА и пользователя (неправильная установка МНИ, повторные прогоны данных, использование не тех программ, запуск работы с неверного места, неправильный ввод задания и др.). 2. Несанкционированные и ошибочные корректировки пользователем записей и данных. 3. Деструктивные действия компьютерных вирусов. 4. Ошибки (всех видов) в КПС. 5. Сбой (отказ) КСА, ЭВМ, МНИ (не механической части) из-за скачков напряжения в сети питания, неисправностей энергоснабжения и др.). 6. Динамический перекос головок МНИ. 7. Катастрофический отказ ЭВМ, каналов связи и передачи данных, МНИ (случайное включение стирающей головки).
Разрушение магнитного носителя	1. Ошибки персонала КСА. 2. Износ МНИ (КТС). 3. Отпечатки на магнитной поверхности (FeO). 4. Вытягивание и продольное коробление (сабельность) МНИ.	1. Неправильное обращение с МНИ обслуживающего персонала. 2. Скол магнитной поверхности. 3. Обрыв, сдвиг витков или неровная намотка магнитных лент. 4. Глянцевые пятна, потертость или царапины на магнитной поверхности. 5. Неисправность лентопротяжных механизмов МНИ (механических частей). 6. Неисправность контроллеров МНИ, КТС.

Эксплуатационные разрушающие факторы (табл. 2) обусловлены неправильной (некомпетентной или недобросовестной) эксплуатацией МНИ и КСА в целом[12], в результате чего возможны механические повреждения, приводящие к выпадению сигналов при записи-считывании, искажения, модификация, разрушение ИМ и др.

Естественный износ МНИ (см. табл. 2) носит характер старения, когда с течением времени (5–10 лет и более) характеристики МНИ претерпевают «возрастные» изменения, приводящие к невозможности использования информации. Износ и старение, в частности, магнитных лент, широко используемых в архивах и дата-центрах, являются основными причинами потери информации при длительном хранении [5]. Увеличить срок сохранности ИМ можно, используя специальные процедуры чистки магнитных лент, их проверки и регенерации.

Проверка ИМ — процедура контроля путем записи-считывания информации для определения количества и местоположения ошибок. Если имеется возможность проверки ИМ и исправления искаженной информации, применяются специальные тестовые процедуры контроля, позволяющие уменьшать количество ошибок [5].

Регенерация ИМ — процедура перезаписи информации со старого МНИ на новый. При этом существует *рациональный* (оптимальный, удовлетворительный) *период* регенерации, при котором достигается минимум суммарных затрат на перезапись и потерь от уничтожения хранимой информации. В методах определения рациональных периодов регенерации ИМ используются известные[13] модели оптимизации регламентных и профилактических мероприятий.

При увеличении масштабов и сложности эргасистем усложняется работа операторов и организация разграничения доступа к ИМ и программно-техническим ресурсам. Поэтому возрастает доля разрушения информации вследствие ошибок операторов (использование ИМ не по назначению и др.) и несанкционированных корректировок. Ошибки операторов на этапе ввода и размещения исходных данных являются наиболее опасными, поскольку часто их обнаружение становится возможным спустя долгое время после их появления. Кроме того, операторы, имеющие доступ к ресурсам КСА, могут злонамеренно составить и использовать специальную машинную программу (ком-

[12] *Иыуду К. А.* Надёжность, контроль и диагностика вычислительных машин и систем. М. : Высшая школа, 1989. 216 с.

[13] Герцбах И. Б. Модели профилактики. М. : Сов. Радио, 1973. 250 с.

Рис. 8. Классификация способов и средств резервирования информационных массивов

пьютерный вирус и др.) для искажения или разрушения информационно-программного обеспечения КСА.

Способы резервирования ИМ с целью обеспечения сохранности информации включают (рис. 8):

оперативное (краткосрочное) резервирование — создание и хранение резервных рабочих копий и (или) *предысторий* ИМ, используемых только для решения функциональных задач эргасистемы;

восстановительное резервирование — создание и хранение дополнительных резервных (восстановительных) копий и (или) предысторий ИМ, используемых только для восстановления разрушенных рабочих копий и (или) предысторий ИМ;

долговременное (долгосрочное) резервирование — создание, длительное (десятки лет и более) хранение и обслуживание архивов оригиналов, дубликатов, резервных копий и (или) предысторий ИМ, используемых только для получения и восстановления разрушенных рабочих и дополнительных (восстановительных) копий и (или) предысторий ИМ.

Задачами *оперативного* резервирования ИМ являются определение (расчет) оптимального числа копий и (или) предысторий, обеспечивающих:

максимизацию коэффициента K_{Γ} готовности КСА переработки информации;

максимизацию вероятности $p_{\text{с}}(T)$ сохранности в заданном интервале времени T использования ИМ;

минимизацию суммарных эксплуатационных затрат $\Sigma_j c_j$ эргасистемы и др.

Основными задачами *восстановительного* резервирования ИМ являются [5]:

определение областей наиболее эффективного его использования при различных условиях эксплуатации КСА;

определение типа носителей информации для размещения восстановительного резерва;

выбор оптимальных методов и структур восстановления потерянной информации;

выбор оптимальных стратегий резервирования с учетом возможности восстановления разрушенных ИМ.

Основными задачами *долговременного* резервирования ИМ являются [5]:

определение (расчет) рационального (необходимого) числа копий и (или) предысторий ИМ, обеспечива-

ющих заданный уровень вероятности сохранности ИМ-*оригинала* (основного ИМ);

создание и организация функционирования специализированных хранилищ и архивов МНИ (периодических проверок работоспособности, регенерации ИМ и др.);

определение оптимальных периодов создания долгосрочного восстановительного резерва.

Обоснованное комбинирование комплектов генерируемых копий, предысторий и дубликатов ИМ с учетом параметров режима (переходный, установившийся и др.) работы КСА позволяет реализовать рациональные (экономичные, оперативные и др.) ситуационные стратегии резервирования постоянных и текущих данных.

Общую математическую постановку з*адачи обеспечения сохранности информации* (ОСИ) как задачи поиска оптимальной стратегии S_3 сохранения и подготовки ИМ (т. е. определения схем восстановления и регенерации ИМ, выбора методов резервирования ИМ, обнаружения и исправления ошибок и др.), которая обеспечивает максимизацию вероятности p_z успешного решения частной задачи эргасистемы при ограничении на среднее время $t'_{\text{ф}}$ функционирования КСА и суммарные потери и затраты $\Sigma_j c_j$, можно представить в виде:

$$K\colon p_z(S_3^*) = \max_{\{S3\}},$$
$$t'_{\text{ф}}(S_3^*) \le t'^{\,0}_{\text{ф}}, \quad (9)$$
$$\Sigma_j c_j(S_3^*) \le C_3^{\,0},$$
$$\Sigma_j c_j = c_1 + \check{c}_2 = \{s_1(t'_{\text{ф}} - \theta) + s_2(n)\} + \quad (10)$$
$$+ s_3(1 - p_z),$$

где c_1 — затраты, связанные с резервированием ИМ; $\check{c}_2$ — математическое ожидание потерь, которые несет эргасистема в результате разрушения основного ИМ M_0 и его копий; s_1 — стоимость единицы машинного времени; $s_2(n)$ — стоимость материального носителя ИМ, зависящая от количества n запоминающих устройств для хранения копий либо предысторий ИМ M_0; s_3 — потери эргасистемы в результате разрушения ИМ M_0 и его копий; θ — время решения частной задачи эргасистемы.

Кроме того, эффективность применения различных стратегий $S_3 \in \Delta_3$ ОСИ часто определяется также с использованием следующих *показателей готовности* КСА переработки информации различного типа [5]:

– готовность в установившемся режиме — относительное время полезной работы КСА на достаточно большом интервале времени:

$$K_\Gamma = t'_{\text{ф}}/[t'_{\text{ф}} + (1 - p_z)t'_v], \quad (11)$$

где t'_v — среднее время восстановления КСА;

– готовность в заданном интервале — относительное время нахождения КСА в работоспособном состоянии на ограниченном интервале T времени функционирования:

$$K_\Gamma = (T - T_v)/T, \quad (12)$$

где T_v — суммарные затраты времени на восстановление КСА в интервале $[0, T]$;

– мгновенная готовность — вероятность того, что в произвольный момент времени КСА работоспособен:

$$K_\Gamma = 1 - Q(t), \quad (13)$$

где $Q(t)$ — вероятность того, что ИМ неработоспособен в момент времени t хранения;

– коэффициент эксплуатационной надёжности — вероятность решения задачи эргасистемы с учётом начального состояния КСА:

$$K_{\text{э}} = p_z K_\Gamma; \quad (14)$$

– коэффициент полезной работы, определяемый как отношение времени полезной работы КСА к суммарному времени доступа к КСА при решении задачи:

$$K_{\text{п}} = \theta/t'_{\text{ф}}. \quad (15)$$

Таким образом, рассмотрена непротиворечивая совокупность *принципов* КЗИ в эргасистеме, следование которым обеспечивает, как показала практика, необходимый уровень защищённости перерабатываемой информации от основных разрушающих факторов, ошибок переработки, несанкционированного доступа и использования на основе применения соответствующих *методов* КЗИ.

Литература

1. Анин Б. Ю. Защита компьютерной информации. СПб. : БХВ-Санкт-Петербург, 2016. 384 с.
2. Барсуков В. С., Водолазний В. В. Современные технологии безопасности. М. : Нолидж, 2014. 496 с.
3. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. М. : Горячая линия — Телеком, 2010. 272 с.
4. Дейт К. Дж. Введение в системы баз данных. М. : Изд. дом «Вильямс», 2005. 1328 с. ISBN 5-8459-0788-8.
5. Кульба В. В., Ковалевский С. С., Шелков А. Б. Достоверность и сохранность информации в АСУ. М. : Синтег, 2004. 496 с.
6. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : Росс. гос. ун-т правосудия, 2016. 316 с.
7. Ловцов Д. А. Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере. II. Качество информации // Правовая информатика. 2015. № 2. С. 53–61.
8. Ловцов Д. А. Информационная безопасность и нетрадиционные угрозы // Федеральный справочник. Т. 8. Оборонно-промышленный комплекс России. М. : Центр стратег. исследований, 2013. С. 507—512.
9. Ловцов Д. А. Информационная теория эргасистем : тезаурус. М. : Наука, 2005. 248 с.
10. Ловцов Д. А., Ермаков И. В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // НТИ. Сер. 2. Информ. процессы и системы. 2005. № 2. С. 1–7.

11. Ловцов Д. А., Ермаков И. В. Защита информации от доступа по нетрадиционным информационным каналам // НТИ. Сер. 2. Информ. процессы и системы. 2006. № 9. С. 1–9.
12. Ловцов Д. А., Князев К. В. Защищённая биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2013. № 1. С. 100–103; II. Качество информационно-математического обеспечения // Информация и космос. 2013. № 2. С. 95–100.
13. Ловцов Д. А., Терентьева Л. В. Правовое регулирование международных коммерческих электронных контрактов. Технологические и правовые аспекты электронной подписи // Lex russica. 2020. Т. 73. № 7. С. 115–126. DOI: 10.17803/1729-5920.2020.164.7.115-126.
14. Монахов М. Ю., Монахов Ю. М., Полянский Д. А. Модели обеспечения достоверности и доступности информации в информационно-телекоммуникационных системах : монография. Владимир : Изд-во ВлГУ, 2015. 208 с. ISBN 978-5-9984-0634-8.
15. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. М. : ДМК, 2017. 448 с.
16. Федосеев С. В. Применение современных технологий больших данных в правовой сфере // Правовая информатика. 2018. № 4. С. 50–58. DOI 10.21681/1994-1404-2018-4-50-58.

Рецензент: ***Цимбал Владимир Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, профессор кафедры автоматизированных систем управления Филиала Военной академии им. Петра Великого, г. Серпухов, Московская область, Российская Федерация.*
E-mail: tsimbalva@mail.ru

PRINCIPLES OF ENSURING INFORMATION SECURITY IN ERGASYSTEMS

Dmitrii Lovtsov, *Dr.Sc. (Technology), Professor, Meritorious Scientist 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, Russian Federation, Moscow.*
E-mail: *dal-1206@mail.ru*

Keywords: *ergasystem, information security, reliability, confidentiality, integrity, principles of ensuring, processing errors, destructive factors, unauthorised access and use, ways to protect information, mathematical structures.*

Abstract.
Purpose of the work: improving the scientific and methodological basis of the theory of information security in ergasystems.
Methods used: system analysis, pragmatic classification and mathematical modelling of the basic specific tasks of ensuring information security in ergasystems.
Results obtained: a justification is given for a consistent set of principles for information control and protection from processing errors, destructive factors, and unauthorised access and use, for a pragmatic classification of information processing errors, destructive factors, sources of potential information leaks as well as corresponding ways to protect information, mathematical structures for models of problems ensuring information reliability, confidentiality and integrity in ergasystems are defined, proofs for assertions on raising information reliability, on perfect semantic concealment and on energy concealment of dynamic information are given.
The obtained results are the conceptual basis for creating appropriate efficient information and mathematical support for control and protection of information in ergasystems.

References

1. Anin B. Iu. Zashchita komp'iuternoi informatsii. SPb. : BKhV-Sankt-Peterburg, 2016, 384 pp.
2. Barsukov V. S., Vodolaznii V. V. Sovremennye tekhnologii bezopasnosti. M. : Nolidzh, 2014, 496 pp.
3. Vorona V. A., Tikhonov V. A. Sistemy kontrolia i upravleniia dostupom. M. : Goriachaia liniia – Telekom, 2010, 272 pp.
4. Deit K. Dzh. Vvedenie v sistemy baz dannykh. M. : Izd. dom "Vil'iams", 2005, 1328 pp. ISBN 5-8459-0788-8.
5. Kul'ba V. V., Kovalevskii S. S., Shelkov A. B. Dostovernost' i sokhrannost' informatsii v ASU. M. : Sinteg, 2004, 496 pp.
6. Lovtsov D. A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : Ross. gos. un-t pravosudiia, 2016, 316 pp.

7. Lovtsov D. A. Lingvisticheskoe obespechenie pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. II. Kachestvo informatsii. Pravovaia informatika, 2015, No. 2, pp. 53—61.
8. Lovtsov D. A. Informatsionnaia bezopasnost' i netraditsionnye ugrozy, Federal'nyi spravochnik. T. 8. Oboronno-promyshlennyi kompleks Rossii. M. : Tsentr strateg. issledovanii, 2013, pp. 507—512.
9. Lovtsov D. A. Informatsionnaia teoriia ergasistem : tezaurus. M. : Nauka, 2005, 248 pp.
10. Lovtsov D. A., Ermakov I. V. Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme, NTI. Ser. 2. Inform. protsessy i sistemy, 2005, No. 2, pp. 1-7.
11. Lovtsov D. A., Ermakov I. V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam, NTI. Ser. 2. Inform. protsessy i sistemy, 2006, No. 9, pp. 1-9.
12. Lovtsov D. A., Kniazev K. V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy. Informatsiia i kosmos, 2013, No. 1, pp. 100-103; II. Kachestvo informatsionno-matematicheskogo obespecheniia. Informatsiia i kosmos, 2013, No. 2, pp. 95-100.
13. Lovtsov D. A., Terent'eva L. V. Pravovoe regulirovanie mezhdunarodnykh kommercheskikh elektronnykh kontraktov. Tekhnologicheskie i pravovye aspekty elektronnoi podpisi. Lex russica, 2020, t. 73, No. 7, pp. 115-126. DOI: 10.17803/1729-5920.2020.164.7.115-126 .
14. Monakhov M. Iu., Monakhov Iu. M., Polianskii D. A. Modeli obespecheniia dostovernosti i dostupnosti informatsii v informatsionno-telekommunikatsionnykh sistemakh : monografiia. Vladimir : Izd-vo VlGU, 2015, 208 pp. ISBN 978-5-9984-0634-8.
15. Petrov A. A. Komp'iuternaia bezopasnost'. Kriptograficheskie metody zashchity. M. : DMK, 2017, 448 pp.
16. Fedoseev S. V. Primenenie sovremennykh tekhnologii bol'shikh dannykh v pravovoi sfere. Pravovaia informatika, 2018, No. 4, pp. 50-58. DOI 10.21681/1994-1404-2018-4-50-58 .

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ВОПРОСЫ ВНЕДРЕНИЯ СТОЙКИХ ЧАСТНЫХ КРИПТОСИСТЕМ

*Гриднев В. А., Володин И. С., Желудкова А. М.**

***Ключевые слова**: правовое регулирование, защита информации, права человека, национальная безопасность, стойкое шифрование, честная криптосистема, шифрование с депонированными ключами, пороговые схемы разделения секрета, контроль аутентичности теней.*

Аннотация.

Цель работы: исследование задачи правового регулирования отношений в области стойкого шифрования личной информации граждан в различных странах и способов ее решения.

Метод: системный организационно-правовой анализ влияния нормативно-правового обеспечения на развитие частных криптографических систем.

Результаты: рассмотрена оценка степени влияния нормативных правовых документов и законодательных актов на развитие криптографических систем для частного использования; обоснована наиболее перспективная технология развития систем депонированного шифрования личной информации граждан, основанная на реализации пороговой схемы разделения секрета с возможностью контроля аутентичности теней ключа шифрования.

DOI:10.21681/1994-1404-1-51-60

Введение

Вплоть до 90-х годов XX в. стойкое компьютерное шифрование использовалось по большей части национальными правительствами и крупными компаниями. Однако в июне 1991 г. американский программист Фил Циммерман, убежденный в необходимости защиты электронной почты от перехвата, открыл шифрование онлайн-коммуникаций частным лицам, поместив разработанную им программу *PGP* на электронной доске объявлений *Usenet*. С этого момента доступ к устойчивой криптографии получил любой желающий, и вокруг права на шифрование разгорелась дискуссия, которая фактически свелась к вопросу о том, должны ли правительства законодательно запретить использование стойкой криптографии своим гражданам или же нет. Споры не утихают по сей день[1] [1].

Убежденность правозащитников в необходимости доступа частных лиц к шифрованию основывается на ст. 12 Всеобщей декларации прав человека 1948 г.[2]: *«Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту от такого вмешательства или таких посягательств».* Аналогичные нормы закреплены в п. 1 ст. 8 Конвенции о защите прав человека и основных свобод 1950 г., ст. 17 Международного пакта о гражданских и политических правах 1966 г. и иных международных договорах.

Но практически в любом государстве, в том числе и в России, есть серьезные основания полагать, что широкое использование криптографии может содейство-

[1] Advances in Cryptology — CRYPTO '92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992. Proceedings [Текст]. Springer, 2003. 593 p.; Правовое регулирование шифрования онлайн-коммуникаций. URL https://digitalrights.center/blog/pravovoe-regulirovanie-shifrovaniya-onlayn-kommunikatsiy/ (дата обращения 10.12.2020).

[2] Всеобщая декларация прав человека. М.: Права человека, 1996. — 16 с.

* ***Гриднев Виктор Алексеевич,*** *кандидат технических наук, доцент кафедры информационных систем и защиты информации Тамбовского государственного технического университета, Российская Федерация, г. Тамбов.*
E-mail: vikadres@yandex.ru

Володин Иван Сергеевич, *студент Тамбовского государственного технического университета, Российская Федерация, г. Тамбов.*
E-mail: ivolodin98@gmail.com

Желудкова Анастасия Михайловна, *студент Тамбовского государственного технического университета, Российская Федерация, г. Тамбов.*
E-mail: anasanutasia@gmail.com

вать преступным и террористическим организациям. Поэтому во многих законах прописано, чтобы надлежащее государственное учреждение при обстоятельствах, разрешенных законом, в рамках своей работы могло получить открытый текст любого шифрованного сообщения. В настоящее время это требование выражается в принуждении граждан к использованию слабых криптосистем, т. е. таких, которые надлежащие органы власти (но, естественно, и все желающие) могут взломать с умеренными усилиями, либо к раскрытию секретного ключа шифрования органам власти.

Приведем цитату из «Книги шифров» Саймона Сингха, в которой автор приводит аналогию, сформулированную Роном Ривестоном, одним из создателей алгоритма шифрования *RSA*: «*Плохо без разбора запрещать технологию только потому, что некоторые преступники могут использовать ее в своих целях. Так, любой гражданин США может свободно купить пару перчаток, даже при том, что ими мог бы воспользоваться грабитель, чтобы обчистить дом, не оставив отпечатков пальцев. Криптография — это средство для защиты данных, точно так же, как перчатки — средство для защиты рук. Криптография защищает данные от хакеров, корпоративных шпионов и мошенников, в то время как перчатки предохраняют руки от порезов, царапин, жары, холода, инфекции. Первая может воспрепятствовать ФБР прослушивать телефонные разговоры, а вторые — помешают ФБР найти отпечатки пальцев. И криптография, и перчатки — они дешевле пареной репы и есть везде*» [10].

В Российском законодательстве пока еще не отражена такая тема, как собственноручная передача ключей шифрования спецслужбам со стороны граждан и организаций [6]. Но эта идея активно обсуждается. Она не вызывает недовольства у производителей — им не придётся вносить никаких доработок в свои продукты. Проект не очень-то масштабируем[3], но это не помешало некоторым государствам вместо депонирования ключей внедрить способ законного получения ключей от самих пользователей по требованию правоохранительных органов. В противном случае гражданам грозит уголовная ответственность за отказ в помощи следствию. В России таких норм на данный момент нет.

Законодательство и криптография

В России данная тема пока не актуальна, ключи у нас сейчас требуют только от операторов распространения информации, зарегистрированных в специальном реестре ФСБ, а простые граждане пока ограничены только Законом о лицензировании отдельных видов деятельности[4]. На рис. 1 приведены примеры государств, которые ввели у себя законы о передаче ключей шифрования (по данным английской Википедии, ссылающейся на законодательные акты соответствующих стран).

В Латвии в ноябре 2015 г. стало известно о готовящихся поправках в Уголовный кодекс, которые могут ввести наказание за использование программного обеспечения, препятствующего работе спецслужб[5].

Франция, посмотрев на предыдущий опыт США, попыталась в конце 20 в. внедрить у себя систему депонирования ключей. Премьер-министр Жоспен выразил желание внедрить данную систему, но уже через пару месяцев все работы по этому вопросу были прекращены. Министр внутренних дел Франции Бернар Казнев, ссылаясь на террористическую опасность, выступил за ограничение коммуникаций, защищенных *сквозным (оконченным)* шифрованием[6].

Йемен выступил с заявлением о своей собственной системе депонирования в 1997 г., правда, спустя год был объявлен перенос разработок на более дальний срок и по факту проект был заморожен [11].

В Великобритании с 2000 г. действует Акт «О правовом регулировании следственной деятельности» (*Regulation of Investigatory Powers Act* 2000), обязывающий пользователей систем шифрования по требованию властей предоставлять необходимые для расшифровки информации ключи и пароли. Отказ выполнить эти требования влечет за собой уголовное преследование[7].

В 2014–2016 гг. дискуссия о праве на шифрование и анонимность в Интернете достигла международного уровня. Проанализировав особенности и мотивы использования технологий шифрования в контексте основных прав человека, ООН признала анонимность в Интернете необходимым условием осуществления прав на свободу слова в цифровую эпоху[8].

В докладе Специального докладчика ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Дэвида Кея[9] дается оценка и интерпретация правам пользователей на шифрование в контексте основных прав и свобод человека, гарантируемых Международным пактом о гражданских и политических правах 1966 г. Основные его тезисы имеют принципиальное значение для понимания правового статуса шифрования в цифровой век.

---

[3] Из-за различий в законодательствах государств проблематично обеспечить широкое применение разработанного прикладного программного обеспечения, что неизбежно приводит к его удорожанию.

[4] Федеральный закон РФ от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» СПС «КонсультантПлюс».

[5] Сильная криптография. URL: https://ru.qaz.wiki/wiki/Strong_crypto-graphy (дата обращения 25.10.2020).

[6] Там же.

[7] History of cryptography. URL: https://en.wikipedia.org/wiki/History_of_ cryptography (дата обращения 11.10.2020).

[8] Правовое регулирование шифрования онлайн-коммуникаций. URL: https://digitalrights.center/blog/pravovoe-regulirovanie-shifrovaniya-onlayn-kommunikatsiy/ (дата обращения 10.12.2020).

[9] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Дэвида Кея 22 мая 2015 г. №A/HRC/29/32. URL: https://undocs.org/ru/A/HRC/29/32 (дата обращения 18.10.2020).

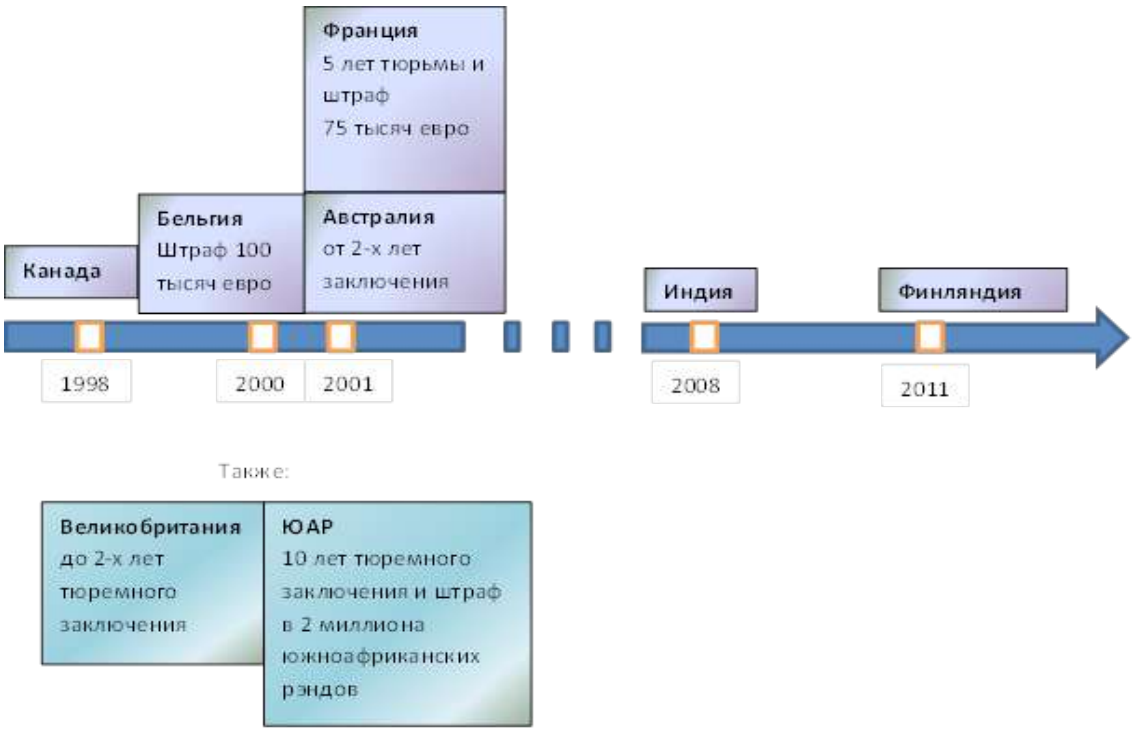


Рис. 1. Даты принятия законов и наказания за их несоблюдение

Сегодня в законах лишь некоторых стран официально содержатся статьи, регулирующие депонирование ключей. В Испании требуют разделять ключи для телекоммуникаций еще с 1998 г., но система так и не была принята для повсеместного использования. Великобритания в течение нескольких лет пыталась продвинуть политику, согласно которой национальные *удостоверяющие центры* могли получить соответствующую лицензию на работу только при условии получения приватных ключей у граждан. В конечном итоге от данной политики и в Великобритании тоже отказались.

В настоящее время в США нет никаких законов, обязывающих американских производителей внедрять какие-либо лазейки в подсистемы шифрования своих продуктов, так как это напрямую нарушает Пятую поправку к американской Конституции. Все вопросы по данной теме регулируются через суд, и результат всегда различается — некоторых принуждают предоставлять ключи, некоторых нет. Хотя в частном порядке такие системы разрабатывались, но не получили широкой огласки.

Итак, многие страны, не имея возможности требовать разделения ключей и не имея собственных разработчиков средств шифрования и телекоммуникационных средств, использующих криптографическую защиту, которые могли бы внедрить системы для восстановления ключей или иные лазейки, требуют от граждан и бизнеса предоставлять ключи шифрования по требованию государства[10].

Россия только встаёт на этот путь (началом можно считать закон, который в народе назвали по имени одного из инициаторов его принятия: «Пакет Яровой») и такие альтернативы тревожат многих активных граждан, считающих, что неприкосновенность частной жизни должна быть важнее национальной безопасности и задач правоохранительных органов.

Криптосистемы с депонированием ключей

Чтобы граждане могли воспользоваться всеми преимуществами сильной криптографии, совершенно не обязательно становиться на путь криптоанархии. Есть очень перспективная альтернатива — шифрование с депонированными криптоключами (или *депонированное шифрование*)[11] [9, 13]. Суть такого шифрования заключается в соединении преимуществ сильного шифрования и аварийного дешифрования. Стандартный ключ не должен быть тем ключом, который используется при нормальном дешифровании, однако он должен обеспечивать доступ к такому ключу по решению суда. Ключ дешифрования разделяется на части и находится у доверенных лиц, которыми могут быть государственные службы, суд, нотариусы или даже частные компании. Организации, являющиеся агентами по депонированию, могут также иметь собственные средства и ключи для аварийного дешифрования. Правоохранительные органы для получения доступа к зашифрован-

[10] Сильная криптография. URL: https://ru.qaz.wiki/wiki/Strong_cryptography (дата обращения 25.10.2020).

[11] Micali S. Fair Public-Key Cryptosystems, «Advancesin Cryptology CRYPTO '92» Proceedings, Springer-Verlag, 1993, pp. 113-138.

ной информации должны обратиться в суд и получить ордер на получение ключа для дешифровани.

Высказанная выше идея не нова. Впервые вопрос о депонировании ключей был поднят в США в 1992 г. Эта система позволяла бы спецслужбам получать доступ к защищенным перепискам граждан для проведения расследования. Изначально было задумано, что такую возможность будут автоматически встраивать во все устройства шифрования, разрабатываемые в то время в США. Альтернативным решением была идея встраивать в телекоммуникационные средства специальные потайные ходы, которые позволяли бы расшифровать данные переписки даже без знания ключа.

Администрация президента Клинтона вынесла предложение использовать специально спроектированный при сотрудничестве *NSA* и *NIST* чип *Clipper*, который мог использовать новый на то время криптографический алгоритм *Skipjack*, созданный для замены *DES*[12] [2]. Ключ в 80 бит у *Skipjack* считался более надежным, чем 56 бит у *DES*, однако для восстановления данных государство обязывало хранить все ключи в специальной закрытой базе данных. Технология разделения ключа была вшита в чип по умолчанию, и производители, которые будут встраивать чип в свои устройства, должны будут дополнительно передавать ключи для дешифрования в соответствующие органы. Для того чтобы продвинуть чип *Clipper* на рынке, администрация Клинтона планировала оснастить все телефоны и компьютеры, используемые в государственных учреждениях, этим чипом, создав большой госзаказ для снижения конечной стоимости продукта.

Несмотря на принятые меры, инициатива администрации президента по внедрению чипа *Clipper* предсказуемо встретила, как и следовало ожидать, сильное недовольство со стороны американского бизнеса и общественности, которое сопровождалось тремя ключевыми тезисами:

- использование чипа *Clipper* приводит к нарушению конституционных прав граждан на тайну переписки и личной жизни;
- защищенность базы данных с ключами для дешифрования не гарантирует невозможность её взлома и утечки ключей [4];

алгоритм *Skipjack* был секретным и частные эксперты не могли провести анализ на предмет уязвимостей и незадокументированных возможностей. У экспертов возникли явные подозрения, что кроме базы данных ключей алгоритм содержит дополнительные лазейки, которые позволили бы расшифровывать данные даже без знания ключа[13].

В конечном итоге инициатива с чипом *Clipper* провалилась, но провал не смог остановить администрацию Клинтона и в 1995 г. она выпустила обновленный план *Clipper* II. В новой редакции программы *Clipper* допускалось хранение баз ключей у частных независимых организаций, к которым сотрудники спецслужб все равно могли получить полный доступ.

В 1996 г. 20 мая был выпущен документ под названием *Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure*, который критики без промедления прозвали *Clipper* III. Этот проект выделялся от предыдущих большей интеллектуальностью — в нём не использовались никакие дополнительные чипы в устройствах, идея которых была изначально мёртвой. Вместо этого была предложена новая система управления ключами, которая давала простым гражданам и частному бизнесу легкий способ подтверждения сертификатов открытых ключей, так нужных в электронной коммерции. По сути, речь шла о *федеральном удостоверяющем центре*, целью которого стало бы хранение ключей пользователей в базе данных. Эксперты полностью раскритиковали и эту идею, как и две предыдущие [1].

В 1996 г. 1 октября администрация Клинтона снова выступила с новой инициативой, которая должна была вступить в силу с 1 января 1997 г. Планировалось передать ответственность за экспорт криптографии из Министерства юстиции в Министерство торговли. Длина ключей, которые были разрешены к экспорту без ограничений, была увеличена с 40 до 56 *бит*. Кроме того, производители получили бы право экспортировать и более сильные криптографические средства, получая специальное разрешение в Министерстве торговли. Однако на деле снова было одно очень отталкивающее ограничение — разрешение на экспорт сопровождалось требованием встроить в механизмы шифрования средство для восстановления ключей, которое позволило бы спецслужбам снова получить полный доступ к защищённым данным. Как и следовало ожидать, данная инициатива была опять встречена очень негативными отзывами со стороны производителей, и администрация Клинтона, наконец, устав бороться с противниками усиления национальной безопасности, передала все полномочия по всем вопросам, связанным с криптографией, в Конгресс[14].

Прошло немного времени, и на рассмотрение в Конгресс был выдвинут проект закона *Security and Freedom Through Encryption Act* (*SAFE*), который установил некоторые спорные с точки зрения правозащитников положения:

- запрещено требовать от американских производителей встраивать в свои продукты в механизмы для разделения или восстановления ключа;

[12] McCullough B. The NSA tried this before — what the 90s debate over the clipper chip can teach us about digital privacy. URL: http://www.internethistorypodcast.com /2014/08/the-nsa-tried-this-before-what-the-90s-debate-over-the-clipper-chip-can-teach-us-about-digital-privacy-de-bates/ (дата обращения: 10.10.2020); Ловцов Д. А. Контроль и защита информации в АСУ. М.: ВА им. Петра Великого, 1991. 172 с.

[13] Там же.

[14] Правовое регулирование шифрования онлайн-коммуникаций. URL: https://digitalrights.center/blog/pravovoe-regulirovanie-shifrovaniya-onlayn-kommunikatsiy/ (дата обращения 10.12.2020).

- на территории США разрешено производство, распространение и использование любых средств шифрования, независимо от используемых алгоритмов и размера ключей (по принципу «бизнес-выбора» [3]);
- разрешено производить на экспорт криптографические средства, если на международном рынке присутствует схожий продукт;
- запрещено использовать средства шифрования для незаконных целей.

Интересный факт: в одну из версий данного закона предлагали включить пункт, гласящий, что любое импортируемое в США криптографическое оборудование или программное обеспечение должно иметь возможность восстановления ключей шифрования, но данная норма, естественно, не была принята. Сегодня в США на импортированные средства шифрования нет никаких ограничений.

Законопроект *SAFE* рассматривался в Конгрессе около 2 лет, но так и не был принят. Впоследствии в Конгресс было внесено большое число новых законов, которые пытались узаконить требования по вопросам применения и экспорта шифровальных средств, среди них:

- *The Promote Reliable Online Transactions to Encourage Commerce and Trade (PROTECT) Act;*
- *The Electronic Rights for the 21stCentury Act;*
- *The Encryption for the National Interest Act;*
- *The Secure Public Networks Act* и др.

Но ни один из разработанных законопроектов так и не был подписан Президентом США. С 2001 г. ни один законопроект на данную тематику так и не был вынесен на обсуждение в Конгресс.

В 1998 г. в регламент экспорта шифровальных средств были внесены некоторые исправления, которые установили точный список стран и индустрий, в которые можно экспортировать американские шифровальные средства без ограничений, в иных случаях Министерство торговли США должно было выдавать специальное разрешение. Требования к системам депонирования ключей стали ниже, а позднее, в 2000 г., и вовсе были сняты. Все это было связано не только с препятствиями, с которыми столкнулась администрация Клинтона, но и с подписанием в декабре 1996 г. Вассенарских (Нидерланды, г. Вассенар) соглашений[15]. Принятые договоренности, по сути, полностью запретили разделение ключей для дешифрования. США попытались получить некоторые льготы и послабления на экспорт средств, отнесенных к технологиям, предназначенным для военного и гражданского использования, но им это не удалось. В итоге США пришлось полностью отказаться от своих планов, потому что эксперты в рабочей группе не смогли прийти к единому соглашению.

Возможные перспективы частной криптографии

Идея возможности использования сильной криптографии в частных целях впервые была предложена в 1993 г. Сильвио Микали, американским ученым в области теории вычислительных систем, лауреатом премии Геделя 1993 г. и премии Тьюринга 2012 г. Свою идею он назвал *"честной криптосистемой"*. Она заключается в создании криптосистемы, которая может обеспечивать хороший баланс между потребностями правительства и потребностями граждан. Честные криптосистемы гарантируют [4] две вещи:

1. конфиденциальность законопослушного пользователя не может быть нарушена;
2. злоумышленники не могут рассчитывать на конфиденциальность[16].

В честной криптосистеме есть фиксированное количество заранее назначенных доверенных лиц и произвольное количество пользователей. Доверенными лицами могут быть федеральные судьи, нотариусы, а также различные общественные организации, такие как группа гражданских прав, или компьютеры, контролируемые ими и оснащенные прикладным программным обеспечением, специально созданным для этой цели. Доверенные лица вместе с отдельными пользователями и центром распределения ключей играют решающую роль в уровне доверия честным криптосистемам[17].

Данная схема может быть усовершенствована использованием пороговой схемы разделения секрета, позволяющей восстановить разделенный секрет по k из n частей (теней). Пользователь может создать свой собственный закрытый ключ и распределить его части среди n доверенных лиц. Ни один из них не может восстановить закрытый ключ. Однако каждый может проверить аутентичность своей части (тени) закрытого ключа[18] [13].

Если судебные власти разрешат подслушивание, соответствующие правоохранительные органы смогут воспользоваться постановлением суда для того, чтобы любые k из n доверенных лиц выдали свои тени ключа. Собрав нужное количество частей, власти восстановят закрытый ключ и смогут подслушивать линии связи пользователя. С другой стороны, чтобы получить возможность восстановить ключ пользователя и нарушить тайну личности, злоумышленнику придется подкупить нужное количество доверенных лиц [9].

Для конкретности рассмотрим принципы построения пороговой схемы разделения секрета два из трех: <2; 3>.

[15] Вассенарские договоренности (33 страны) по экспортному контролю за обычными вооружениями, товарами и технологиями двойного назначения. URL: https://www.wassenaar. org/ru/ (дата обращения 18.12.2020).

[16] Micali S. Fair Public-Key Cryptosystems, «Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 113-138.

[17] Там же.

[18] Shamir A. How to share a secret [Электронный ресурс] / Communications of the ACM. 1979. Vol. 22, No. 11. URL: https://dl.acm.org/doi/10.1145/359168.359176 (дата обращения 12.11.2020).

Программный модуль вычисления теней создает 3 тени секретного ключа пользователя для последующей их передачи нотариусам и формирует электронную подпись пользователя к каждой тени. Разделение производится таким образом, что:

- для восстановления секрета достаточно двух теней;
- одна сторона не сможет получить никакой информации о секрете.

Такое разделение осуществляется с помощью схемы интерполяционных полиномов Лагранжа (схемы разделения секрета Шамира или схемы Шамира) — схемы разделения секрета, широко используемой в криптографии [13].

Для интерполяции многочлена степени k–1 требуется k точек. Основная идея данной схемы состоит в том, что интерполяция невозможна, если известно меньшее число точек[19]. Например, многочлен степени 1 представляется графически как прямая линия на плоскости и для его восстановления требуется знать значение функции в двух точках (рис. 2). Искомым секретом в данном случае является значение полинома в точке $x = 0$.

Необходимо разделить секрет M между тремя сторонами таким образом, чтобы любые два участника могли восстановить секрет, т. е. нужно реализовать <2; 3>-пороговую схему.

Выберем некоторое простое число $p > M$. Это число можно открыто сообщать всем участникам. Оно задает конечное поле размера p. Над этим полем построим линейное уравнение, т. е. случайно выберем все коэффициенты многочлена, кроме M:

$$F(x) = (a_1 \cdot x + M) \bmod p. \quad (1)$$

В этом многочлене M — это разделяемый секрет; a_1 — некоторое случайное число, которое нужно будет «забыть» после того, как процедура разделения секрета будет завершена.

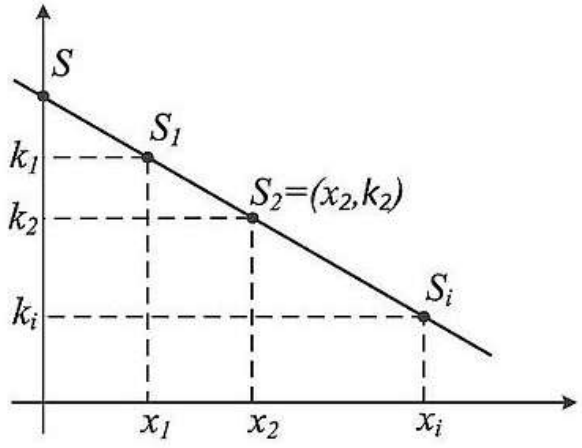


Рис. 2. Графическое представление разделения секрета <2; 3>

Теперь вычисляем «тени» — значения построенного выше многочлена в трех различных точках, причем $x \neq 0$:

$$\begin{aligned} k_1 &= F(1) = (a_1 \cdot 1 + M) \bmod p; \\ k_2 &= F(2) = (a_1 \cdot 2 + M) \bmod p; \\ k_3 &= F(3) = (a_1 \cdot 3 + M) \bmod p. \end{aligned} \quad (2)$$

Аргументы многочлена (номера теней) не обязательно должны идти по порядку, главное — чтобы все они были различны по модулю p.

После этого каждой стороне, участвующей в разделении секрета, выдается доля секрета — тень k_i вместе с номером i. Помимо этого, всем сторонам сообщается степень k–1 многочлена (1) и размер поля p. При этом число p должно быть простым и меньше основного секрета M. Случайный коэффициент a_1 и сам секрет M «забываются»[20].

Для того чтобы нотариус впоследствии мог удостовериться в аутентичности доверенной ему тени, после ее формирования происходит вычисление электронной подписи к этой тени с использованием закрытого ключа пользователя, выдаваемого удостоверяющим центром. Кроме того, использование электронной подписи предоставляет возможность обеспечить следующие свойства при передаче или хранении в системе подписанной тени:

- осуществление контроля *целостности* подписанной тени;
- доказательное подтверждение авторства лиц, подписавших сообщение;
- защита тени от возможной модификации или подмены.

Схематическое представление подписанного сообщения показано на рис. 3 [10].

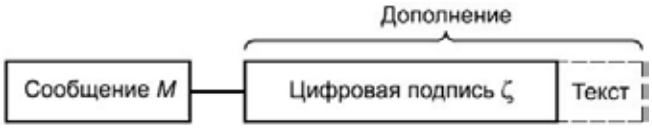


Рис. 3. Структура подписанного сообщения

Под сообщением здесь понимается одна из теней ключа шифрования. Цифровая подпись — это число фиксированной длины, однозначно зависящее от подписываемого сообщения (тени ключа шифрования) и секретного ключа субъекта подписи. Поле «Текст», показанное на рис. 3 и дополняющее поле «Цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени [10].

В качестве алгоритма вычисления электронной подписи можно использовать алгоритм ГОСТ Р 34.10-2012[21].

[19] Shamir A. How to share a secret [Электронный ресурс] / Communications of the ACM. 1979. Vol. 22, No. 11. URL: https://dl.acm.org/doi/10.1145/359168.359176 (дата обращения 12.11.2020)..

[20] Там же.

[21] ГОСТ 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции [5, 7]. Алгоритм вычисления хэш-функции установлен ГОСТ Р 34.11-2012[22].

Сгенерированная тень вместе с электронной подписью пользователя записывается на съемный носитель, предъявляемый нотариусу, либо пересылается доверенным лицам по защищенному каналу связи, а затем гарантированно стирается из памяти устройства.

Для того чтобы нотариус мог удостовериться в аутентичности вручаемой ему тени ключа, нужно специальное прикладное программное обеспечение. Назовем его *модулем проверки корректности теней*.

Так как модуль генерации ключа шифрования совместно с модулем вычисления теней составляют один программно-аппаратный комплекс, вероятность ошибки которого крайне мала, проверка нужна для того, чтобы удостовериться в целостности и аутентичности тени ключа. Это позволяет, с одной стороны, исключить возможность подмены тени, вручаемой нотариусу, а с другой стороны — проверить аутентичность тени, получаемой представителем спецслужбы государства у нотариуса.

Модуль восстановления ключа должен быть в составе информационной системы спецслужб. Он используется, когда нужно восстановить секретный ключ пользователя с разрешения суда. При этом над любыми двумя из трех теней выполняется преобразование, результатом которого является восстановленный ключ.

Зная координаты k (двух) различных точек многочлена, можно восстановить многочлен, включая и свободный член — разделяемый секрет. Для этого можно использовать интерполяционный полином Лагранжа:

$$F(x) = \sum_i l_i(x) y_i (mod\ p),$$
$$l_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} (mod\ p). \quad (3)$$

Обозначения переменных в выражении (3) аналогичны обозначениям в выражении (1).

Особенностью схемы является то, что вероятность раскрытия секрета в случае произвольных k–1 теней (в рассматриваемом случае это будет одна тень) оценивается как p^{-1}. То есть в результате интерполяции по k–1 точкам секретом может быть любой элемент поля с равной вероятностью. При этом попытка полного перебора всех возможных теней не позволит злоумышленникам получить дополнительную информацию о секрете.

Перед непосредственным восстановлением ключа должны быть проверены электронные подписи теней, полученных от нотариусов.

Общая схема взаимодействия субъектов в рассматриваемой системе может быть такой, как описано ниже. Модуль генерации ключа шифрования и модуль вычисления теней составляют один программно-аппаратный комплекс. Он должен быть расположен в защищенном помещении в пределах контролируемой зоны *центра распределения ключей* [3].

Если пользователь желает использовать честную криптосистему, он должен обратиться в центр распределения ключей и подать заявку, указав в ней свои персональные данные (ФИО, серию и номер паспорта, номер телефона), и дожидаться ответа. Центр распределения ключей вносит эту информацию в базу данных, осуществляет выбор нотариусов и извещает участников (пользователя и нотариусов) о времени выдачи ключа шифрования и соответствующих теней. Все это можно сделать с помощью телекоммуникаций [8, 12]. Обеспечение безопасности (конфиденциальности, целостности и доступности) [3] передачи ключа и теней выходит за рамки данной статьи.

Стоит заметить, что данные нотариусов, как и пользователей, вносятся в базу данных центра распределения ключей, и после генерации ключа и распределения теней идентификаторы нотариусов будут включены в запись о соответствующем вручении ключа. Таким образом, в случае разрешения судом прослушивания линий связи пользователя, правоохранительные органы будут знать, у каких доверенных лиц находятся нужные тени.

Пользователь теперь может использовать надежный ключ шифрования, полученный в центре распределения ключей, а нотариусы будут хранить тени этого ключа в секрете.

Нотариус в любой момент может проверить электронную подпись тени, чтобы убедиться в том, что тень сгенерирована конкретным центром распределения ключей и не была модифицирована с момента ее создания. Для этого ему нужно знать открытый ключ центра распределения ключей и иметь программное обеспечение, позволяющее выполнять проверку электронной подписи. Это программное обеспечение представляет собой модуль проверки корректности тени.

В случае разрешения прослушивания судом правоохранительные органы смогут обратиться в центр распределения ключей и выяснить контактные данные нотариусов, которые хранят тени секретного ключа пользователя. Получение хотя бы двух из трех теней позволяет восстановить секрет с помощью модуля восстановления ключа, который также представляет собой специальное программное обеспечение.

Полученный в результате восстановления ключ дает возможность либо успешно расшифровать переписку пользователя, либо уличить его в использовании другого ключа, если электронные подписи всех теней проходят проверку подлинности. Если электронная подпись тени, полученной у нотариуса, не проходит проверку, значит, целостность тени была нарушена и поскольку тень находится у нотариуса, он несет ответственность за ее сохранность.

[22] ГОСТ 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.

Очевидных технических проблем реализации предложенной системы нет. Но у каждого пользователя существует принципиальная возможность, получив депонированный ключ шифрования, для реального информационного обмена использовать иной ключ. Поэтому законодательством должна быть предусмотрена строгая ответственность за такого рода правонарушения.

Заключение

Таким образом, широкое внедрение стойких криптосистем для защиты тайны частной жизни граждан, гарантированной Конституцией, в России, как и в других странах, сопряжено со многими трудностями, связанными прежде всего с обеспечением национальной безопасности. Наиболее перспективной, с учётом опыта других стран, представляется технология *депонированного шифрования*, дополненная пороговой схемой разделения секрета (схема Шамира). Но это, в свою очередь, требует разработки надёжных технических механизмов и юридических процедур, не позволяющих пользователям и доверенным органам подменять тени реальных ключей шифрования ложными файлами, которые не позволят соответствующим государственным органам восстановить реальные ключи даже после соответствующего решения суда. Такие механизмы и процедуры возможно установить в результате:

- принятия Федерального Закона РФ «О защите частной жизни граждан в информационном обществе»;
- внесения в КоАП РФ и в УК РФ изменений и дополнений, предусматривающих ответственность за недобросовестные действия при использовании депонированных ключей шифрования;
- издания Постановления Правительства РФ «О депонировании ключей шифрования личной информации граждан»;
- издания руководящего документа ФСБ России «Методика контроля корректности депонированных ключей шифрования личной информации граждан»;
- разработки, государственной сертификации и регистрации в Федеральном реестре прикладного программного обеспечения ЭВМ, позволяющего генерировать ключи шифрования и их тени, проверять аутентичность теней и восстанавливать ключи по нескольким теням из фиксированного множества (предпочтительно реализовать пороговую схему «два из трёх»).

К настоящему времени на кафедре информационных систем и защиты информации ФГБОУ ВО «Тамбовский государственный технический университет» разработано прикладное программное обеспечение ЭВМ, реализующее различные пороговые схемы разделения секрета.

Весь информационный обмен между субъектами взаимоотношений в данной системе можно реализовать в электронной форме, что неизбежно потребует принятия мер по обеспечению безопасности информации, передаваемой по каналам связи.

Литература

1. Алексеев В. В., Емельянов Е. В., Кастерин Д. А., Стрельцов А. А. Правовой подход к построению системы защиты информации в организации // Правовая информатика. 2020. № 2. С. 54–61. DOI:10.21681/1994-1404-2020-2-54-61.
2. Королев В. Т., Ловцов Д. А. Качество стандартизованной системы алгоритмов шифрования данных в ГАС РФ «Правосудие» // Правовая информатика. 2018. № 2. С. 49–59. DOI:10.21681/1994-1404-2018-2-49-59.
3. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере : монография. М.: РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
4. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66–74. DOI:10.21681/1994-1404-2017-3-66-74.
5. Ловцов Д. А. Информационная безопасность автоматизированных блокчейн-систем: угрозы и способы повышения // Тр. II Междунар. науч.-прак. конф. «Трансформация национальной социально-экономической системы России» (22 ноября 2019 г.) / РГУП. Москва: РГУП, 2020. С. 464–473. ISBN 978-5-93916-823-6.
6. Ловцов Д. А. Развитие информационной сферы общественно-производственной деятельности: достижения, угрозы безопасности и правовое регулирование // Государство и право в новой информационной реальности: Сб. науч. тр. / Отв. ред. Е. В. Алферова, Д. А. Ловцов. М.: ИНИОН РАН, 2018. С. 15–37. ISBN 978-5-248-00888-9.
7. Ловцов Д. А., Терентьева Л. В. Правовое регулирование международных коммерческих электронных контрактов. Технологические и правовые аспекты электронной подписи // Lex russica. 2020. Т. 73. № 7. С. 115–126. DOI: 10.17803/1729-5920.2020.164.7.115-126.
8. Ловцов Д. А., Кабелев Д. Б. Технология и проблемы рационального управления ключевой информацией в АСУ // Труды XXIX Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (24–25 июня 2010 г.) в 5-ми тт. Т. 4 / РАО. Серпухов: Серп. воен. ин-т, 2010. С. 144–148.
9. Мао В. Современная криптография: теория и практика. М.: Вильямс, 2005. 768 с.

10. Сингх С. Книга шифров: тайная история шифров и их расшифровки. М.: Аванта, 2009. 463 с.
11. Сунаид Х. А., Яковлев А. В. Состояние и перспективы развития государственной информационно-телекоммуникационной системы Йемена / Труды науч.-прак. конф. «Информационные системы и процессы» (15 июня 2018г.) / ТГУ. Тамбов: Междунар. информ. нобел. центр, 2018. С. 76–89.
12. Хучиров А. Г., Яковлев Ал. В., Яковлев Ан. В. Реализация метода кластерного анализа в математической модели процессов взаимообмена информационными ресурсами в автоматизированной системе управления специального назначения // Перспективы науки. Тамбов: «Фонд развития науки и культуры», 2017. №1. С. 75–79. ISS. 2077-6810.
13. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. М.: Вильямс, 2016. 1024 с.

Рецензент: ***Алексеев Владимир Витальевич,*** *доктор технических наук, профессор, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Россия.*
E-mail: vvalex1961@mail.ru

ORGANIZATIONAL AND LEGAL QUESTIONS OF IMPLEMENTING STRONG PRIVATE CRYPTOSYSTEMS

Victor Gridnev, *Ph.D., Associate, Associate Professor of the Department of Information Systems and Information Security, Tambov State Technical University, Russian Federation, Tambov.*
E-mail: *vikadres@yandex.ru*

Ivan Volodin, *student of the Tambov State Technical University, Russian Federation, Tambov.*
E-mail: *ivolodin98@gmail.com*

Anastasiya Zheludkova, *student of the Tambov State Technical University, Russian Federation, Tambov.*
E-mail: *anasanutasia@gmail.com*

Keywords: *legal regulation, information protection, human rights, national security, strong encryption, honest cryptosystem, encryption with escrow keys, threshold secret sharing schemes, control over the authenticity of shadows.*

Abstract.
Purpose of the work: to study the task of legal regulation of relations in the field of strong encryption of personal information of citizens in various countries and ways to solve it.
Method: system organizational and legal analysis of influence of normative and legal support on the development of private cryptographic systems.
Results: estimation of the degree of influence of regulatory documents and legislative acts on the development of cryptographic systems for private use is discussed; the most promising technology for the development of deposited encryption systems for personal information of citizens was substantiated, based on the implementation of a threshold secret sharing scheme with the ability to control the authenticity of the encryption key shadows.

References

1. Alekseev V. V., Emel`ianov E. V., Kasterin D. A., Strel`tcov A. A. Pravovoi` podhod k postroeniiu sistemy` zashchity` informatcii v organizatcii // Pravovaia informatika. 2020. № 2. S. 54-61. DOI:10.21681/1994-1404-2020-2-54-61.
2. Korolev V. T., Lovtcov D. A. Kachestvo standartizovannoi` sistemy` algoritmov shifrovaniia danny`kh v GAS RF «Pravosudie» // Pravovaia informatika. 2018. № 2. S. 49-59. DOI:10.21681/1994-1404-2018-2-49-59.
3. Lovtcov D. A. Sistemologiia pravovogo regulirovaniia informatcionny`kh otnoshenii` v infosfere : monografiia. M.: RGUP, 2016. 316 s. ISBN 978-5-93916-505-1.
4. Lovtcov D. A. Problema garantirovannogo obespecheniia informatcionnoi` bezopasnosti krupnomasshtabny`kh avtomatizirovanny`kh sistem // Pravovaia informatika. 2017. № 3. S. 66-74. DOI:10.21681/1994-1404-2017-3-66-74.
5. Lovtcov D. A. Informatcionnaia bezopasnost` avtomatizirovanny`kh blokchei`n-sistem: ugrozy` i sposoby` povy`sheniia // Tr. II Mezhdunar. nauch.-prak. konf. «Transformatciia natcional`noi` sotcial`no-e`konomicheskoi` sistemy` Rossii» (22 noiabria 2019 g.) / RGUP. Moskva: RGUP, 2020. S. 464-473. ISBN 978-5-93916-823-6.

6. Lovtcov D. A. Razvitie informatcionnoi` sfery` obshchestvenno-proizvodstvennoi` deiatel`nosti: dostizheniia, ugrozy` bezopasnosti i pravovoe regulirovanie // Gosudarstvo i pravo v novoi` informatcionnoi` real`nosti: Sb. nauch. tr. / Otv. red. E. V. Alferova, D. A. Lovtcov. M.: INION RAN, 2018. C. 15-37. ISBN 978-5-248-00888-9.
7. Lovtcov D. A., Terent`eva L. V. Pravovoe regulirovanie mezhdunarodny`kh kommercheskikh e`lektronny`kh kontraktov. Tekhnologicheskie i pravovy`e aspekty` e`lektronnoi` podpisi // Lex russica. 2020. T. 73. № 7. S. 115-126. DOI: 10.17803/1729-5920.2020.164.7.115-126.
8. Lovtcov D. A., Kobelev D. B. Tekhnologiia i problemy` ratcional`nogo upravleniia cliuchevoi` informatciei` v ASU // Trudy` XXIKH Vseross. nauch.-tekhn. konf. «Problemy` e`ffektivnosti i bezopasnosti funktcionirovaniia slozhny`kh tekhnicheskikh i informatcionny`kh sistem» (24–25 iiunia 2010 g.) v 5-mi tt. T. 4 / RAO. Serpuhov: Serp. voen. in-t, 2010. S. 144-148.
9. Mao V. Sovremennaia kriptografiia: teoriia i praktika. M.: Vil`iams, 2005. 768 s.
10. Singkh S. Kniga shifrov: tai`naia istoriia shifrov i ikh rasshifrovki. M.: Avanta, 2009. 463 s.
11. Sunaid KH. A., Iakovlev A. V. Sostoianie i perspektivy` razvitiia gosudarstvennoi` informatcionno-telekommunikatcionnoi` sistemy` I`emena / Trudy` nauch.-prak. konf. «Informatcionny`e sistemy` i protcessy`» (15 iiunia 2018g.) / TGU. Tambov: Mezhdunar. inform. nobel. centr, 2018. S. 76-89.
12. Huchirov A. G., Iakovlev Al. V., Iakovlev An. V. Realizatciia metoda clasternogo analiza v matematicheskoi` modeli protcessov vzaimoobmena informatcionny`mi resursami v avtomatizirovannoi` sisteme upravleniia spetcial`nogo naznacheniia // Perspektivy` nauki. Tambov: «Fond razvitiia nauki i kul`tury`», 2017. №1. S. 75 — 79. ISS. 2077-6810.
13. Shnai`er B. Pricladnaia kriptografiia. Protokoly`, algoritmy` i ishodny`i` kod na C. M.: Vil`iams, 2016. 1024 s.

КРИТЕРИЙ «НАПРАВЛЕННОЙ ДЕЯТЕЛЬНОСТИ» ПРИМЕНИТЕЛЬНО К ОТНОШЕНИЯМ, СВЯЗАННЫМ С ЗАЩИТОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ[1]

Терентьева Л. В.*

Ключевые слова*: персональные данные, судебная юрисдикция, направленная деятельность, защита прав потребителей, экстратерриториальная юрисдикция, киберпространство, контролер, лицо, обрабатывающее персональные данные.*

Аннотация.

Цель работы: уточнение сферы распространения Закона РФ «О персональных данных» (2006 г.) и выявление соотношения сферы применения указанного закона с основанием установления юрисдикции российского суда, предусмотренного в п. 10 ч. 3 ст. 402 ГПК РФ.

Метод: сравнительно-правовой анализ законодательных и доктринальных подходов к определению понятия «направленная деятельность»: при установлении судебной юрисдикции по делу о защите персональных данных, определении сферы применения Закона РФ «О персональных данных», и применении механизма коллизионной защиты в отношении потребителя, предусмотренной в ст. 1212 ГК РФ.

Результаты: установлена необходимость дифференциации подходов к определению содержания критерия «направленной деятельности» как условия применения законодательства о персональных данных и как условия предоставления специальной коллизионной защиты потребителю, принимая во внимание отличный механизм защиты при поиске применимого права к потребительским договорам и распространения законодательства о персональных данных в отношении иностранных операторов; доказывается, что, принимая во внимание общие тенденции проявления экстратерриториальной законодательной (предписывающей) и судебной юрисдикции, основания распространения ФЗ «О персональных данных» должны совпадать с основаниями установления судебной юрисдикции по делу о защите прав субъекта персональных данных.

DOI:10.21681/1994-1404-2021-1-61-69

Масштабное развитие киберпространства [10] способствовало смешению границ национальных правовых пространств и количественному увеличению случаев установления экстратерриториальной юрисдикции.

Возможность наступления последствий на территории одного государства в результате принятия актов на территории других государств послужила обоснованием доктринальной позиции о том, что *концепции расширенной юрисдикции* становятся частью правовой системы России и многих других государств [1].

В этой связи критерий разграничения территориального или экстратерриториального проявления юрисдикции в современных условиях в большей степени становится зависимым не от четкой территориальной демаркации между государствами, а от того, затрагиваются ли значимые интересы одного государства в результате реализации юрисдикционных полномочий другого государства. Иллюстрацией установления экстратерриториальной предписательной юрисдикции может служить законодательство государств о *персональных данных*.

Закон Австралии о конфиденциальности (1988 г.) распространяется на любую организацию или оператора малого бизнеса, имеющих связь с Австралией, в частности, осуществляющих предпринимательскую деятельность в Австралии (*Sec*. 5*B*, *par*.3(*b*))[2]. Закон о защите персональных данных 2012 г. Сингапура распространяется на организации, собирающие персональные

[2] Privacy Act Australia of 1988. URL: https://www.legislation.gov.au/Details/C2014C00076// (дата обращения: 20.11.2020).

[1] Статья подготовлена при финансовой поддержке Российского фонда фундаментальных исследований в рамках научно-исследовательского проекта № 18-29-16061.

* ***Терентьева Людмила Вячеславовна,*** *кандидат юридических наук, доцент, доцент кафедры международного частного права Московского государственного университета имени О. Е. Кутафина, Российская Федерация, г. Москва.*

E-mail: terentevamila@mail.ru

данные физических лиц в Сингапуре, независимо от того, присутствует ли сама организация в Сингапуре[3].

Экстратерриториальная сфера действия была заложена и в Регламенте Европейского Парламента и Совета ЕС (2016 г.) о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (далее — Регламент о персональных данных)[4].

В ст. 3 Регламента, носящей название «территориальное действие», раскрывается как территориальная, так и экстратерриториальная сфера распространения Регламента в зависимости от того, учреждены ли контролер (оператор) или лица, обрабатывающие персональные данные, в Европейском союзе. В соответствии с п. 2 ст. 3 Регламента он применяется в отношении обработки персональных данных субъектов данных, находящихся в Союзе, контролером или обрабатывающим данные лицом, не учрежденными в Союзе, если обработка данных касается:

(*a*) предоставления товаров и услуг субъектам данных в Союзе вне зависимости от того, требуется ли оплата от указанного субъекта данных, или

(*b*) мониторинга их деятельности при условии, что деятельность осуществляется на территории Союза.

Обращение в Регламенте к такому критерию объясняется возможностью обработки персональных данных лиц, находящихся практически в любой точке мира, в результате использования *современных информационно-коммуникационных технологий* [6].

В соответствии с п. 23 и п. 24 Преамбулы Регламента, а также ст. 3 (*b*), 27 (3) Регламента о персональных данных под мониторингом деятельности субъектов понимается потенциальная возможность последовательного использования технологий обработки персональных данных, посредством которых осуществляется составление профиля физического лица, для принятия решений относительно анализа либо прогнозирования его личных предпочтений, особенностей поведения, а также личностных характеристик. Под мониторинг активности граждан попадает и использование файлов *cookies*[5].

В п. 23 Преамбулы Регламента о персональных данных поясняется, что для того, чтобы определить, предлагает ли контролер или оператор, обрабатывающий данные, товары или услуги субъектам данных, которые находятся в Европейском союзе, необходимо установить очевидность их намерения по предложению услуг субъектам данных в одном или нескольких государствах-членах Европейского союза. При этом одна лишь доступность интернет-сайта контролера или оператора, обрабатывающего данные, адреса электронной почты или иных контактных данных, или же использование языка государства, в котором учрежден оператор, не являются достаточными для обозначения намерения.

Намерение оператора предлагать товары или услуги субъектам данных в Европейском союзе в п. 23 Регламента обозначается в качестве возможности заказа товаров или услуг на языке, используемом в одном или нескольких государствах-членах Европейского союза, или использования валюты, распространенной в одном или нескольких государствах-членах Европейского союза. К числу факторов, указывающих на намерение оператора предлагать товары или услуги субъектам данных в Европейском союзе, также относятся упоминание покупателей или пользователей, находящихся в Европейском союзе.

Обозначение *намерения* предлагать товары или услуги не является принципиально новым для европейского законодательства. Такого рода критерий был использован применительно к потребительским отношениям в Регламенте Европейского парламента и Совета Европейского Союза 1215/2012 от 12 декабря 2012 г. «О юрисдикции, признании и исполнении судебных решений по гражданским и коммерческим делам» (далее — «Брюссель I *bis*»)[6] и в Регламенте Европейского Парламента и Совета Европейского Союза от 17 июня 2008 г. «О праве, подлежащем применению к договорным обязательствам» (далее — "Рим I")[7].

В соответствии с указанными регламентами факт осуществления «*направленной деятельности*» является основанием предоставления потребителю *защитной юрисдикции* и специального *коллизионного регулирования*. Само понятие «направленная деятельность» не раскрывалось ни в Регламенте "Брюссель I (*bis*)", ни в Регламенте "Рим I". Уточнение и конкретизация его содержания имели место в предложении Европейского парламента 1999 г.[8] и в совместном заявлении Совета и Комиссии в отношении применения ст. 15 Регламента (ЕС) № 44/2001 (ст. 17 в редакции от 12 декабря 2012 г.)[9].

[3] Personal Data Protection Act Singapore of 2012 (No. 26 of 2012)// Personal Data Protection Act of 2012 (No. 26 of 2012). URL: www.dlapiperdataprotection.com/index.html?t=law&c=SG. (дата обращения: 20.11.2020).

[4] General Data Protection Regulation (GDPR) // GDPR Archives. URL: GDPR.eu (дата обращения: 20.11.2020).

[5] Файлы cookies — это часть текстовых данных, хранящаяся в браузере. В них содержится информация, которую пользователь передает сайтам при их посещении. Именно она помогает запомнить все действия, чтобы при очередном входе на сайт облегчить навигацию. URL: proudalenku.ru) (дата обращения: 30.11.2020).

[6] Regulation (eu) no 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:en:PDF (дата обращения: 16.06.2020).

[7] Регламент Европейского Парламента и Совета Европейского Союза от 17 июня 2008 г. N 593/2008 «О праве, подлежащем применению к договорным обязательствам» // СПС «Гарант».

[8] European Parliament, "Proposal for a Council Regulation (EC) on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (Presented by the Commission)", COM (1999) 348 final 99/0154 (CNS). URL: https://1library.net/document/rz34nxmy-proposal-regulation-jurisdiction-recognition-enforcement-judgments-commercial-commission.html (дата обращения: 03.08.2020).

[9] European Commission, Justice and Home Affairs DG Statement on Articles 15 and 73. URL: http://ec.europa.eu/civiljustice/homepage/homepage_ec_en_declaration.pdf (дата обращения: 03.08.2020).

В предложении Европейского парламента 1999 г. был сформулирован отказ от подхода, основанного на постулате, что электронная торговля товарами и услугами, доступными в другом государстве-члене, составляет деятельность, направленную на это государство.

В соответствии с совместным заявлением Европейской комиссии по вопросам юстиции и внутренних дел в отношении ст. 15 Регламента (ЕС) № 44/2001 для применения п. (c) 1 ст. 15 (в текущей редакции п. 1(c) ст. 17 "Брюсселя I *bis*") одиночный факт осуществления направленной деятельности профессиональной стороны на государство-участник по месту жительства потребителя считается недостаточным, необходим также факт заключения *договора* между потребителем и профессиональной стороной в рамках её деятельности. Данное положение Европейская комиссия распространяет и в отношении контрактов, заключенных *дистанционным способом*, в том числе и посредством сети Интернет. Только лишь факт доступности интернет-сайта потребителю не будет считаться достаточным для применения данной статьи. Должно быть также принято во внимание то обстоятельство, что, *во-первых*, такой интернет-сайт способствует заключению дистанционных договоров и, *во-вторых*, договор был заключен дистанционно с помощью любых средств связи. Язык сайта или используемая при оплате услуг или товаров валюта также не должны являться значимыми факторами[10].

Концепция целенаправленно ориентированной деятельности была детализирована в судебных делах *Peter Pammer v. Reederei Karl Schlüter GmbH & C° KG* (*C*-585/08) и *Hotel Alpenhof GesmbH v Oliver Heller* (*C*-144/09), рассмотренных Европейским судом 07.12.2010[11].

При рассмотрении данных дел судом были выработаны содержательные *характеристики критерия* «направленной деятельности» профессиональной стороны на страну места жительства потребителя, к которым Европейский суд отнес, в частности:

– ориентирование профессиональной стороны на заключение трансграничных потребительских контрактов;

– использование доменного имени верхнего уровня, отличного от национального домена соответствующего государства места нахождения профессиональной стороны;

– демонстрацию наличия клиентов-потребителей, проживающих в иностранных государствах;

– обозначение маршрута к месту нахождения профессиональной стороны с территории других государств;

– возможность использования языка или валюты, отличных от используемых в государстве места нахождения профессиональной стороны, с возможностью осуществления и подтверждения бронирования на другом языке;

– указание телефонных номеров с международным кодом;

– наличие расходов на поисковую систему ссылок (например, *Google*), в целях облегчения доступа к сайту профессиональной стороны или его посредника для потребителей, проживающих в других государствах[12].

Необходимо добавить, что в решении Европейского суда не было установлено, достаточно ли лишь одного критерия для признания факта целенаправленного ориентирования сайта состоявшимся или необходима их совокупность. В то же время перечисление столь широкого перечня обстоятельств, положенных в основу критерия «направленной деятельности», позволяет допустить, что содержание направленной деятельности как проявления тесной связи отношения с правопорядком страны потребителя должно включать в себя как *объективную* составляющую — в виде ориентирования деятельности предпринимателя на страну потребителя, так и *субъективную* — в виде предвидения предпринимателем распространения на него законодательства страны потребителя (подробнее о юрисдикционной и коллизионной защите потребителя в [11–13]).

Именно такой подход, позволяющий учитывать совокупность обстоятельств, в большей степени способствует как предоставлению защитной юрисдикции, так и предотвращению ситуации злоупотребления потребителями своими правами, недобросовестного поведения потребителей и прочих действий, подпадающих под понятие *потребительского экстремизма* [2, 5]. В работе [15] целевой подход к определению сферы юрисдикции признается наиболее приемлемым.

Между тем наделение равным содержанием критерия «направленной деятельности» как *условия распространения* законодательства о персональных данных и как *условия предоставления* специальной коллизионной защиты потребителю не является целесообразным. Это может быть объяснимо использованием отличных механизмов защиты потребителя от применения иностранного права и защиты субъектов персональных данных. Если потребительские отношения преимущественно лежат в частноправовой плоскости, то в отношении защиты персональных данных, как обоснованно показано в [3], превалируют меры публично-правового регулирования и административная ответственность.

Беспрецедентный масштаб сбора и обмена персональными данными в рамках государственных и частных компаний при осуществлении ими своей де-

[10] В иностранной доктрине было отмечено, что язык сайта и используемая валюта расчетов в ряде случаев могут демонстрировать намерение профессиональной стороны заниматься маркетингом в конкретной стране. Если в данной стране используется весьма специфический язык или валюта, то он может быть принят во внимание при решении вопроса о том, что профессиональная сторона целенаправленно ориентирована на данную страну [16].

[11] Joined cases C-585/08 and C-144/09 Pammer/Alpenhof [2010] ECR I-12527. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62008CJ0585 (дата обращения: 19.05.2020).

[12] Judgment of the Court (Grand Chamber) of 7 December 2010 (references for a preliminary ruling from the Oberster Gerichtshof (Austria)) — Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CA0585 (дата обращения: 10.06.2020).

ятельности, а также коммерческая ценность подобной информации способствовали появлению на рынке различных *баз данных*, содержащих персональные данные. Такого рода информация может быть востребована как компаниями, которые предоставляют товары и услуги потребителям, так и лицами, занимающимися незаконной деятельностью (мошенничество, вымогательство и др.) [8].

Последствия использования критерия «направленной деятельности» при предоставлении потребителю коллизионной защиты и решении вопроса о распространении закона о персональных данных не одинаковы. Если в *первом* случае суд стоит лишь перед выбором применимого права страны потребителя или права профессиональной стороны, то во *втором* случае решается вопрос предоставления или не предоставления защиты субъекту персональных данных в результате оценки направленной деятельности иностранного оператора.

Это обусловливает необходимость *дифференцированного* подхода к установлению содержания критерия направленной деятельности как *условия применения* законодательства о персональных данных и как *условия предоставления* специальной коллизионной защиты потребителю. Такого рода подход можно усмотреть и в европейском праве.

Если, как было указано, в совместном заявлении Европейской комиссии по вопросам юстиции и внутренних дел в отношении статьи 15 Регламента (ЕС) № 44/2001, язык сайта или используемая при оплате услуг или товаров валюта не являются значимыми факторами при установлении защитной юрисдикции и выбора применимого права в отношении потребителей, то в п. 23 Преамбулы Регламента о персональных данных *язык*, используемый в одном или нескольких государствах-членах Европейского союза, может являться самостоятельным основанием для сферы его применения.

Обработка персональных данных может иметь место и при отсутствии заключенного договора между иностранным лицом, обрабатывающим данные, и физическим лицом, тогда как защита потребителя от применения иностранного права может предоставляться только при направленной деятельности предпринимателя на территорию страны потребителя при наличии договора между ними. Если контролер или обработчик предлагают товары или услуги или осуществляют мониторинг субъектов данных в Союзе, то Регламент может быть применим к их деятельности.

Пункт «а» ч. 2 ст. 3 Регламента о персональных данных применяется к предложению товаров независимо от того, требуется ли оплата. Бизнес в Интернете все чаще ведется бесплатно для потребителя. *Facebook* представляет собой пример деятельности, в рамках которой услуги предлагаются бесплатно, при этом обрабатываются огромные объемы персональных данных. Такого рода компании имеют другие способы монетизации своих предложений, например, доход от рекламы. В доктрине было определено, что ограничение применимости Регламента о персональных данных к предложениям, требующим оплаты, ставит под угрозу возможность защиты персональных данных лиц, которые являются своего рода «товаром» в том случае, если они не оплачивают предоставляемые им услуги[13].

В п. 23 Преамбулы Регламента о персональных данных не говорится о том, что изложенные в нем обстоятельства должны исследоваться в совокупности, из чего следует, что каждый отдельный фактор — использование валюты, языка, упоминание покупателей — может являться самостоятельным критерием, обозначающим намерение оператора предлагать товары или услуги субъектам данных в Европейском союзе.

В российской юридической доктрине было определено, что доказательствами намерения предложения услуги в ЕС может стать наличие у российских компаний (интернет-магазинов, финансовых компаний, социальных сетей) сайта на языке хотя бы одного из государств — членов Союза или сайта, поддерживающего платежи в валюте стран ЕС [9].

Принимая во внимание положения Регламента, достаточно хотя бы одного из перечисленных условий. В случае нарушения Регламента о персональных данных ст. 83 предусматривает штраф до € 20 000 000, а в случае если нарушителем является предприятие, может быть взыскано до 4% от общего годового оборота предыдущего финансового года, в зависимости от того, что выше. Столь высокие штрафы, не представляющие собой угрозы для крупного бизнеса, но создающие большие проблемы для малого и среднего бизнеса, подвергались критике в литературе [14].

В доктрине по-разному решается, должна ли включаться субъективная составляющая при оценке направленной деятельности, а именно, должно ли учитываться «предвидение» контролера или лица, обрабатывающего данные, о предложении их услуг субъектам данным, находящимся в иностранном государстве.

В работе [15] показана необходимость сбалансированных критериев, которые, с *одной* стороны, обеспечивали бы достаточную степень определенности и предсказуемости, позволяя участникам рынка предвидеть возможность применения законодательства о персональных данных, а с *другой* — создавали бы необходимую степень гибкости применения, тем самым сводя к минимуму соблазны для уклонения от закона.

Вместе с тем можно заметить, что в Преамбуле Регламента о персональных данных говорится не столько о предсказуемости, сколько о необходимости повышения уровня *правовой определенности* и *практической достоверности* [4, 6] для физических лиц, субъектов экономической деятельности и органов государственной власти (Пар. 7).

---

[13] Gullaker H. The extraterritorial scope of European data protection law: The changes in extraterritorial scope between the Data Protection Directive and the General Data Protection Regulation. URL: https://www.duo.uio.no/bitstream/handle/10852/60636/586.pdf?sequence=1&isAllowed=y.

Субъективный подход к направленной деятельности был подвергнут критике в иностранной доктрине. В частности, в [16] обосновывается необходимость учета результата деятельности контролера или лица, обрабатывающего данные. По мнению автора, фокусирование на субъективных аспектах может способствовать возникновению ситуации, когда данные субъектов обрабатываются, тогда как субъекты данных лишаются своей защиты в соответствии с Регламентом в связи с тем, что контролер или лицо, обрабатывающее данные, смогли доказать свою неосведомленность и отсутствие намерения ориентировать информацию на лиц государств — членов ЕС.

Можно согласиться с данным подходом. Как было сказано, последствия нераспространения *закона* о персональных данных, принимая во внимание их впечатляющие массивы и легкость трансграничного обращения, являются не соизмеримыми с постановкой вопроса о выборе юрисдикции и применимого права к потребительским спорам. В последнем случае речь идет именно о выборе, а не о факте предоставления или непредоставления юрисдикционной и коллизионной защиты.

В этой связи при квалификации направленной деятельности контролера или лица, обрабатывающего данные, на субъекта персональных данных именно наличие объективных факторов в виде оценки последствий указанной деятельности играет доминирующую роль по отношению к субъективной составляющей.

В российском законодательстве о персональных данных воспринят ряд положений европейского законодательства в связи с тем, что Федеральный закон «О персональных данных» 2006 г. (далее — Закон РФ о персональных данных)[14] был принят сразу после ратификации Россией Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 г.[15]. При этом, в отличие от Регламента о персональных данных, в российском законе отсутствуют специальные положения, регламентирующие сферу его действия по территории и кругу лиц. В этой связи была сформирована специальная рабочая группа, возглавляемая А. И. Савельевым, при Консультативном совете Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Результаты, к которым пришли члены рабочей группы, были отражены в отчете для внутреннего использования Роскомнадзора и в официальных комментариях Министерства цифрового развития, связи и массовых коммуникаций РФ (Министерства связи) Федерального закона от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (далее — Федеральный закон № 242-ФЗ)[16].

В рамках подхода, обозначенного в рекомендациях Министерства связи, предписывается руководствоваться критерием направленной деятельности. В пояснительной записке Министерства связи наличие направленности интернет-сайта на территорию РФ предложено определять следующими факторами:

1) использование доменного имени, связанного с РФ или субъектом РФ (.ru, .рф, .su, .москва, moscow и др.) и (или)

2) наличие русскоязычной версии интернет-сайта, созданной владельцем такого сайта или по его поручению иным лицом (использование на сайте или самим пользователем плагинов, предоставляющих функционал автоматизированных переводчиков с различных языков, не должно приниматься во внимание).

А. И. Савельев регистрацию и фактическое использование географических доменных имен, связанных с Российской Федерацией или ее регионами (.ru, .su, .рф, .Москва и др.), считал оправданными, поскольку такого рода условия должны быть истолкованы как воля компании осуществлять свою деятельность «имея в виду Россию», принимая во внимание устойчивую связь таких доменных имен с территорией Российской Федерации [15].

Что касается второго пункта, то в пояснительной записке установлено, что поскольку русский язык широко используется в некоторых странах за пределами РФ, для определения направленности интернет-сайта именно на территорию РФ дополнительно необходимо наличие как минимум одного из следующих элементов:

- возможности осуществления расчетов в российских рублях;
- возможности исполнения заключенного на таком интернет-сайте договора на территории Российской Федерации (доставки товара, оказания услуги или пользования цифровым контентом на территории России);
- использование рекламы на русском языке, отсылающей к соответствующему интернет-сайту;
- использование иных обстоятельств, явно свидетельствующих о намерении владельца интернет-сайта включить российский рынок в свою бизнес-стратегию.

Использование функции автоматического перевода, позволяющей переводить на несколько выбранных пользователем языков, по мнению А.И. Савельева, не может быть основанием для вывода о том, что веб-сайт ориентирован на Российскую Федерацию. Скорее можно утверждать, что он ориентирован на международ-

[14] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (часть I). Ст. 3451.

[15] Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 г. // СЗ РФ. 2014. № 5. Ст. 419.

[16] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Пояснительная записка. Сфера действия ФЗ-242 по территории и кругу лиц. URL:https://digital.gov.ru/ru/personaldata/ (дата обращения: 20.08.2020).

ную аудиторию в целом, без ее национальной дифференциации [15].

Таким образом, в рамках указанного подхода только факт размещения информации в национальной доменной зоне РФ является самостоятельным критерием, свидетельствующим о направленности сайта. Русскоязычная версия сайта, размещенная в функциональных доменных зонах или национальных доменных зонах иностранных государств, может быть принята во внимание в качестве критерия направленной деятельности сайта только при наличии дополнительных обстоятельств в виде осуществления расчетов в российских рублях, исполнения договора в РФ и др.

В пояснительной записке также обозначено, что одной лишь доступности интернет-сайта на территории РФ недостаточно для вывода о том, что на него распространяется законодательство РФ. В этой связи рекомендовано обращение к критерию направленности деятельности лица на территорию РФ, используемого в международном частном праве и законодательстве о защите прав потребителей (ст. 1212 Гражданского кодекса РФ) как *условия применения* законодательства РФ к отношениям с иностранным субъектом.

Статья 1212 ГК РФ, хотя и оперирует понятием направленной деятельности, но содержание данного понятия не раскрывает. Впервые уточнение содержательных аспектов данного понятия имело место в Постановлении Пленума Верховного Суда РФ № 24 от 9 июля 2019 г. «О применении норм международного частного права судами РФ» (далее — Постановление Пленума ВС РФ от 2019 г. № 24)[17]. В п. 45 указанного Постановления сказано, что «…*профессиональная сторона считается направляющей свою деятельность на территорию страны места жительства потребителя, в частности, в том случае, когда она поддерживает в сети «Интернет» сайт, содержание которого свидетельствует о его ориентации на потребителей из соответствующей страны*».

К квалифицирующим признакам ориентирования сайта в сети Интернет на российских потребителей в Постановлении Пленума ВС РФ № 24 от 2019 г. относятся: использование на сайте среди прочих русского языка, указание цен в российских рублях, а также контактных телефонов с российскими кодами. Перечень не является исчерпывающим, поскольку суду предлагается также оценить и иные аналогичные доказательства (например, владелец сайта заказывал услуги, направленные на повышение цитируемости его сайта у российских пользователей сети Интернет). При этом в Постановлении Пленума ВС РФ № 24 от 2019 г. установлено, что достаточно соблюдения одного из указанных условий для применения судом по своей инициативе защиты прав потребителя, предоставляемой императивными нормами права страны места жительства потребителя.

Как можно заметить, предложенное в Постановлении Пленума понимание «направленной деятельности» является более широким по сравнению с толкованием, приведенным в пояснительной записке Министерства связи РФ, где расчеты и используемый язык предлагается относить к *факультативным* признакам, требующим наличия дополнительных факторов.

Впоследствии Роскомнадзором был уточнен подход о действии российского закона о персональных данных[18]. На официальном сайте Роскомнадзора размещен комментарий к Федеральному закону № 242-ФЗ[19].

Хотя в комментарии отмечено, что критерии направленности сайтов на территорию России пока еще только вырабатываются, в то же время сформулировано *предложение*, какие факторы к ним можно относить:

1) использование доменного имени, связанного с Россией (.ru, .рф, .su); и/или

2) наличие русскоязычной версии сайта, созданной владельцем сайта или по его поручению иным лицом; и/или

3) возможность исполнения на территории России заключенного на сайте договора (доставка товара, оказание услуги, пользование цифровым контентом).

Указанные обстоятельства отделяются друг от друга как соединительным, так и разделительным союзом, что позволяет сделать вывод о возможности использования каждого из них в качестве самостоятельного критерия. Из этого следует более широкое содержание оснований, предусмотренных в рамках второго подхода по сравнению с подходом, предложенным ранее Министерством связи РФ.

Именно второй подход в большей степени соответствует сложившемуся в праве ЕС толкованию намерения оператора предлагать товары или услуги субъектам данных в Европейском союзе. Между тем применительно к российским реалиям определение сферы применения российского закона о персональных данных, исходя только из факта наличия русскоязычной версии сайта, представляется не совсем корректным. Русский язык является широко используемым в других государствах. Размещение коммерческой рекламы на русском языке в доменных зонах иностранных государств может свидетельствовать об ориентировании данной информации не на российских потребителей, а на русскоговорящих потребителей того или иного иностранного государства, как это имеет место в национальных доменных зонах Белоруссии, Казахстана, Украины и др.

В этой связи более точным представляется подход, который предложен ранее в пояснительной записке

[17] Постановление Пленума Верховного Суда РФ от 9 июля 2019 г. «О применении норм международного частного права судами РФ» // РГ. 2019. 17 июл.

[18] Федеральная служба по надзору в сфере связи информационных технологий и массовых коммуникаций. Методические рекомендации. URL: https://pd.rkn.gov.ru/library/p195/ (дата обращения: 20.08.2020).

[19] Там же.

Министерства связи РФ, в рамках которого устанавливаются как *самостоятельные* критерии (размещение информации в рамках национальной доменной зоны), так и *факультативные* критерии (язык, валюта), требующие дополнительных оснований подтверждения направленной деятельности иностранного оператора на российских физических лиц.

Общие тенденции проявления экстратерриториальной законодательной (предписывающей) юрисдикции сказываются и на особенностях реализации судебной юрисдикции в отношении рассмотрения трансграничных споров. Используя фразеологизм американского судьи Х. Кабранеса о том, что ограничение судебной власти должно следовать в кильватере законодательной власти[20], нужно заметить, что установление экстратерриториальной судебной юрисдикции берет свое начало в экстратерриториальном проявлении законодательной (предписывающей) юрисдикции.

Между тем необходимо обратить внимание на то, что, если распространение Закона РФ о персональных данных в отношении интернет-сайтов операторов персональных данных ограничивается критерием направленности сайта, исходя из предложенных критериев Министерством связи и Роскомнадзором, иной подход предусмотрен при установлении юрисдикции суда по делу о защите прав субъекта персональных данных.

В соответствии с п. 10 ч. 3 ст. 402 ГПК РФ суды РФ вправе рассматривать дела с участием иностранных лиц, в случае если по делу о защите прав субъекта персональных данных, в том числе о возмещении убытков и (или) компенсации морального вреда, истец имеет место жительства в РФ.

Отсутствие в указанном основании учета специфики деятельности операторов персональных данных в киберпространстве предполагает, что судебная юрисдикция может быть установлена в отношении оператора персональных данных на основании простого доступа к информации. Столь широкие основания реализации юрисдикции применительно к отношениям, связанных с защитой персональных данных, способствуют обострению конфликта юрисдикции.

В российской судебной практике при установлении юрисдикции суда по делам о защите персональных данных также не ставится вопрос о направленности деятельности ответчика на территорию РФ, что обусловливает широкие основания для установления экстратерриториальной судебной юрисдикции. При обращении Роскомнадзора РФ с иском в суд на основании п. 5 ч. 3 ст. 23 ФЗ «О персональных данных» 2006 г., а также ч. 2 ст. 46 ГПК РФ с исковыми заявлениями в защиту прав субъектов персональных данных, Роскомнадзор пользуется всеми процессуальными правами истца, в том числе правом выбора подсудности, предусмотренным п. 10 ч. 3 ст. 402 ГПК РФ[21].

В целях установления сбалансированного подхода, основания распространения ФЗ «О персональных данных» 2006 г. в отношении иностранного оператора должны коррелировать с основаниями установления судебной юрисдикции по делу о защите прав субъекта персональных данных.

В качестве наиболее адекватного механизма по установлению юрисдикции можно использовать алгоритм, предложенный в пояснительной записке Министерства связи РФ, в соответствии с которым размещение информации в рамках национальной доменной зоны устанавливается в качестве основного критерия, имеющего самостоятельное значение, тогда как использование русскоязычной версии сайта предлагается в качестве факультативного критерия, который требует дополнительных оснований подтверждения направленной деятельности иностранного оператора на российских физических лиц в виде доставки товара, оказания услуги или пользования *цифровым* [7] контентом на территории России и др.

При этом целесообразно дифференцированное понимание направленной деятельности как *критерия предоставления* потребителю коллизионной защиты и как *условия применимости* законодательства о персональных данных к иностранному оператору. В связи с чем представляется ошибочной рекомендация обращения к критерию направленности деятельности лица на территорию РФ, используемого в международном частном праве и законодательстве о защите прав потребителей (ст. 1212 Гражданского кодекса РФ) как *условия применения* законодательства РФ к отношениям с иностранным субъектом, которая размещена на сайте Министерства связи. Здесь также заметим, что в рамках Европейского союза отсутствуют рекомендации при определении такого рода намерения апеллировать к пониманию критерия «направленной деятельности», который в Регламентах "Брюссель I (*bis*)" и Регламенте "Рим I" используется в качестве основания предоставления потребителю защитной юрисдикции и специального коллизионного регулирования.

Таким образом, общим подходом оценки направленной деятельности при решении вопроса о предоставлении потребителю коллизионной защиты и при решении вопроса о распространении законодательства о персональных данных должно являться то, что оценка направленной деятельности не должна исходить из возможности простого доступа к сайту. Отличие проявляется в том, что если при решении вопроса о предоставлении потребителю коллизионной защиты оценка направленной деятельности профессиональной стороны исходит из *субъективной* (предвидение

[20] Cabranes J.A. Withholding Judgment. Why U.S. Courts Shouldn't Make Foreign Policy. Foreign Affairs. 2015. URL: https://www.foreignaffairs.com/articles/2015-08-18/withholding-judgment (дата обращения 7.03.2020).

[21] Постановление Московского городского суда от 20 июня 2014 г. № 44г-70/14; Апелляционное определение Московского городского суда от 16 декабря 2014 г. № 33-40431/14; Апелляционное определение СК по гражданским делам Свердловского областного суда от 15 июня 2017 г. по делу № 33-10343/2017.

предпринимателем ориентирования его деятельности на страну потребителя) и *объективной* («принципа эффекта», выраженного в реальном фактическом взаимодействии потребителя и предпринимателя) составляющих, то при исследовании квалификации направленной деятельности иностранного оператора должна превалировать *объективная* составляющая в виде оценки последствий обработки иностранными операторами персональных данных. Такого рода подход не позволяет оператору персональных данных необоснованно ссылаться на отсутствие намерения ориентировать информацию на лиц иностранных государств и не лишает физических лиц защиты, на которую они имеют право рассчитывать в соответствии с законодательством о персональных данных.

К объективной составляющей критерия направленной деятельности иностранного оператора представляется целесообразным относить как *самостоятельные* критерии (размещение информации в рамках национальной доменной зоны), так и *факультативные* критерии (язык, валюта), требующие дополнительных оснований подтверждения направленной деятельности иностранного оператора на российских физических лиц.

Такого же рода условия должны лежать и в содержании основания установления судебной юрисдикции по делу о защите прав субъекта персональных данных, принимая во внимание общие тенденции проявления экстратерриториальной законодательной (предписывающей) и судебной юрисдикции.

Литература

1. Бабаев А.Б., Бабкин С.А., Бевзенко Р.С., Белов В.А., Тарасенко Ю.А. Гражданское право. Актуальные проблемы теории и практики. В 2-х тт. Т. 2 / Под общ. ред. В. А. Белова. М.: Юрайт, 2015. 1161 с.
2. Бежан А. Потребительский экстремизм // Корпоративный юрист. 2009. № 3. С. 53–57.
3. Долинская В. В. Защита прав в сфере персональных данных в России и ЕС // Журнал «Законы России: опыт, анализ, практика». 2019. № 9. С. 22–29.
4. Ершов В. В. Правовое и индивидуальное регулирование общественных отношений: Монография. М.: РГУП, 2018. 628 с. ISBN 978-5-93916-631-7
5. Кусков А. С., Сирик Н. В. Потребительский экстремизм в сфере туризма // Гражданин и право. 2017. № 9. С. 71–78.
6. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере: Монография. М.: Росс. гос. ун-т правосудия, 2016. 316 с. ISBN 978-5-93916-505-1.
7. Ловцов Д. А. Информационно-правовые основы правоприменения в цифровой сфере // Мониторинг правоприменения. 2020. № 2(35). С. 44–52. DOI: 10.21681/2226-0692-2020-2-44-52
8. Ловцов Д. А., Галахова А. Е. Защита интеллектуальной собственности в сети Интернет // Информационное право. 2011. № 4. С. 13–20.
9. Талапина Э. В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды института государства и права Российской академии наук. 2018. № 5. С. 117–150.
10. Терентьева Л. В. Понятие киберпространства и очерчивание его территориальных контуров // Правовая информатика. 2018. № 4. С. 66–71. DOI:10.21681/1994-14042018-4-66-71
11. Терентьева Л. В. Соглашение о международной подсудности с участием потребителя: предоставление защитной юрисдикции потребителю в цифровую эпоху // Вестник МГЮА. 2019. № 10. С. 110–125.
12. Терентьева Л. В. Основания установления международной судебной юрисдикции применительно к трансграничным потребительским спорам в цифровую эпоху // Lex Russica. Закон русский. 2019. № 11. С. 96–107.
13. Терентьева Л. В. Критерий направленной деятельности профессиональной стороны на территорию страны места жительства потребителя как условие специального коллизионного регулирования потребительских отношений //Актуальные проблемы российского права. 2020. Т. 15. № 4. С. 142–154.
14. Mercen A. G. The extraterritorial application of European Union data protection law // The Spanish Yearbook of International Law. 2019. № 23. P. 413-425.
15. Savelyev A. Russia's new personal data localization regulations: A step forward or a self-imposed sanction? // Computer law & security review. 2016. Vol. 32. P. 128-145.
16. Svantesson D. J. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation // International Data Privacy Law. 2015. Vol. 5. P. 226-234.
17. Tang Z. S. Consumer contracts and the Internet in EU private international law // A. Savin, J. Trzaskowski, ed. Research Handbook on EU Internet Law. Cheltenham: Edward Elgar, 2014. P. 254-284.

Рецензент: ***Чубукова Светлана Георгиевна,*** *доцент кафедры информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), Москва, Россия.*
E-mail: csg57@yandex.ru

THE CRITERION OF "TARGETED ACTIVITIES" AS APPLIED TO RELATIONS LINKED TO PERSONAL DATA PROTECTION

Ludmila Terent'eva, *Ph.D., Associate Professor of the Chair of International Private Law in Kutafin Moscow State Law University, Russian Federation, Moscow.*
E-mail: *terentevamila@mail.ru*

Keywords: *personal data, judicial jurisdiction, directed activity, consumer protection, extraterritorial jurisdiction, cyberspace, controller, person processing personal data.*

Abstract.

Purpose of the article: The purpose of the work is to clarify the scope of the Act "On Personal Data" of the Russian Federation" (2006). The author also compares the scope of this act with the basis for establishing the jurisdiction of the Russian court, provided for in paragraph 10 of Part 3 of Article 402 of the Civil Code of the Russian Federation.

Method used: This study uses the comparative and legal analysis of legislative and doctrinal approaches to the definition of "directed activity" regarding to the establishment of jurisdiction in the case on protection of personal data; to the determining the scope of application of the Act "On Personal Data"; and to the application of the mechanism of collision protection to the consumer provided for in article 1212 of the civil code.

Results: The author has established the need to differentiate approaches to determining the content of the criterion of "directed activity" as a condition for applying the legislation on personal data and as a condition for providing special conflict of laws protection to the consumer. This article argues that the basis of the scope of the Act "On Personal Data" should coincide with the bases of establishing jurisdiction in the case of the protection of the data subject.

References

1. Babaev A.B., Babkin S.A., Bevzenko R.S., Belov V.A., Tarasenko Iu.A. Grazhdanskoe pravo. Aktual`ny`e problemy` teorii i praktiki. V 2-kh tt. T. 2 / Pod obshch. red. V. A. Belova. M.: Iurai`t, 2015. 1161 s.
2. Bezhan A. Potrebitel`skii` e`kstremizm // Korporativny`i` iurist. 2009. № 3. S. 53-57.
3. Dolinskaia V. V. Zashchita prav v sfere personal`ny`kh danny`kh v Rossii i ES // Zhurnal «Zakony` Rossii: opy`t, analiz, praktika». 2019. № 9. S. 22-29.
4. Ershov V. V. Pravovoe i individual`noe regulirovanie obshchestvenny`kh otnoshenii`: monografiia. M.: RGUP, 2018. 628 s. ISBN 978-5-93916-631-7
5. Kuskov A. S., Sirik N. V. Potrebitel`skii` e`kstremizm v sfere turizma // Grazhdanin i pravo. 2017. № 9. S. 71-78.
6. Lovtcov D. A. Sistemologiia pravovogo regulirovaniia informatcionny`kh otnoshenii` v infosfere : monografiia. M.: Ross. gos. un-t pravosudiia, 2016. 316 s. ISBN 978-5-93916-505-1.
7. Lovtcov D. A. Informatcionno-pravovy`e osnovy` pravoprimeneniia v tcifrovoi` sfere // Monitoring pravoprimeneniia. 2020. № 2(35). S. 44-52. DOI: 10.21681/2226-0692-2020-2-44-52
8. Lovtcov D. A., Galahova A. E. Zashchita intellektual`noi` sobstvennosti v seti Internet // Informatcionnoe pravo. 2011. № 4. S. 13-20.
9. Talapina E`. V. Zashchita personal`ny`kh danny`kh v tcifrovuiu e`pohu: rossii`skoe pravo v evropei`skom kontekste // Trudy` instituta gosudarstva i prava Rossii`skoi` akademii nauk. 2018. № 5. S. 117-150.
10. Terent`eva L. V. Poniatie kiberprostranstva i ocherchivanie ego territorial`ny`kh konturov // Pravovaia informatika. 2018. № 4.– S. 66-71. DOI:10.21681/1994-14042018-4-66-71
11. Terent`eva L. V. Soglashenie o mezhdunarodnoi` podsudnosti s uchastiem potrebitelia: predostavlenie zashchitnoi` iurisdiktcii potrebiteliu v tcifrovuiu e`pohu // Vestneyk MGIUA. 2019. № 10. S. 110-125.
12. Terent`eva L. V. Osnovaniia ustanovleniia mezhdunarodnoi` sudebnoi` iurisdiktcii primenitel`no k transgranichny`m potrebitel`skim sporam v tcifrovuiu e`pohu // Lex Russica. Zakon russkii`. 2019. № 11. S. 96-107.
13. Terent`eva L. V. Kriterii` napravlennoi` deiatel`nosti professional`noi` storony` na territoriiu strany` mesta zhitel`stva potrebitelia kak uslovie spetcial`nogo kollizionnogo regulirovaniia potrebitel`skikh otnoshenii` //Aktual`ny`e problemy` rossii`skogo prava. 2020. T. 15. № 4. S. 142-154.
14. Mercen A. G. The extraterritorial application of European Union data protection law // The Spanish Yearbook of International Law. 2019. № 23. P. 413-425.
15. Savelyev A. Russia's new personal data localization regulations: A step forward or a self-imposed sanction? // Somputer law & security review. 2016. Vol. 32. P. 128-145.
16. Svantesson D. J. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation // International Data Privacy Law. 2015. Vol. 5. P. 226-234.
17. Tang Z. S. Consumer contracts and the Internet in EU private international law // A. Savin, J. Trzaskowski, ed. Research Handbook on EU Internet Law. Cheltenham: Edward Elgar, 2014. P. 254-284.

30 ЛЕТ МЕЖВУЗОВСКОЙ НАУЧНОЙ ШКОЛЕ «СИСТЕМНАЯ ИНФОРМАТИЗАЦИЯ УПРАВЛЕНИЯ СЛОЖНООРГАНИЗОВАННЫМИ ОБЪЕКТАМИ»

Пинчук А. В.*

***Ключевые слова**: межвузовская научно-педагогическая школа, системная информатизация управления, сложноорганизованные объекты, научно-исследовательская работа, научные труды, информационно-математическое обеспечение, новые информационные технологии, отработка качества новой техники, показатели информационной эффективности, автоматизированные системы управления (АСУ).*

Аннотация.

Цель работы: совершенствование научно-методической базы информационных теорий управления и эргасистем в условиях «цифровизации» экономики и построения информационного общества.

Метод: системный анализ состояния и развития профильной межвузовской научной школы, обеспечивающей исследование информационных аспектов управления сложноорганизованными объектами и их испытаниями.

Результаты: исследованы достижения, задачи и формы развития известной межвузовской научно-педагогической школы «Системная информатизация управления сложноорганизованными объектами» как научно-методической базы промышленного создания эффективного информационно-математического обеспечения новых информационных технологий и внедрения его в существующие и перспективные интегрированные АСУ отработкой качества новой техники с целью повышения их информационной эффективности как информационных систем; представлены значения ряда основных показателей информационной эффективности реальных АСУ в результате внедрения научных и научно-технических результатов, полученных участниками научной школы; рассмотрены формы, методы и результаты выполнения приоритетных научно-исследовательских работ и руководства научной работой соискателей ученых степеней; представлена характеристика лидеров научной школы, в которой подготовлен ряд учёных высшей квалификации, с указанием личных достижений, а также указаны возможные новые приоритетные наукоёмкие направления научно-педагогической деятельности школы.

DOI:10.21681/1994-1404-2021-1-70-79

В наступившем 2021 году исполняется 30 лет известной Межвузовской многопрофильной *научно-педагогической школе* (МНПШ) «Системная информатизация управления сложноорганизованными объектами», выдвинувшей и реализовавшей на практике ряд эффективных общенаучных концепций, включая концепцию комплексного «ИКС»-подхода («информационно-кибернетически-синергетического») к исследованию и оптимизации эргатических систем, а также ряд оригинальных профильных научных концепций: информационной эффективности эргасистем, информационной безопасности эргасистем, информационного права и др., которые опубликованы в авторитетных научных журналах России («Автоматика и Телемеханика» РАН, «Известия РАН. Теория и системы управления», «НТИ РАН. Информационные процессы и системы», «Космические исследования», «Информация и Космос», «Известия Института инженерной физики», «Философские исследования», «Философия права», «Военная мысль», «Вопросы кибербезопасности», «Вопросы защиты информации», «Государство и право», «Информатика и образование», «Педагогика», «Информационное право», «Обозреватель-*Observer*», «Зарубежная радиоэлектроника» и др.) и за рубежом.

Свое начало МНПШ берёт с 1991–1996 гг., когда в Военной академии имени Ф. Э. Дзержинского сложилось первое направление межвузовской научной школы — «системная информатизация управления силами и средствами ракетных и космических комплексов» [1, 2]. Особенностью школы с тех пор является то, что в ней принимают участие представители различных структурных подразделений академии, а также российских вузов и научно-исследовательских институтов. Исходной теоретической базой МНПШ стали научные труды отечественных учёных-кибернетиков проф. В. Н. Калинина, проф. Ф. М. Килина, проф. Б. М. Резникова, проф. А. Г. Мамиконова, проф. А. В. Солодова [3–7].

* ***Пинчук Александр Васильевич,*** *кандидат военных наук, доцент, Учёный секретарь Военной академии ракетных войск стратегического назначения имени Петра Великого, Российская Федерация, г. Москва.*

E-mail: pinchuk_alex@inbox.ru

Ловцов
Дмитрий Анатольевич

Основоположником МНПШ является Ловцов Дмитрий Анатольевич[1], *доктор технических наук, профессор, заслуженный деятель науки РФ, почётный работник высшего профессионального образования РФ, почётный радист РФ, изобретатель СССР, почётный профессор Военной академии РВСН им. Петра Великого, академик Академии военных наук, лауреат Премии Минобороны РФ в области образования (2009), лауреат премий РВСН в области науки* (2004, 2007), лауреат Всероссийского конкурса на лучшую научную книгу (2016).

Д. А. Ловцов является известным учёным в области системной информатизации управления. В частности, он разработал новую *информационную теорию эргатических* (человеко-машинных) *систем*, которой посвятил свою докторскую диссертацию, защищённую в 1996 г. в *Военной академии* имени Ф. Э Дзержинского, две авторские монографии, одна из которых вышла в 2005 г. в издательстве РАН «Наука», и др. научные труды. Он внёс весомый вклад в развитие информационно-кибернетической системологии, *с приложениями* в сфере национальной безопасности, в космонавтике, ракетостроении, педагогике, экономике, правоведении, военном деле, о чём свидетельствует множество его научных публикаций по данной проблематике более чем в **40** научных журнальных изданиях РАН, РАО, РИА, АИН, АВН и др. Всего им опубликовано более **600** научных работ, включая более **100** монографий, учебников, словарей и учебных пособий, более **200** журнальных научных статей, в том числе 35 — в журналах Российской академии наук, **30** — за рубежом и др. Научные труды Д. А. Ловцова имеются во всех 100 библиотеках США.

С 1999 г. активно руководит Межвузовским постоянно действующим научным семинаром «Информатизация управления сложноорганизованными объектами», который стал основной формой подготовки научных и научно-педагогических кадров — участников научной школы. Ведёт большую общественно-научную деятельность. Член редколлегий научно-практических журналов «Правовая информатика» (с 2016 г. главный редактор), «Информационное право» (с 2004 г.), «Вестник МГЭУ» (с 2016 г.), «Профессорский журнал. Серия «Технические науки» (с 2018 г.). Руководитель коллектива разработчиков первых в мире стандартов защиты информации от нетрадиционных информационных угроз [41, 42].

Литературная, научная и учебная «продукция» участников МНПШ — ученых, преподавателей, аспирантов, адъюнктов и соискателей учёных степеней — за период её существования составляет более **1000** публикаций, включая фундаментальные монографии и учебники, прошедшие рецензирование руководителя и лидеров научной школы и изданные в центральных издательствах («Наука», «Радиотехника», «Машиностроение», «Высшая школа», «РАУ-Университет» и др.) [8–40], а также отчёты об итогах приоритетных НИР, выполненных по заказу Минобороны РФ, Минобрнауки РФ, Минпромторга РФ, Верховного Суда РФ, Роскосмоса, Российской академии наук, Академии военных наук, Российского фонда фундаментальных исследований и др., отражающих как последние *достижения* науки и техники в соответствующей предметной области системной информатизации, так и современные *требования* к высшему образованию.

Проведенные *практические апробации* достижений МНПШ на многочисленных международных, всероссийских, межведомственных и др. научных конференциях, симпозиумах, салонах, семинарах специалистов в 1991–2020 гг. неоднократно подтвердили, что общая *совокупность научных и научно-технических результатов*, полученных членами МНПШ, обладает научной новизной, соответствует мировому научно-техническому уровню и обеспечивает выработку соответствующих обоснованных технических предложений в проекты промышленного создания эффективного информационно-математического обеспечения (ИМО) новых информационных технологий (НИТ) и внедрение его в существующие и перспективные интегрированные АСУ отработкой качества новой техники (ОКНТ) с целью повышения (обеспечения) информационной эффективности АСУ ОКНТ как информационных систем (рис. 1). От зарубежных аналогов отличается наличием обоснованного теоретико-методологического базиса ИМО НИТ.

[1] См.: Ловцов, Дмитрий Анатольевич. URL: *https://ru.wikipedia.org/wiki*

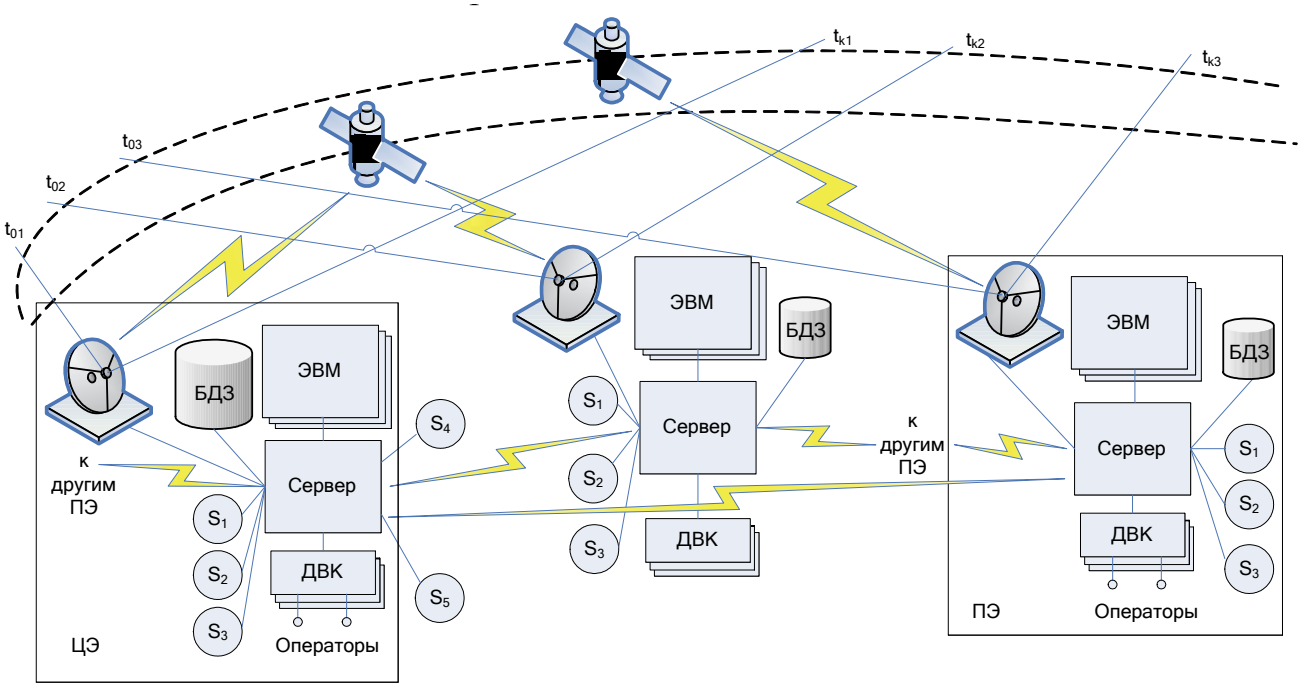


Рис. 1. Общая технико-топологическая структура АСУ ОКНТ

В период 1991–2020 гг. по проблематике МНПШ было подготовлено более 75 отчётов об итогах 50 приоритетных научно-исследовательских работ (научный руководитель — Д. А. Ловцов), имеющих важное народнохозяйственное или оборонное значение и направленных на повышение информационной эффективности специальных автоматизированных систем.

В частности, ряд основных научных и научно-технических результатов, полученные членами МНПШ, *реализован* в 2001–2012 гг. на практике в организационно-методическом и информационно-программном обеспечении реальных *АСУ ОКНТ* (рис. 2) *на базе* государственных испытательных космодромов МО РФ, *Государственного центрального межвидового полигона МО РФ, ГИЦИУ КС МО*.

Реализация научных результатов обеспечила улучшение следующих основных *информационных* показателей АСУ ОКНТ:

достоверность оценивания тактико-технических характеристик и параметров объектов отработки в условиях ограниченных объёмов измерительной информации возросла на 10–12%;

полнота определения навигационных параметров объектов отработки возросла на 13–15%;

точность прогнозирования навигационных параметров объектов отработки возросла на 10–15% как в режиме реального времени, так и в режиме послесеансной обработки измерительной информации; получения оценок навигационных параметров — на 75% (с 20 м до 5 м); измерения параметров промаха целей — 5 м;

При этом сбор и переработка измерительной информации в ходе лётных экспериментов осуществляется в *реальном масштабе времени* (рис. 3).

Полученные членами научной школы научные и *научно-технические* результаты являются базисными для промышленной разработки эффективного прикладного ИМО реальных АСУ ОКНТ, включающего, в частности:

– алгоритмы ИМО имитационно-игрового моделирования функционирования управлений заказов и поставок вооружения, военной и специальной техники (ВВСТ) с использованием современных математических методов поддержки подготовки и принятия управленческих решений;

– алгоритмы ИМО информационно-поисковой системы, базирующейся на основе современных технологий извлечения, накопления и использования знаний, обеспечения хранения и доступа к информационным объектам АСУ процессами создания, отработки, закупки и поставки ВВСТ;

– алгоритмы ИМО функциональных подсистем наблюдения, идентификации и диагностирования бортовой аппаратуры отрабатываемых образцов перспективного ВВСТ;

– алгоритмы ИМО функциональной подсистемы навигационных определений отрабатываемых образцов перспективного ВВСТ;

– алгоритмы ИМО планирования и координации защищённых информационных процессов в реальных АСУ ОКНТ на уровнях организационно-административного и организационно-технологического управления;

– электронную (компьютеризированную) документацию сведений на перспективные комплексы ВВСТ и др.

Практическая значимость полученных результатов заключается в разработке научно-прикладной методологии (принципов, методов и средств), обеспе-

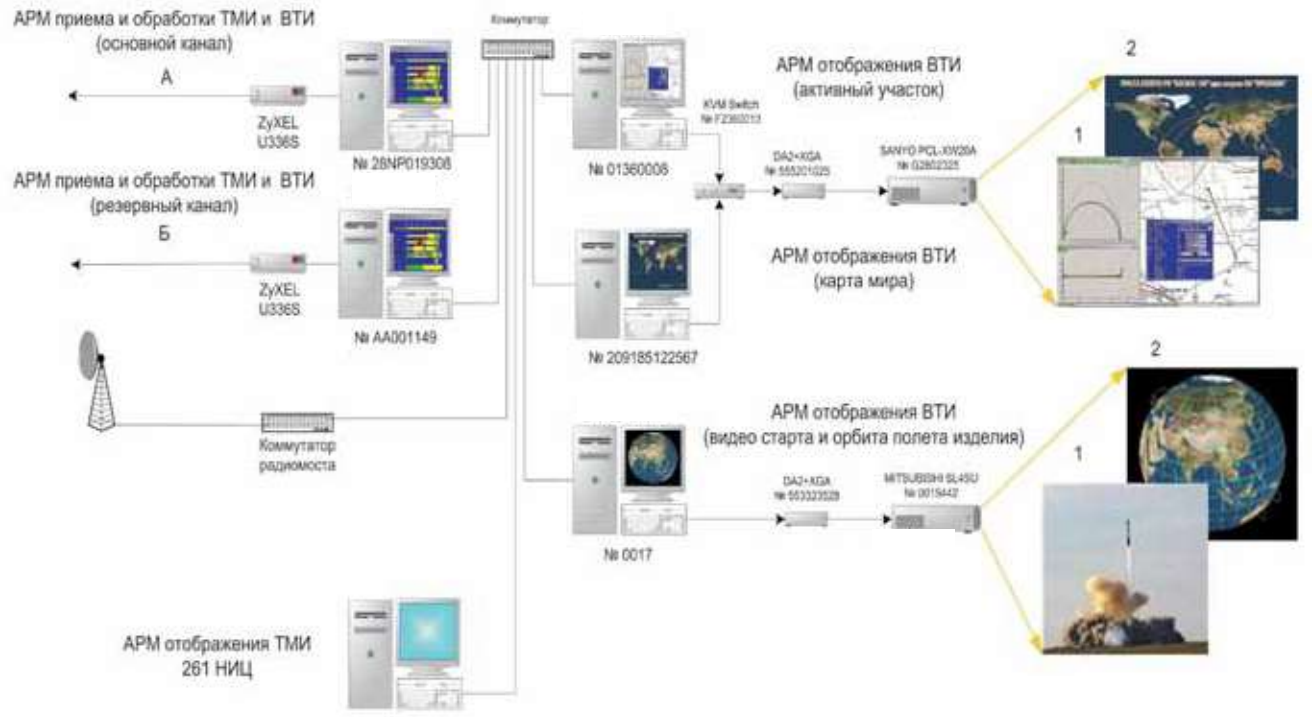


Рис. 2. Конфигурация комплекса средств автоматизации проведения лётных экспериментов

чивающей выработку обоснованных программ дальнейшего развития ВВСТ и создания отечественных АСУ ОКНТ нового поколения, обладающих повышенной информационной эффективностью; в разработке методического и информационно-программного обеспечения АСУ государственных испытательных полигонов и космодромов МО РФ, организационно-методического и информационно-программного обеспечении системы распределённой обработки и контроля сложных технических комплексов на полигонах МО РФ, а также в совершенствовании подготовки специалистов и обучения персонала АСУ ОКНТ. Общий выигрыш в *информационной производительности* реальных АСУ ОКНТ составляет 20–25%.

Результаты работы МНПШ в целом обеспечивают выработку соответствующих обоснованных технических предложений в проекты промышленного создания эффективного ИМО новых информационных технологий и внедрение его в существующие и перспективные интегрированные АСУ ОКНТ с целью повышения (обеспечения) *информационной эффективности* АСУ как информационных систем.

Всего в рамках МНПШ за время существования подготовлено более 80 ученых, в том числе 12 докторов наук, из которых в академии сейчас активно трудятся: К. Р. Байрамов, В. В. Гончаров, А. В. Зайцев, В. В. Князев, Д. А. Ловцов, А. В. Сухов. Диссертации на соискание учёной степени доктора наук защитили:

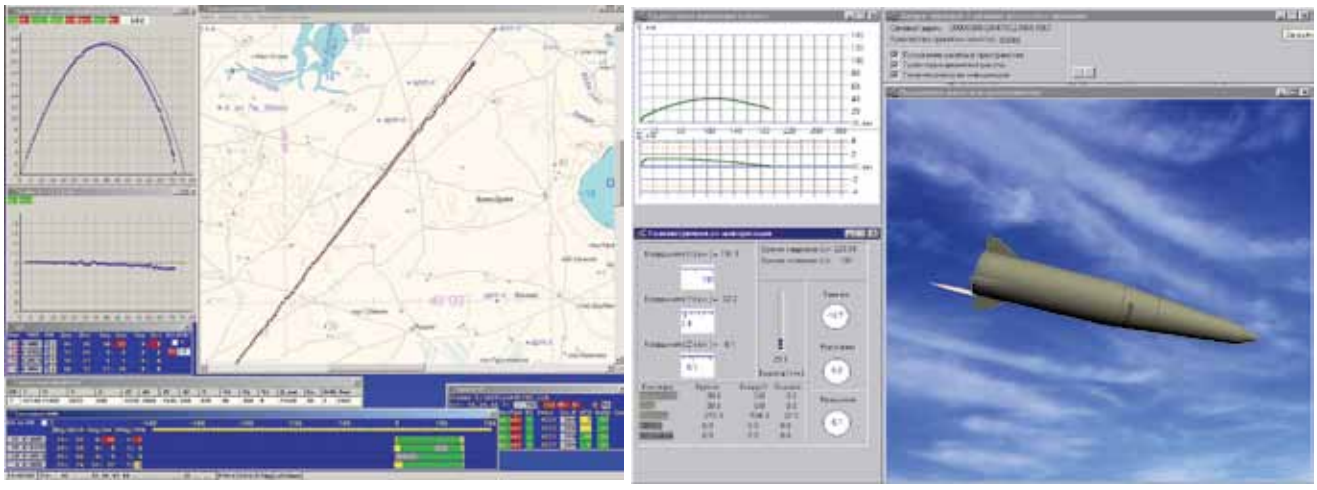


Рис. 3. Оперативное отображение результатов работы элементов информационно-программного обеспечения АСУ ОКНТ

– **Ловцов** Дмитрий Анатольевич (1996), разработавший информационную теорию АСУ отработкой качества новой техники (АСУ ОКНТ);
– **Бетанов** Владимир Вадимович (1997), разработавший теоретические основы решения обобщённых некорректных навигационно-баллистических задач в АСУ ОКНТ;
– **Омельченко** Виктор Валентинович (1997), разработавший теоретические основы классификации нечётких диагностических ситуаций при испытании объектов новой техники в АСУ ОКНТ;
– **Лысенко** Игорь Валентинович (2001), разработавший теоретические основы решения обобщённых некорректных задач оценивания лётно-технических характеристик объектов новой техники в АСУ ОКНТ;
– **Зайцев** Александр Владимирович (2002), разработавший теоретические основы обеспечения точности систем управления объектов новой техники в условиях активного противодействия;
– **Гараган** Сергей Александрович (2002), разработавший теоретические основы организации и технологии постановки специальных задач силам и средствам объектов новой техники;
– **Сухов** Андрей Владимирович (2005), разработавший теоретические основы обеспечения информационного противодействия при отработке объектов новой техники в АСУ ОКНТ;
– **Гончаров** Владимир Васильевич (2008), разработавший теоретические основы обоснования интегрированных систем информационной безопасности объектов новой техники;
– **Лебедев** Георгий Станиславович (2009), разработавший теоретические основы информационного обеспечения телеизмерений и теледиагностики в АСУ;
– **Князев** Владимир Владимирович (2010), разработавший теоретические основы обеспечения заданного качества измерительной информации в АСУ ОКНТ;
– **Байрамов** Казым Рашид оглы (2012), разработавший теоретические основы оперативных навигационных определений в АСУ ОКНТ;
– **Богданова** Марина Валерьевна (2012), разработавшая теоретические основы управления оборотом результатов интеллектуальной деятельности предприятий оборонно-промышленного комплекса.

Признание достижений научной школы подтверждается, в частности, присуждением двух ведомственных премий авторским коллективам членов научной школы за научные разработки (2004, 2007 гг.), получением наград и дипломов ежегодных Всероссийских научно-технических выставок «Армия», «Диверсификация ОПК: технологии двойного применения», Международных форумов «Высокие технологии XXI века», «Интерполитех», «Expopriority», ежегодного Международного салона промышленной собственности «Архимед» и др., а также награждением членов научной школы ведомственными медалями, почётными знаками и грамотами.

В частности, в конкурсе на лучшие научные разработки РВСН в 2004 г. научно-исследовательской работе «Теоретические и экспериментальные исследования и разработка информационно-математического обеспечения АСУ ОКНТ» присуждена первая премия, а членам авторского коллектива — дипломы 1 степени (Д. А. Ловцов — руководитель, А. И. Башилов, Ю. Г. Булычёв, А. А. Ефименко, А. В. Зайцев).

В конкурсе на лучшие научные разработки РВСН в 2007 г. вторая премия присуждена научной разработке «Научно-методическое обеспечение планирования активного лётного эксперимента для организации лётной отработки образцов новой техники в АСУ ОКНТ», членам авторского коллектива — дипломы 2 степени (Д. А. Ловцов — руководитель, А. А. Ефименко, А. В. Зайцев, Д. С. Карпов, А. А. Микрюков).

В 1996–2020 гг. получено более 50 патентов на изобретения. Среди них такие, как системы защиты информации, системы управления малыми космическими и летательными аппаратами, регистрации событий в специальных системах, альтернативная энергетика и другие инновационные направления. За успехи в изобретательской работе ответственный за это направление С. Н. Куканков отмечен медалью Ордена «За заслуги перед Отечеством» II степени.

Признание достижений МНПШ подтверждается также присвоением членам научной школы почётных званий:

«Заслуженный деятель науки РФ» — Д. А. Ловцову, В. В. Омельченко;

«Заслуженный работник высшей школы РФ» — В. В. Гончарову, А. В. Зайцеву;

«Заслуженный машиностроитель РФ» — В. В. Муравнику;

«Почётный работник высшего профессионального образования РФ» — Д. А. Ловцову, В. В. Гончарову;

«Почётный радист РФ» — Д. А. Ловцову;

«Отличник статистики РФ» — М. В. Богдановой;

«Почётный профессор ВА РВСН им. Петра Великого» — Д. А. Ловцову, В. В. Гончарову.

Избраны действительными членами (академиками) Академии военных наук РФ Д. А. Ловцов (2001), В. В. Гончаров (2009) и В. В. Бетанов (2017); членом-корреспондентом РАРАН — В. В. Бетанов (1997).

Современное состояние МНПШ характеризуется постоянным расширением предметной области научных исследований, которая включает уже ряд относительно самостоятельных направлений, включая такие, как:

– системная информатизация управления силами и средствами ракетных и космических комплексов (с 1991 г.) — на базе Военной академии им. Ф. Э. Дзержинского (с 1997 г. — ВА имени Петра Великого);

– системная информатизация правового регулирования информационных отношений в инфосфере» (с 2004 г.) — на базе Российского государственного университета правосудия[2];

[2] *Ловцов Д. А.* Системная информатизация правового регулирования информационных отношений в инфосфере // Российское правосудие. 2018. № 51. С. 120–130.

– обеспечение информационной безопасности и защита ядерного оружия от несанкционированного применения в АСУ специального назначения (с 2017 г.) — на базе ВА им. Петра Великого («ВНШ-412»)[3];

– обеспечение информационной безопасности и защита от несанкционированных действий в АСУ войсками, оружием и робототехническими комплексами военного (специального) назначения (с 2020 г.) — на базе ВА им. Петра Великого.

Лидерами МНПШ в настоящее время являются учёные высшей квалификации, среди которых наибольшую известность получили доктора технических наук, члены докторских диссертационных советов, активные члены редакционной коллегии известного научно-практического журнала «Правовая информатика»:

- Профессор **Д. А. Ловцов**, подготовивший 7 докторов и 35 кандидатов наук и издавший 15 научных монографий, из них 6 — во всероссийских изданиях; имеет 35 работ в журналах Российской академии наук. *В настоящее время — профессор* Военной академии им. Петра Великого и заместитель директора по научной работе Института точной механики и вычислительной техники имени С. А. Лебедева Российской академии наук; член докторских диссертационных советов Военной академии им. Петра Великого, Института точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук (заместитель председателя совета), Научно-производственного объединения «Элерон» Росатома.

Бетанов
Владимир Вадимович

- Профессор **В. В. Бетанов**, подготовивший 3 докторов и 9 кандидатов наук и издавший 12 научных монографий, из них 7 — во всероссийских изданиях; имеет 12 работ в журналах Российской академии наук. В настоящее время — заместитель начальника центра АО «Российские космические системы»; член докторских диссертационных советов МВТУ им. Н. Э. Баумана (двух), АО «Ракетно-космические системы» Роскосмоса.

Сухов
Андрей Владимирович

- Профессор **А. В. Сухов**, подготовивший 2 докторов и 7 кандидатов наук и издавший 3 монографии; имеет 4 работы в журналах Российской академии наук. В настоящее время — профессор Военной академии им. Петра Великого и Московского авиационного института; член докторских диссертационных советов Военной академии им. Петра Великого, ФГУП «Стандартинформ», АО «Ракетно-космические системы» Роскосмоса.
- Профессор **В. В. Омельченко**, подготовивший 5 кандидатов наук и издавший 10 научных монографий, из них 6 — во всероссийских изданиях; имеет 2 работы в журналах Российской академии наук. В настоящее время — советник секретариата НТС по науке Военно-промышленной корпорации «НПО Машиностроения»; член докторских диссертационных советов Института точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук, ВПК «НПО Машиностроения».

Омельченко
Виктор Валентинович

В составе МНПШ ряд молодых ученых активно работают в настоящее время над докторскими диссертациями (Д. А. Гаврилов, М. И. Кудряшов, В. Е. Вовасов, Г. И. Андреев, Ф.А. Самсонов, С. А. Федосеев и др.), научными консультантами которых выступают лидеры научной школы.

В работе данной межвузовской научной школы в разное время по отдельным научным вопросам принимали участие известные учёные: заслуженные деятели науки РФ, доктора технических наук, профессора Ю.Г. Булычёв, Б.И. Глазов, А.П. Панюков, В.А. Цимбал; заслуженный работник высшей школы РФ, лауреат Государственной премии, доктор физико-математических наук, профессор А.В. Чечкин; заслуженный конструктор РФ, доктор физико-математических наук, профессор А.В. Князев; доктор технических наук, профессор, академик РАЕН,

[3] *См.:* «ВНШ-412»: Обеспечение информационной безопасности и защита ядерного оружия от несанкционированного применения в АСУ войсками, оружием и РТК ВН // 200 лет ВА РВСН им. Петра Великого. Наши достижения 2015–2020. – Балашиха: ВА им. Петра Великого, 2020. С. 38, 46–47.

РАРАН, РИА В.А. Дементьев; лауреат премии Правительства РФ, доктор военных наук, профессор Н.Е. Соловцов; лауреат Государственной премии имени Г.К. Жукова, доктор военных наук, профессор В.Ф. Лата; доктор технических наук, профессор В.В. Васильев; доктор технических наук, профессор А.И. Башилов, доктор технических наук А.С. Бурый и многие другие.

Результаты работы научной школы в целом обеспечили создание *научно-методической базы*, позволяющей её членам сосредоточить свои усилия в настоящее время на новых приоритетных наукоёмких направлениях деятельности, включая, в частности, стратегическое прогнозирование и обоснование государственных программ вооружения и гособоронзаказа на основе имитационно-игрового моделирования процессов развития систем ВВСТ.

Сегодня, в год своего 30-летия, МНПШ «Системная информатизация управления сложноорганизованными объектами» успешно развивается и нацелена на достижение новых значимых результатов.

Литература

1. Гончаров В. В., Карпов Д. С. Системная информатизация управления силами и средствами ракетных и космических комплексов // Летопись Военной академии РВСН им. Петра Великого. Т. 5. Научные школы Военной академии РВСН им. Петра Великого. История развития / Под ред. Н. Е. Соловцова. М.: ВА РВСН, 2010. С. 212–216.
2. Пинчук А. В. Двадцать лет научной школе «Системной информатизации управления силами и средствами ракетных и космических комплексов» // Петровский вестник. 2011. № 5(46). С. 14–15.
3. Калинин В. Н. Теоретические основы управления активными подвижными объектами. – Л.: ЛВИА им. А. Ф. Можайского, 1974. 130 с.
4. Килин Ф. М. Теория и принципы построения автоматизированных систем управления. – Л.: ЛВИА им. А. Ф. Можайского, 1974. 263 с.
5. Мамиконов А. Г. Управление и информация. М.: Наука, 1975. 184 с.
6. Резников Б. А. Анализ и оптимизация сложных систем. Планирование и управление в АСУ. Л.: ЛВИИ им. А. Ф. Можайского, 1981. 148 с.
7. Солодов А. В. Теория информации и ее применение к задачам автоматического управления и контроля. М.: Наука, 1967. 432 с.
8. Ловцов Д. А. Информационная теория эргасистем. Тезаурус: Монография. М.: Наука, 2005. 248 с. ISBN 5-02-033779-X.
9. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере : монография. М.: Рос. гос. ун-т правосудия, 2016. 316 с. ISBN 978-5-93916-505-1
10. Ловцов Д. А. Введение в информационную теорию АСУ: Монография. М.: ВА им. Петра Великого, 1996. 434 с.
11. Ловцов Д. А. Терминология информационной теории АСУ // Военный энциклопедический словарь РВСН / Гл. ред. И. Д. Сергеев. М.: Большая Российская энциклопедия, 1999. 632 с. (С. 16, 40, 48, 210–213, 226, 405, 478, 516, 577, 595, 605). ISBN 5-85270-315-X.
12. Ловцов Д. А., Гаврилов Д. А. Моделирование оптико-электронных систем дистанционно пилотируемых аппаратов: Монография. М.: Технолоджи-3000, 2019. 164 с. ISBN 978-5-94472-036-8.
13. Ловцов Д. А., Сергеев Н. А. Управление безопасностью эргасистем : монография / Под ред. Д. А. Ловцова. М.: РАУ Университет, 2001. 224 с. ISBN 5-86014-131-9.
14. Ловцов Д. А., Богданова М. В., Лобан А. В., Паршинцева Л. С. Статистика (компьютеризированный курс): Учебник / Под ред. Д. А. Ловцова. М.: Росс. гос. ун-т правосудия, 2020. 400 с. ISBN 978-5-93916-834-2.
15. Ловцов Д. А., Черных А. М. Геоинформационные системы. – М.: Росс. гос. ун-т правосудия, 2012. 188 с. ISBN 978-5-93916-340-8.
16. Лобан А. В. Информационная технология распределенного диагностирования космических аппаратов: Монография. М., Берлин: Директ-Медиа, 2015. 146 с. ISBN 978-5-4475-4451-5.
17. Бетанов В. В. Введение в теорию решения обобщенных некорректных задач НБО управления ЛА. М.: ВА им. Петра Великого, 1997. 365 с.
18. Бетанов В. В. Терминология баллистико-навигационного обеспечения РКВ // Военный энциклопедический словарь РВСН / Гл. ред. И. Д. Сергеев. М.: Большая Российская энциклопедия, 1999. 632 с. (С. 44–46, 137, 358, 359, 361, 365, 409, 550, 5551). ISBN 5-85270-315-X.
19. Бетанов В. В., Тюлин А. Е. Лётные испытания космических объектов. Определение и анализ движения по экспериментальным данным : монография. М.: Радиотехника, 2016. 332 с.
20. Бетанов В. В., Тюлин А. Е., Яшин В. Г. Орбитальные сегменты космических систем пространственно-временного обеспечения : монография. Ч. 1. Орбитальное движение, маневры и методы определения параметров орбит космических аппаратов / Под ред. А. Е. Тюлина. М.: Инновационное машиностроение, 2020. 336 с. ISBN 978-5-907104-33-4.
21. Бетанов В. В., Тюлин А. Е., Кобзарь А. А. Навигационно-баллистическое обеспечение полета ракетно-космических средств: Монография. Кн. 1. Методы, модели и алгоритмы оценивания параметров движения. М.: Радиотехника, 2018. 479 с.

22. Бетанов В. В., Тюлин А. Е., Юрасов В. С., Стрельников С. В. Навигационно-баллистическое обеспечение полета ракетно-космических средств : монография. Кн. 2. Системный анализ НБО. М.: Радиотехника, 2018. 486 с.
23. Бетанов В. В., Тюлин А. Е., Ларин В. К. Системный подход к решению задач информационного обеспечения управления КА. М.: Радиотехника, 2018. 252 с.
24. Бетанов В. В., Лысенко Л. Н., Звягин Ф. В. Теоретические основы баллистико-навигационного обеспечения космических полётов : монография. М.: Изд-во МГТУ им. Н. Э. Баумана, 2014. 520 с. ISBN 978-5-7038-3891-4.
25. Бетанов В. В., Байрамов К. Р., Ступак Г. Г., Урличич Ю. М. Управление космическими объектами. Методы, модели и алгоритмы решения некорректных задач навигационно-баллистического обеспечения : монография. М.: Радиотехника, 2012. 360 с. ISBN 978-5-88070-335-7.
26. Информатизация управления: монография / Д. А. Ловцов, А. В. Сухов, А. В. Чечкин и др. Под ред. Д. А. Ловцова. М.: ВА им. Петра Великого, 2003. 263 с.
27. Информационно-измерительное обеспечение натурных испытаний сложных технических комплексов : монография / Под общ. ред. А. П. Панина и В. В. Васильева. М.: «Машиностроение — Полёт», 2016. 439 с. ISBN 978-5-9906491-3-2.
28. Информатика и математика : учебник / Под ред. Д. А. Ловцова. М.: «Высшая школа», 2008. 308 с. ISBN 978-5-06-005945-8.
29. Омельченко В. В. Общая теория классификации : монография. В 2-х ч. Ч. 1. Основы системологии познания действительности / Предисл. Д. А. Ловцова. М.: «Книжный мир», 2008. 434 с. ISBN 978-5-91146-297-0.
30. Омельченко В. В. Общая теория классификации : монография. В 2-х ч. Ч. 2. Теоретико-множественные основания. М.: Кн. дом «Либроком», 2010. 296 с. ISBN 978-5-397-01327-7.
31. Омельченко В. В. Основы цветокодирования : монография. Кн. 1. Методологические аспекты цветокодирования информации. М.: «Ленанд», 2019. 230 с.
32. Омельченко В. В. Основы цветокодирования : монография. Кн. 2. Общие методы цветокодирования информации — государственный контроль и управление по результатам. М.: «Ленанд», 2019. 376 с.
33. Омельченко В. В. Основы систематизации. Методология и философские аспекты. Принципы и законы познания реальной действительности : монография. М.: «Либроком», 2012. 480 с. ISBN 978-5-397-02383-2.
34. Омельченко В. В. Теоретические основы классификации нечётких ситуаций при испытаниях сложных технических комплексов. М.: ВА им. Петра Великого, 1999. 434 с.
35. Программно-математическое обеспечение АСУ космическими аппаратами : учебник / В. В. Бетанов, Д. А. Ловцов, А. В. Сухов и др. Под общ. ред. Д. А. Ловцова. М.: ВА им. Петра Великого, 1995.412 с.
36. Финансовая математика : монография / Д. А. Ловцов, М. В. Богданова, Н. А. Сергеев, и др. Под ред. Ю. М. Осипова, Р. М. Нижегородцева. М.: ТЕИС — МГУ, 2001. 416 с. ISBN 5-7218-0327-4.
37. Богданова М. В. Экономические и организационно-правовые механизмы управления результатами интеллектуальной деятельности предприятий оборонно-промышленного комплекса : монография. М.: Гос. ун-т упр-я, 2008. 248 с.
38. Зайцев А. В. Пути повышения точности систем управления летательных аппаратов в условиях активного противодействия. М.: ВА им. Петра Великого, 2009. 375 с.
39. Князев В. В. Методологические основы формализации обеспечения информационной безопасности отработки качества сложных динамических объектов. М.: ВА им. Петра Великого, 2009. 307 с.
40. Государство и право в новой цифровой реальности : монография / Под общ. ред. Д. А. Ловцова, И. А. Конюховой-Умновой. М.: ИНИОН РАН, 2020. 259 с. ISBN 978-5-248-00959-6.
41. ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения. М.: Ростехрегулирование, 2008. 32 с. Исполн. А. А. Грушо, А. В. Гусев, Д. Б. Кобелев, Д. А. Ловцов, А. Ф. Ронжин.
42. ГОСТ Р 53113.2-2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 2. Рекомендации по организации защиты. М.: Ростехрегулирование, 2009. 32 с. Исполн. А. А. Грушо, А. В. Гусев, Д. Б. Кобелев, Д. А. Ловцов, А. Ф. Ронжин.

THIRTY YEARS OF THE INTER-UNIVERSITY SCHOOL OF THOUGHT "SYSTEM INFORMATIZATION OF CONTROL OF COMPLEX OBJECTS"

Alexander Pinchuk, *Candidate of military Sciences, Docent, Academic Secretary of the Strategic Missile Force Academy named after Peter the Great, Russian Federation, Moscow.*
E-mail: *pinchuk_alex@inbox.ru*

Keywords: *interuniversity scientific and pedagogical School, system informatization of control, complex objects, scientific works, research work, information and mathematical support, new information technologies, testing the quality of new equipment, information efficiency indicators, automated control systems (ACS).*

Abstract.

Purpose of the article: improving of science and methodical base of information theories of control and ergasystems in terms of economic digitalization and building the Information Society.

Method used: system analysis of the current state and development of profile interuniversity scientific and pedagogical School which supports the researching of information aspects of complex objects control and their trials.

Results: achievements, tasks and forms of development of the known interuniversity scientific and pedagogical School of "system informatization of complex objects control" as scientific-methodical base of industrial creation of efficiency information and mathematical support of new information technologies and its implementation in existing and prospective integrated ACS in order to increase their information efficiency as information systems are investigated; values of a number of base indicators of information efficiency of real ACS as a result of implementation of scientific and scientific-technical developments received by the participants of the scientific School are presented; forms, methods and results of the performance of priority research works and management of scientific work of applicants for academic degrees are considered; the characteristic of the leaders of the scientific School, in which a number of scientist of the top skills is prepared, with the indication of personal achievements, and also the possible new priority knowledge-intensive directions of scientific and pedagogical activity are considered.

References

1. Goncharov V. V., Karpov D. S. Sistemnaia informatizatciia upravleniia silami i sredstvami raketny`kh i kosmicheskikh kompleksov // Letopis` Voennoi` akademii RVSN im. Petra Velikogo. T. 5. Nauchny`e shkoly` Voennoi` akademii RVSN im. Petra Velikogo. Istoriia razvitiia / Pod red. N. E. Solovtcova.M.: VA RVSN, 2010. S. 212-216.
2. Pinchuk A. V. Dvadtcat` let nauchnoi` shkole «Sistemnoi` informatizatcii upravleniia silami i sredstvami raketny`kh i kosmicheskikh kompleksov» // Petrovskii` vestneyk. 2011. № 5(46). S. 14-15.
3. Kalinin V. N. Teoreticheskie osnovy` upravleniia aktivny`mi podvizhny`mi ob``ektami. L.: LVIA im. A. F. Mozhai`skogo, 1974. 130 s.
4. Kilin F. M. Teoriia i printcipy` postroeniia avtomatizirovanny`kh sistem upravleniia. L.: LVIA im. A. F. Mozhai`skogo, 1974. 263 s.
5. Mamikonov A. G. Upravlenie i informatciia. M.: Nauka, 1975. 184 s.
6. Reznikov B. A. Analiz i optimizatciia slozhny`kh sistem. Planirovanie i upravlenie v ASU. L.: LVII im. A. F. Mozhai`skogo, 1981. 148 s.
7. Solodov A. V. Teoriia informatcii i ee primenenie k zadacham avtomaticheskogo upravleniia i kontrolia. M.: Nauka, 1967. 432 s.
8. Lovtcov D. A. Informatcionnaia teoriia e`rgasistem. Tezaurus : monografiia. M.: Nauka, 2005. 248 c. ISBN 5-02-033779-X.
9. Lovtcov D. A. Sistemologiia pravovogo regulirovaniia informatcionny`kh otnoshenii` v infosfere : monografiia. M.: Ros. gos. un-t pravosudiia, 2016. 316 s. ISBN 978-5-93916-505-1
10. Lovtcov D. A. Vvedenie v informatcionnuiu teoriiu ASU: Monografiia. M.: VA im. Petra Velikogo, 1996. 434 c.
11. Lovtcov D. A. Terminologiia informatcionnoi` teorii ASU // Voenny`i` e`ntciclopedicheskii` slovar` RVSN / Gl. red. I. D. Sergeev. M.: Bol`shaia Rossii`skaia e`ntciclopediia, 1999. 632 s. (S. 16, 40, 48, 210–213, 226, 405, 478, 516, 577, 595, 605). ISBN 5-85270-315-X.
12. Lovtcov D. A., Gavrilov D. A. Modelirovanie optiko-e`lektronny`kh sistem distantcionno pilotiruemy`kh apparatov : monografiia. M.: Tekhnolodzhi-3000, 2019. 164 s. ISBN 978-5-94472-036-8.
13. Lovtcov D. A., Sergeev N. A. Upravlenie bezopasnost`iu e`rgasistem : monografiia / Pod red. D. A. Lovtcova. M.: RAU — Universitet, 2001. 224 c. ISBN 5-86014-131-9.
14. Lovtcov D. A., Bogdanova M. V., Loban A. V., Parshintceva L. S. Statistika (komp`iuterizirovanny`i` kurs): Uchebnik / Pod red. D. A. Lovtcova. M.: Ross. gos. un-t pravosudiia, 2020. 400 s. ISBN 978-5-93916-834-2.
15. Lovtcov D. A., Cherny`kh A. M. Geoinformatcionny`e sistemy`. M.: Ross. gos. un-t pravosudiia, 2012. 188 s. ISBN 978-5-93916-340-8.
16. Loban A. V. Informatcionnaia tekhnologiia raspredelennogo diagnostirovaniia kosmicheskikh apparatov : monografiia. M., Berlin: Direkt-Media, 2015. 146 s. ISBN 978-5-4475-4451-5.
17. Betanov V. V. Vvedenie v teoriiu resheniia obobshchenny`kh nekorrektny`kh zadach NBO upravleniia LA. M.: VA im. Petra Velikogo, 1997. 365 s.
18. Betanov V. V. Terminologiia ballistiko-navigatcionnogo obespecheniia RKV // Voenny`i` e`ntciclopedicheskii` slovar` RVSN / Gl. red. I. D. Sergeev. M.: Bol`shaia Rossii`skaia e`ntciclopediia, 1999. 632 s. (S. 44-46, 137, 358, 359, 361, 365, 409, 550, 5551). ISBN 5-85270-315-X.
19. Betanov V. V., Tiulin A. E. Lyotny`e ispy`taniia kosmicheskikh ob``ektov. Opredelenie i analiz dvizheniia po e`ksperimental`ny`m danny`m : monografiia. M.: Radiotekhnika, 2016. 332 s.

20. Betanov V. V., Tiulin A. E., Iashin V. G. Orbital`ny`e segmenty` kosmicheskikh sistem prostranstvenno-vremennogo obespecheniia: Monogorafiia. Ch. 1. Orbital`noe dvizhenie, manevry` i metody` opredeleniia parametrov orbit kosmicheskikh apparatov / Pod red. A. E. Tiulina. M.: Innovatcionnoe mashinostroenie, 2020. 336 s. ISBN 978-5-907104-33-4.
21. Betanov V. V., Tiulin A. E., Kobzar` A. A. Navigatcionno-ballisticheskoe obespechenie poleta raketno-kosmicheskikh sredstv: Monografiia. Kn. 1. Metody`, modeli i algoritmy` ocenivaniia parametrov dvizheniia. M.: Radiotekhnika, 2018. 479 s.
22. Betanov V. V., Tiulin A. E., Iurasov V. S., Strel`nikov S. V. Navigatcionno-ballisticheskoe obespechenie poleta raketno-kosmicheskikh sredstv : monografiia. Kn. 2. Sistemny`i` analiz NBO. M.: Radiotekhnika, 2018. 486 s.
23. Betanov V. V., Tiulin A. E., Larin V. K. Sistemny`i` podhod k resheniiu zadach informatcionnogo obespecheniia upravleniia KA. M.: Radiotekhnika, 2018. 252 s.
24. Betanov V. V., Ly`senko L. N., Zviagin F. V. Teoreticheskie osnovy` ballistiko-navigatcionnogo obespecheniia kosmicheskikh polyotov : monografiia. M.: Izd-vo MGTU im. N. E`. Baumana, 2014. 520 s. ISBN 978-5-7038-3891-4.
25. Betanov V. V., Bai`ramov K. R., Stupak G. G., Urlichich Iu. M. Upravlenie kosmicheskimi ob``ektami. Metody`, modeli i algoritmy` resheniia nekorrektny`kh zadach navigatcionno-ballisticheskogo obespecheniia: monografiia. M.: Radiotekhnika, 2012. 360 s. ISBN 978-5-88070-335-7.
26. Informatizatciia upravleniia: Monografiia / D. A. Lovtcov, A. V. Suhov, A. V. Chechkin i dr. Pod red. D. A. Lovtcova. M.: VA im. Petra Velikogo, 2003. 263 c.
27. Informatcionno-izmeritel`noe obespechenie naturny`kh ispy`tanii` slozhny`kh tekhnicheskikh kompleksov : Monografiia / Pod obshch. red. A. P. Panina i V. V. Vasil`eva. M.: «Mashinostroenie — Polyot», 2016. 439 s. ISBN 978-5-9906491-3-2.
28. Informatika i matematika : uchebnik / Pod red. D. A. Lovtcova. M.: «Vy`sshaia shkola», 2008. 308 c. ISBN 978-5-06-005945-8.
29. Omel`chenko V. V. Obshchaia teoriia classifikatcii : monografiia. V 2-kh ch. Ch. 1. Osnovy` sistemologii poznaniia dei`stvitel`nosti / Predisl. D. A. Lovtcova. M.: «Knizhny`i` mir», 2008. 434 s. ISBN 978-5-91146-297-0.
30. Omel`chenko V. V. Obshchaia teoriia classifikatcii : monografiia. V 2-kh ch. Ch. 2. Teoretiko-mnozhestvenny`e osnovaniia. M.: Kn. dom «Leebrokom», 2010. 296 s. ISBN 978-5-397-01327-7.
31. Omel`chenko V. V. Osnovy` tcvetokodirovaniia : monografiia. Kn. 1. Metodologicheskie aspekty` tcvetokodirovaniia informatcii. M.: «Lenand», 2019. 230 s.
32. Omel`chenko V. V. Osnovy` tcvetokodirovaniia : monografiia. Kn. 2. Obshchie metody` tcvetokodirovaniia informatcii — gosudarstvenny`i` kontrol` i upravlenie po rezul`tatam. M.: «Lenand», 2019. 376 s.
33. Omel`chenko V. V. Ocnovy` sistematizatcii. Metodologiia i filosofskie aspekty`. Printcipy` i zakony` poznaniia real`noi` dei`stvitel`nosti: Monografiia. M.: «Leebrokom», 2012. 480 s. ISBN 978-5-397-02383-2.
34. Omel`chenko V. V. Teoreticheskie osnovy` classifikatcii nechyotkikh situatcii` pri ispy`taniiakh slozhny`kh tekhnicheskikh kompleksov. M.: VA im. Petra Velikogo, 1999. 434 c.
35. Programmno-matematicheskoe obespechenie ASU kosmicheskimi apparatami: Uchebnik / V. V. Betanov, D. A. Lovtcov, A. V. Suhov i dr. Pod obshch. red. D. A. Lovtcova. M.: VA im. Petra Velikogo, 1995. 412 c.
36. Finansovaia matematika : monografiia / D. A. Lovtcov, M. V. Bogdanova, N. A. Sergeev, i dr. Pod red. Iu. M. Osipova, R. M. Nizhegorodtceva. M.: TEIS — MGU, 2001. 416 s. ISBN 5-7218-0327-4.
37. Bogdanova M.V. E`konomicheskie i organizatcionno-pravovy`e mehanizmy` upravleniia rezul`tatami intellektual`noi` deiatel`nosti predpriiatii` oboronno-promy`shlennogo kompleksa : monografiia. M.: Gos. un-t upr-ia, 2008. 248 s.
38. Zai`tcev A. V. Puti povy`sheniia tochnosti sistem upravleniia letatel`ny`kh apparatov v usloviiakh aktivnogo protivodei`stviia. M.: VA im. Petra Velikogo, 2009. 375 s.
39. Kniazev V. V. Metodologicheskie osnovy` formalizatcii obespecheniia informatcionnoi` bezopasnosti otrabotki kachestva slozhny`kh dinamicheskikh ob``ektov. M.: VA im. Petra Velikogo, 2009. 307 s.
40. Gosudarstvo i pravo v novoi` tcifrovoi` real`nost i: monografiia / Pod obshch. red. D. A. Lovtcova, I. A. Koniuhovoi`-Umnovoi`. M.: INION RAN, 2020. 259 s. ISBN 978-5-248-00959-6.
41. GOST R 53113.1-2008. Informatcionnaia tekhnologiia. Zashchita IT i AS ot ugroz informatcionnoi` bezopasnosti, realizuemy`kh s ispol`zovaniem skry`ty`kh kanalov. Ch. 1. Obshchie polozheniia. M.: Rostekhregulirovanie, 2008. 32 s. Ispoln. A. A. Grusho, A. V. Gusev, D. B. Kobelev, D. A. Lovtcov, A. F. Ronzhin.
42. GOST R 53113.2-2009. Informatcionnaia tekhnologiia. Zashchita IT i AS ot ugroz informatcionnoi` bezopasnosti, realizuemy`kh s ispol`zovaniem skry`ty`kh kanalov. Ch. 2. Rekomendatcii po organizatcii zashchity`. M.: Rostekhregulirovanie, 2009. 32 s. Ispoln. A. A. Grusho, A. V. Gusev, D. B. Kobelev, D. A. Lovtcov, A. F. Ronzhin.

Над номером работали:

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