Правовая информатика

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
№ 4, 2018 г.
Выходит 4 раза в год

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

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

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 20.12.2018 г.
Общий тираж 100 экз. Цена свободная.

Адрес редакции:
125437, Москва, Михалковская ул.,
65, стр.1
Телефон: +7 (495) 539-25-29
E-mail: inform360@yandex.com
Требования, предъявляемые к рукописям, размещены на сайте
http://uzulo.su/prav-inf/ru/ru_i.htm

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс: 44723

LEGAL INFORMATICS

RESEARCH AND PRACTICE JOURNAL
2018, No. 3
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 2nd of November 1996.

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

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 20th of December, 2018.
Number of items printed: 100. Free price.

Postal address:
Mikhalkovskaya str., bld. 65/1,
125 438, Moscow, Russia
Telephone: +7 (495) 539-23-14
E-mail: inform360@yandex.com
Guidelines for preparing manuscripts for publication can be found on the website
http://uzulo.su/prav-inf/ru/ru_i.htm

CONTENTS

The journal can be subscribed to at post offices through the Press of Russia (Pressa Rossii) Catalogue. Publication index: 44740.

ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ В СИСТЕМЕ БОРЬБЫ С «ОТМЫВАНИЕМ» ПРЕСТУПНЫХ ДОХОДОВ: РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД

*Ващекин А. Н., Ващекина И. В.**

Ключевые слова: *«отмывание» нелегальных доходов, информационное взаимодействие, финансовый мониторинг, международные объединения российские организации, риски, методы противодействия, внешнеполитический кризис.*

Аннотация.

Цель: *исследование информационного взаимодействия в системе противодействия «отмыванию» преступных доходов и финансированию терроризма (ПОД/ФТ), задачей которой является осуществление финансового мониторинга с целью предотвращения функционирования «теневого» сектора экономики, формирования организованной преступности и осуществления террористической деятельности в мировом сообществе.*

Методы: *аналитический и экспертный методы системного анализа и математическое моделирование.*

Результаты*: определены основные уровни функционирования системы ПОД/ФТ, первый из которых формируется международными объединениями, второй – общенациональными структурами ПОД/ФТ, третий – отдельными финансовыми и коммерческими организациями, взаимодействующими с первыми двумя уровнями и в пределах полномочий контролируемыми ими. Российская национальная система ПОД/ФТ опирается на взаимодействие Росфинмониторинга, Банка России и других организаций, перечень которых определяется российским законодательством. Они обеспечивают соответствие деятельности российских кредитных организаций рекомендациям ФАТФ, Вольфсбергским принципам, взаимодействие с ЕАГ и Эгмонт, меры по снижению Базельского AML-индекса России.*

Обоснована необходимость международного информационного взаимодействия в борьбе с «отмыванием» нелегальных доходов как одной из задач обеспечения конкурентоспособности отечественной экономики, способствующей созданию позитивного инвестиционного климата, повышающей международный авторитет страны в целом, усиливающей ее политические позиции. Рекомендовано применение риск-ориентированного подхода как методологической основы при организации финансового мониторинга на основе освоения зарубежной практики ПОД/ФТ. Оценку риска предложено проводить с опорой на модернизированные вероятностные методы и метод нечетких множеств.

DOI:10.21681/1994-1404-2018-4-04-14

Введение

Непрерывный процесс глобальной информатизации, развитие международного сотрудничества в разнообразных областях, деятельность транснациональных корпораций, распространение международных торговых и финансовых операций вызвали в последние десятилетия значительное увеличение трансграничных переводов. Количественное их увеличение уже само по себе затрудняет контроль за легальностью и прозрачностью операций, а вследствие формирования новых взаимно сопряженных структур и развития *информационных технологий*, активно применяющихся в финансовой сфере вследствие информационной природы платежных средств, эти трудности увеличиваются многократно [13].

Государственные и финансовые организации развитых стран, учитывая потенциальную общественную опасность вовлечения национальных финансовых рынков и банковских структур в процессы легализации преступных доходов и формирования теневой экономики, ещё в конце прошлого века стали обмениваться необходимой информацией и вырабатывать *организационно-правовые меры* по предотвращению отрицательного влияния преступных финансовых операций, как на национальные экономики, так и на мировую хозяйственную систему в целом.

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

Email: vaschekin@mail.ru

Ващекина Ирина Викторовна*, кандидат экономических наук, доцент, доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Россия.*

E-mail: vaschekina@mail.ru

В последние десятилетия значение международных организаций, действующих в целях контроля и противодействия «отмыванию» доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ) постоянно возрастает [9]. При этом сложилась *многоуровневая* система обмена информацией, мониторинга и взаимного контроля, образуемая организациями на трех уровнях, *первый* из которых формируется международными объединениями, *второй* – общенациональными структурами ПОД/ФТ, *третий* – отдельными финансовыми и коммерческими организациями, взаимодействующими с первыми двумя уровнями и в пределах полномочий контролируемыми ими.

1. Международные объединения ПОД/ФТ

Первые шаги по контролю за финансовым «отмыванием» денег были сделаны в 1974 г., когда для выработки рекомендаций по правилам и методам *контроля* за банковскими операциями был образован Базельский комитет. Сейчас членами комитета являются представители 10 государств: Бельгии, Великобритании, Германии, Италии, Канады, США, Франции, Швеции, Швейцарии, Японии. В 1988 г. комитет опубликовал Базельскую декларацию, направленную на защиту банковской системы от использования при «отмывании» доходов от наркоторговли – наиболее значимой составляющей доходов в сфере организованной преступности (задачи комитета впоследствии были расширены).

В 1989 г. по инициативе стран «большой семерки» образовалась группа по разработке рекомендаций, направленных на противодействие «отмыванию» преступных доходов (*Financial Action Task Force on Money Laundering – FATF*). ФАТФ является межправительственной организацией, определяющей общие стандарты в сфере противодействия «отмыванию» преступных доходов и финансированию терроризма, а также оценивающей соответствие национальных систем ПОД/ФТ отдельных стран своим стандартам. ФАТФ стала самым значительным объединением в этой сфере, включающей 35 стран и две международные организации (Еврокомиссия и Совет сотрудничества арабских государств Персидского залива, а в ранге наблюдателей – ещё 20 организаций и две страны – Израиль и Саудовская Аравия). ФАТФ тесно взаимодействует с МВФ, Всемирным банком, Управлением ООН по наркотикам и преступности, реализующими собственные программы, нацеленные на противодействие «отмыванию» денег.

Основной целью ФАТФ видит установление *стандартов* и содействие эффективному осуществлению правовых, нормативных и оперативных мер по борьбе с «отмыванием» денег, финансированием терроризма и другими связанными с ними угрозами целостности международной финансовой системы. Организацией подготовлен список из сорока рекомендаций, которые не носят обязательного характера и не содержат жестких требований, поскольку признают различия в законодательствах разных стран. Тем не менее, они составлены с учетом максимального территориального охвата без потери информационной составляющей. С 2000 г. рекомендации ФАТФ распространяются в том числе и на страны, не входящими в эту организацию в ранге действительных членов. В мире функционирует также несколько *региональных групп*, функционально напоминающих ФАТФ и осуществляющих с ней тесное информационное взаимодействие, с другими ключевыми международными институтами, а также между собой. По мере накопления опыта в разработке рекомендаций в области ПОД/ФТ, а также с ростом интенсивности безналичного оборота в международных финансовых расчетах, авторитет ФАТФ возрастает.

Первый список рекомендаций ФАТФ был предложен еще в 1990 г. для защиты финансовых систем от лиц, «отмывающих» денежные средства, полученные от наркоторговли. В 1996 г. список получил развитие на основе изучения новых тенденций, приемов «отмывания», а также расширения сферы применения этих приемов за пределы сферы торговли наркотиками. П стал осле использования резонансных терактов в США в 2001 г. ФАТФ существенно расширила сферу своей деятельности, распространив ее на предупреждение финансового обеспечения террористических организаций.

В результате возникли восемь дополнительных рекомендаций по борьбе с финансированием терроризма (позднее добавили девятую). В последующие годы борьба ФАТФ с финансовой поддержкой международного терроризма вышла на передний план и информационное взаимодействие с национальными институтами с целью предупреждения использования легализованных доходов для финансирования терроризма заметно возросло.

Рекомендации ФАТФ со временем стали более целенаправленными. В настоящий момент число государств, которое ими руководствуется, приближается к двум сотням. Наиболее важные рекомендации для финансовых учреждений выглядят следующим образом:

- следует избегать ведения анонимных (или открытых на вымышленные имена) счетов;
- нужно уделять особое внимание любым возможным способам «отмывания» доходов, порождаемым новыми или разрабатываемыми информационными технологиями, повышающих степень анонимности;
- нужно обращать внимание на все сложные и крупные сделки, а также необычные схемы их совершения, имеющие неясную экономическую или законную цель;
- имеет смысл внедрять собственные программы по борьбе с «отмыванием» денег и финансированием терроризма;
- следует уделять особое внимание деловым отношениям и сделкам с лицами (компаниями и учреждениями), зарегистрированными в странах, игнорирующих выполнение рекомендаций ФАТФ.

Также отмечается, что государственным органам необходимо быстро, и конструктивно осуществлять широкую взаимопомощь в связи с проведением расследований, судебным преследованием и сопутствующими процедурами ПОД/ФТ.

Приоритетом ФАТФ на протяжении всего периода деятельности остается обеспечение прозрачности и своевременного доступа к информации о бенефициарном. В 2014 г. ФАТФ выпустила Руководство по прозрачности и бенефициарной собственности, выполнение которого позволяет получить доступ к актуальной информации о корпоративных структурах и установить процедуры для облегчения обработки информационных запросов от зарубежных коллег.

В 2017 г. ФАТФ разработала консолидированные стандарты по обмену информацией, где определены гарантии и меры защиты при взаимном обмене информацией между странами, организациями и предприятиями.

Шесть изложенных выше рекомендаций (всего их сорок) дают достаточное представление о направленности указаний ФАТФ. Они полностью согласуются с деятельностью российских организаций, и прежде всего – Росфинмониторинга, а изложенные в них принципы, прослеживаются в Федеральном законе № 115-ФЗ от 7 августа 2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансирования терроризма». Основные цели этого закона видны из его разделов: предупреждение ОД/ФТ, организация ПОД/ФТ, международное сотрудничество в сфере ПОД/ФТ.

С момента принятия указанного закона на фоне постоянно развивающихся преступных методов в него были внесено пятьдесят поправок в рамках единого систематического подхода к созданию препятствий для совершения экономических преступлений на мировом уровне. В результате Российская Федерация получила возможность не просто эффективно координировать силы уполномоченных организаций, но и действовать в тесном информационном контакте со всеми экономическими системами заинтересованных стран [4].

К ключевым изменениям, внесенным ФАТФ, относятся: риск-ориентированный подход; прозрачность; международное сотрудничество; операционные стандарты; новые угрозы и новые приоритеты (рис. 1).

Рис. 1. Эволюция рекомендаций ФАТФ

Применение рекомендаций ФАТФ способствует решению трех важнейших функциональных *задач*: идентификация участников потенциально нелегальной финансовой операции, фиксирование сведений о подозрительной операции и информирование специального официального органа об этой операции. Однако практические способы выполнения этих процедур международными стандартами четко не регламентируются, поэтому на своем уровне каждая страна формирует собственные подходы к реализации каждого стандарта [14].

В указаниях ФАТФ отмечено, что риски ОД/ФТ нередко сложно четко описать или измерить количественно, однако приблизительную оценку уровня риска можно произвести, исходя из вероятности осуществления рисков и из анализа их последствий. Кроме того, ФАТФ констатирует различия в оценках национального риска ОД/ФТ в разных странах, где применяются как *формальные* методы (статистический анализ, математическое моделирование и др.), так и *экспертные* (выводы и заключения по итогам групповых обсуждений). Заметим, что в отечественной науке вероятностные методы оценки рисков существенно модернизированы и позволяют успешно формализовать экспертные оценки – например, используются копула-функции в многомерных моделях Монте-Карло [11]. Наряду с вероятностными применяются по виду схожие, а по сути принципиально иные математические методы, успешно обеспечивающие представление качественных характеристик информации в количественном виде – методы нечётких множеств [5].

ФАТФ приводит примеры проведения оценок риска на национальном уровне лишь для некоторых стран (США, Австралия, Нидерланды).

Страны, в которых риски наиболее высоки, перечислены в «черном списке ФАТФ», который составляют три группы государств:

- игнорирующие ФАТФ (Иран, Северная Корея), которые характеризуются наибольшим уровнем риска и подвергаются ограничительным мерам;
- взаимодействующие с ФАТФ, но вследствие различных причин обладающие высоким уровнем риска, против которых меры не принимаются (Куба, Боливия, Пакистан, Сирия, Турция);
- декларирующие готовность к сотрудничеству, но не имеющие возможности для полноценного участия в борьбе с экономическими преступлениями (Алжир, Ангола, Камбоджа, Намибия, Туркменистан).

Международные электронные операции, в которых участвуют представители «черного списка ФАТФ», автоматически считаются подозрительными.

В современных условиях наиболее значимым для нашей страны наднациональным *институтом контроля* стало институциональное подразделение ЕврАзЭС – Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ), образованная девятью государствами (Бе-

лоруссия, Индия, Казахстан, Китай, Кыргызстан, Россия, Таджикистан, Туркменистан, Узбекистан). ЕАГ является ассоциированным членом ФАТФ и действует в соответствии с его методологией. Эти страны – надежные экономические партнеры, настроенные на сотрудничество в торговой и финансовой сфере. С учетом роста товарооборота и взаимопроникновения капитала, При составлении рейтинга учитывается также информация *Transparency International*, Всемирного Банка и Всемирного экономического форума.

На протяжении шести лет список стран с наиболее высоким индексом (табл. 1) не претерпевал существенных изменений, а отдельные государства являются его

Таблица 1
Базельский индекс AML

2012	2013	2014	2015	2016	2017
Иран	Афганистан	Иран	Иран	Иран	Иран
Кения	Иран	Афганистан	Афганистан	Афганистан	Афганистан
Камбоджа	Камбоджа	Камбоджа	Таджикистан	Таджикистан	Гвинея-Бисау
ГаитИ	Таджикистан	Таджикистан	Гвинея-Бисау	Уганда	Таджикистан
Таджикистан	Ирак	Гвинея-Бисау	Мали	Гвинея-Бисау	Лаос
Мали	Гвинея-Бисау	Ирак	Камбоджа	Камбоджа	Мозамбик
Уганда	Гаити	Мали	Мозамбик	Мозамбик	Мали
Парагвай	Мали	Свазиленд	Уганда	Мали	Уганда
Белиз	Свазиленд	Мозамбик	Свазиленд	Судан	Камбоджа

представляется обоснованным инициировать разработку стандартизованных средств и методов взаимного обмена информацией в платежном и кредитном секторах, не ограничиваясь лишь общими рекомендациями по типу ФАТФ, чтобы получить в рамках ЕврАзЭС действенный инструмент ПОД/ФТ на основе собственных оценок риска.

В качестве ориентира можно обратиться к изучению опыта специалистов Базельского института управления, оценивающими уязвимость страны к проведению на ее территории нелегальных операций по ОД/ФТ на меры базе «антиотмывочного» индекса (*The Basel AML Index*). Индекс рассчитывается с 2012 г. Риски оцениваются по десятибалльной шкале: чем выше значение индекса, тем больше уязвимость страны к «отмыванию» преступных доходов. Он учитывает риски ОД/ФТ (весовой коэффициент в совокупной оценке составляет 65%), подверженность страны коррупции (10%), прозрачность функционирования государственного и финансового секторов (5% и 15%, соответственно), а также политические риски (5%).

В свою очередь, оценка фактора «риски ОД/ФТ» складывается из результатов взаимной оценки национального режима ПОД/ФТ государства, проведенной ФАТФ или региональной группой, ее заменяющей (30%), индекса финансовой секретности, публикуемого *Tax Justice Network* (25%), и выводов ежегодного доклада Государственного департамента США «О стратегии контроля за международным оборотом наркотиков». постоянными фигурантами[1]. Стоит, однако, заметить, что *AML Index* оценивает не фактически зафиксированные объемы нелегальных операций, а потенциальную уязвимость страны к ОД/ФТ.

Самый высокий (негативный) балл присвоен Ирану (8,60), самый низкий – Финляндии (3,04). Наша страна в рейтинге 2017 г. находится на 64 месте, имея 6,22 балла. В 2016 г. Россия занимала 58 место (с той же оценкой – 6,22 балла).

Другим положительным для нашей страны примером успешно действующей системы реального информационного обмена служит группа Эгмонт – неформальное объединение подразделений финансовой разведки (ПФР), ставшее в последние годы эффективным межправительственным объединением по борьбе с ОД/ФТ. В центре внимания этой группы находится «отмывание» денег, при этом она выполняет важную роль в международных усилиях по борьбе с финансированием терроризма. Финансовая информация, доступная ПФР, распространяется среди национальных ведомств, которые занимаются конкретными расследованиями.

Основная цель группы Эгмонт в настоящее время – *информационное взаимодействие* ПФР во всем мире в целях борьбы с ОД/ФТ, а также для реализации внутренних программ, в том числе расширения и систематизации международного сотрудничества в области

[1] Basel Committee on Banking Supervision. Oficial'nyj sajt [jelektronnyj resurs] – http://www.bis. org/publ/bcbs275.pdf

обмена информацией, обмена кадрами, внедрения современных информационных технологий (глобальная защищенная сеть Эгмонт, *ESW*) и др. Учитывая позитивный опыт, рекомендуется при разработке отечественных информационных систем, обеспечивающих ПОД/ФТ, обеспечивать технологическую совместимость с подобными сетями, а в перспективе – расширить действие этих систем на страны ЕАГ.

И, наконец, немаловажным институтом первого уровня является Вольфсбергская группа (*Wolfsberg group*). Это международное объединение крупнейших мировых банков, которые в 2000 г. выработали собственные принципы противодействия легализации преступных доходов в частном банковском секторе. Всеобщие директивы по противодействию «отмыванию» доходов в частном банковском секторе (Вольфсбергские принципы) подписали ведущие на тот момент банки мира.

Эти *принципы* включают приоритетные направления политики банков по предотвращению использования банковской системы для легализации преступных доходов. Опираясь на них, банки устанавливают отношения только с теми клиентами, законное происхождение доходов которых может быть отметить подтверждено. Включение конкретного механизма противодействия остается на усмотрение банка.

Письмом ЦБ РФ №24-Т от 15 февраля 2001 г. кредитным организациям Российской Федерации было предложено придерживаться Вольфсбергских принципов, и это обеспечило выход России из «черного списка ФАТФ» (2003 г). Некоторых конкретные банки принимали соответствующие решения даже ранее указаний ЦБ, поскольку при установлении корреспондентских отношений иностранные банки часто устанавливали российским партнерам условия по неукоснительному следованию Вольфсбергским принципам. Несмотря на несогласованность и сохранение индивидуальных трактовок, на территории Российской Федерации эти принципы определяли политику отечественных кредитных организаций до формирования Росфинмониторинга, а добросовестные участники рынка придерживаются их без дополнительных указаний [8].

Нетрудно заметить, что принципы, выработанные этой банковской группой во многом схожи с подходами ФАТФ. В них отдельно рассматривается порядок идентификации клиентов, действия при выявлении подозрительных операций, а также механизм формирования отдельных внутрибанковских структур, специализирующихся на ПОД/ФТ. Основная разница состоит в том, что ФАТФ разработала рекомендации на уровне стран, делая упор на работу государства в целом как системы ПОД/ФТ, в то время Вольфсбергская группа ориентируется на отдельные банки. Из этого следует, что для России, в которой банковская система централизована в высокой степени, этот подход вполне применим, и его внедрение может обеспечить высокую степень безопасности банковских операций и надежного противодействия «отмыванию» нелегальных доходов.

2. Национальные организации ПОД/ФТ

Национальные системы ПОД/ФТ обычно включают разнообразные государственные органы, фскн осуществляющие контроль и надзор в осуществляющие области положение ПОД/ФТ. В Российской Федерации это, прежде легализации всего актов, Федеральная служба по финансовому мониторингу (Росфинмониторинг) – федеральный орган исполнительной власти, осуществляющий функции по противодействию легализации преступных доходов, финансированию терроризма и распространения оружия массового уничтожения, по выработке государственной политики и нормативно-правовому регулированию в указанной сфере, по координации соответствующей деятельности других федеральных органов исполнительной власти, иных организаций. Росфинмониторинг также является государственным центром по оценке угроз национальной безопасности, возникающих в результате совершенствования операций (сделок) с денежными средствами или иным имуществом, и по выработке мер противодействия этим угрозам.

На том же уровне находятся и Банк России, производящий контроль и надзор в области ПОД/ФТ в банковской сфере и на финансовых рынках, а также Федеральная налоговая служба (ФНС полученных), Федеральная таможенная служба (ФТС), Пенсионный Фонд России (ПФР), Генеральная прокуратура. Они решают основные задачи по предупреждению, выявлению случаев легализации преступных доходов, недопущению операций по финансированию терроризма.

Позитивным следствием освоения зарубежной практики ПОД/ФТ стало широкое распространение *риск-ориентированного подхода*, ставшего методологической основой при организации финансового планирования в различных сферах экономики. Эта методология заложена в Международные стандарты по противодействию «отмыванию» денег, финансированию терроризма и распространения оружия массового уничтожения ФАТФ, а также отражена в документе «Актуальные вопросы оценки рисков отмывания денег, применения санкций, взяточничества и коррупции», изданном в сентябре 2015 г.

Банк России в своем Информационном письме от 27 декабря 2017 г. № ИН-014-12/64 рекомендует кредитным организациям опираться на риск-ориентированный подход, учитывая, что он позволяет гибко применять меры ПОД/ФТ, с тем, чтобы более эффективно распределить имеющиеся ресурсы и направлять усилия на предупредительные меры в области высокого риска.

Большинство финансовых организаций успешно использует оценки кредитных или рыночных рисков. Специфика оценки финансового преступления состоит в том, что она сосредоточена на оценке «косвенного» риска, отражающего внутреннюю и внешнюю среду финансовой организации, в том числе инструменты контроля, направленные на снижение риска. Тем не

менее, при проведении обоих видов оценки методологии количественной и качественной оценки рисков помогают организациям в оценке рисков, понимании изучаемого явления, анализе источников и влияния риска финансового преступления и разработке инструментов и методов управления этими рисками.

В январе 2014 г. Базельским комитетом были обнародованы рекомендации, в которых отмечено, что эффективное управление риском предусматривает проведение идентификации и анализа рисков «отмывания» денег и финансирования терроризма в банке, а также разработку и эффективное внедрение политики и процедур, соразмерных выявленным рискам. При проведении всесторонней оценки для выявления риска «отмывания» денег и финансирования терроризма, банк должен учитывать все существенные факторы присущего и остаточного риска, чтобы определить соответствующий необходимый уровень их снижения.

Проведение оценки рисков стало привычной практикой во многих странах. Например, в США руководство банка обязано выстраивать банковскую программу в соответствии с профилем риска, идентифицированного по результатам его оценки, разрабатывать соответствующие политику, процедуры и процесс мониторинга и контроля рисков «отмывания» денег[2].

Системы *мониторинга* банка по выявлению, изучению и направлению сообщений о подозрительной деятельности также должны разрабатываться с учетом риска; при этом особое внимание должно уделяться продуктам, услугам, клиентам, лицам и географическим регионам с высоким уровнем риска, идентифицированным банком при проведении оценки. Подобным же образом в Великобритании, Руководство Совместной координационной группы противодействия «отмыванию», опирается на практику применения риск-ориентированного подхода.

Другие подходы к оценке рисков, такие как использование сценариев риска, в рамках которой оцениваются вероятность реализации сценариев ОД/ФТ и степень их воздействия, а также метод расчета присущего риска финансовой организации, также эффективно используются финансовыми организациями [7]. Риск ОД/ФТ тесно связан с другими типами рисков, прежде всего – с репутационным и регуляторным рисками [2].

Так, в 2016 г Центробанк произвел 557 проверок кредитных организаций, по результатам которых за нарушения в сфере ПОД/ФТ были отозваны лицензии на осуществление банковских операций у 35 банков (всего в 2016 г отозвано 97 лицензий), а также у одной некредитной финансовой организации (НФО). Динамика мер воздействия по результатам проверок за 2014 – 2016 гг. представлена в табл. 2[3].

Таблица 2

Меры воздействия, примененные в отношении кредитных организаций

Меры в отношении кредитных Организаций (КО)	2014 г.	2015 г.	2016 г.
Количество проверок КО,	690	626	557
из них в т. ч. по вопросам ПОД/ФТ	-	42%	40%
Отозваны лицензии, в т. ч. в рамках ПОД/ФТ	36	34	35
Предупредительные меры воздействия (кол-во мер/кол-во КО)	133/-	330/-	385/287
Принудительные меры воздействия (кол-во мер/кол-во КО)	1014/-	524/-	1351/560

За последнее десятилетие произошло значительное смещение ожиданий регуляторов в отношении стандартов ПОД/ФТ: если ранее приемлемым считалось следование «хорошей» или «общепринятой» практике, то теперь нормой стало применение наивысших стандартов. По мере роста ожиданий все сложнее становится внедрить действенные процедуры риск-ориентированного подхода, если суждения о нем выносятся на основе нормативного правового регулирования. Издержки, связанные с приведением систем внутреннего контроля в соответствие со стандартами и осуществлением ретроспективного анализа до возникновения нареканий со стороны регулятора, могут быть значительными. За нарушения все чаще применяются санкции, причем нередко со стороны нескольких регулирующих органов, которые инициируют расследования по одним и тем же либо схожим нарушениям.

В отношении российских коммерческих банков оценка риска ОД/ФТ осуществляется на основании «Положения о требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» Центрального банка Российской Федерации от 2 марта 2012 г. № 375-П. В соответствии с ним риск ОД/ФТ складывается из следующих компонентов:

[2] Federal Financial Institutions Examination Council. Официальный сайт [электронный ресурс] https://www.ffiec.gov/financial.htm.

[3] Банк России. Годовой отчет за 2016 г. Официальный сайт [электронный ресурс] http://www.cbr.ru/publ/God/ar_2016.pdf.

- риск совершения клиентом операций в целях ОД/ФТ (или риск клиента) – данный риск связан, прежде всего, с осуществлением клиентами транзитных операций, предшествующих выводу денежных средств за рубеж или их обналичиванию;
- риск вовлеченности кредитной организации и ее сотрудников в использование услуг кредитной организации в целях ОД/ФТ (или риск использования услуг кредитной организации в целях ОД/ФТ) – данный риск связан с осуществлением транзита повышенного риска – схем сомнительных операций (прежде всего, выводу денег за рубеж или их обналичиванию).

3. Нижний уровень системы ПОД/ФТ

Его в нашей стране образуют финансовые посредники – организации, осуществляющие операции с денежными средствами или иным имуществом. Их перечень определяется (и при необходимости дополняется) российским законодательством и в настоящее время включает: кредитные организации; профессиональных участников рынка ценных бумаг; страховые организации и лизинговые компании; организации федеральной почтовой связи; ломбарды; организации, занимающиеся скупкой и куплей-продажей драгоценных металлов, драгоценных камней , ювелирных изделий и лома таких изделий; организации, осуществляющие управление инвестиционными или негосударственными пенсионными фондами; кредитные потребительские кооперативы; микрофинансовые организации.

Все эти организации в обязательном или инициативном порядке информируют Росфинмониторинг о проводимых их клиентами подозрительных операциях с денежными средствами и иным имуществом, которые с высокой долей вероятности указывают на «отмывание» денег.

В России законодательно установлено, что каждая кредитная организация разрабатывает программу управления риском ОД/ФТ, которая является обязательным составным элементом *правил внутреннего контроля*, включает методику выявления и оценки ОД/ФТ в отношении риска клиента и в отношении риска использования услуг кредитной организации в целях ОД/ФТ. При этом подразумевается, что методика выявления и оценки операций на предмет ОД/ФТ формируется каждой организацией самостоятельно, регулятором лишь определены с разной степенью детализации методические рекомендации для его оценки [10].

В отношении НФО действует аналогичный документ Банка России – «Положение о требованиях к правилам внутреннего контроля НФО в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 15 декабря 2014 г. № 445-П, основополагающие тезисы которого идентичны тезисам Положения для кредитных организаций.

Отсутствие четкой регламентации и единых подходов к оценке риска ОД/ФТ кредитными организациями и НФО, с *одной* стороны, создает дополнительные риски в их деятельности, с *другой* же стороны, дает наиболее ответственным участникам рынка организовывать свою деятельность с учетом собственных, повышенных требований, позволяющих сохранить репутацию и избежать возможных репрессивных мер со стороны контролирующих органов [12].

4. Результаты и перспективы развития системы ПОД/ФТ

Таким образом, система противодействия легализации («отмыванию») преступных доходов и финансированию терроризма с участием Российской Федерации имеет три уровня иерархии (рис. 2).

Рис. 2. Структура международной системы противодействия легализации преступных доходов и финансированию терроризма

Все это обусловливает необходимость:

- совершенствования законодательства, регулирующего российскую систему ПОД/ФТ, в том числе в части расширения набора критериев, свидетельствующих о повышенном риске клиента в части легализации («отмывания») доходов;
- изучения и применения лучшего международного опыта такой практик предупреждения в данной уровень области;
- постоянной актуализации и совершенствования системы ПОД/ФТ на первом уровне (на уровне организаций, в том числе кредитных организаций и НФО, являющихся агентами Федерального закона №115-ФЗ), а также осуществления непрерывного мониторинга операций клиентов в рамках действующей системы ПОД/ФТ;
- разработки и внедрению единых подходов к оценке риска легализации («отмывания») доходов и финансирования терроризма, в том числе

на основании сегментации по типу организации и ее бизнес-модели.

Российская Федерация стремится обеспечить полное соответствие международным рекомендациям по выполнению стандартов ПОД/ФТ. Однако международное сотрудничество в этой области осложняется разворачивающимся в последние четыре года внешнеполитическим кризисом, толчком к которому послужил украинский переворот. Тогда США и их сателлитами в отношении России были введены и непрерывно продолжают вводиться все новые санкции экономической направленности. Санкции препятствуют свободному перемещению российских граждан, в том числе бизнесменов, имеющих деловые связи за рубежом. Они предполагают ограничения в распространении технологий и поставок комплектующих в отношении многих предприятий перед которыми вследствие этого возникла *проблема импортозамещения*. В отношении банков и других организаций они запрещают доступ к получению финансовых ресурсов.

Россия вынуждена реагировать и принимать ответные меры к государствам, вводящим эти ограничения. Маховик кросс-санкций все более раскручивается, их количество все возрастает, они охватывают все новые сферы международного экономического взаимодействия. Эта кампания, по сути, лишена смысла, однако ее чрезвычайно трудно остановить. Сами политические группировки, вводящие санкции, признают невозможность получения с их помощью декларируемых конечных результатов. Однако она заметно осложняет международные связи в целом и согласованные действия по борьбе с ОД/ФТ, в частности.

Периодически возникающие затруднения при проведении расчетных операций с использованием платежных систем *Visa* и *Mastercard*, угроза отключения России от финансовой системы *SWIFT* (что уже ранее применялось в отношении других стран) очевидно, затрудняют выполнение требований и рекомендаций международных организаций в отношении ПОД/ФТ.

Имеющиеся *экспертные* оценки [7 – 9] позволяют отобразить графически степень мер противодействия ОД/ФТ в России с учетом совокупных усилий различных участников системы (рис. 3, по горизонтали отложены годы: 2001 – 2016; по вертикали – количественно и объем нелегальных операций). Степень влияния компонентов системы противодействия указана графиками в нижней полуплоскости, а потенциальный и фактический рост нелегальных операций – в верхней. Видно, что наибольшее влияние на обстановку оказывают организации *второго* (национального) уровня, хотя значение международных организаций для сдерживания ОД/ФТ также немаловажно. Затруднения, возникшие в организации сотрудничества, не только негативно влияют на меры противодействия, но и способны нарушить устойчивость системы [6].

Как видно (см. рис. 3), фактически рост ОД/ФТ существенно уступает потенциальному, но в полной мере ограничить его пока не удается. Это происходит потому, что «отмывочная» деятельность характеризуется постоянным усложнением противозаконных схем, ускорением проведения нелегальных операций, использованием транзитных счетов, что приводит к большим финансовым и репутационным потерям.

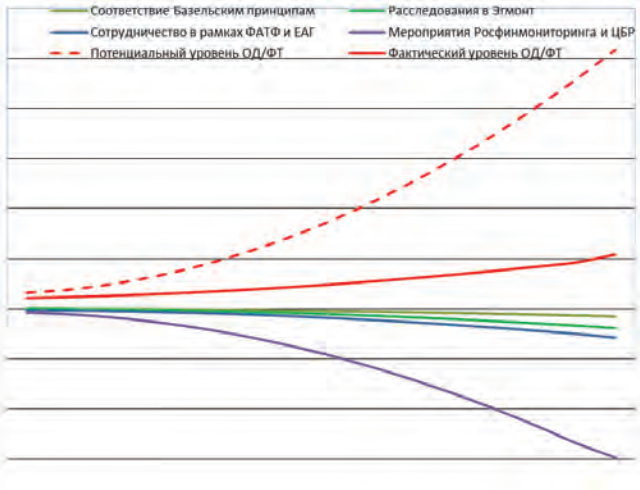

Рис. 3. Противодействие «отмывочной» деятельности в России

Масштабы этой угрозы для банковского сектора сопряжены с возрастающим числом лицензий на осуществление банковской деятельности, отозванных у кредитных организаций (за период 2006 – 2013 гг. за соучастие в противоправных операциях лишилось лицензий более 130 банков). Важным фактором, определяющим развитие ПОД/ФТ, является развитие информационных технологий, доступных обеим противодействующим сторонам, которые активно ими пользуются [3]. Вследствие этого *рекомендуется* наращивать информационное взаимодействие между уровнями системы ПОД/ФТ как по вертикали (стандарты – сверху, отчеты – снизу), так и по горизонтали (информационный обмен между заинтересованными участниками), тем более что противная сторона (группировки, характеризуемые условным термином «преступное сообщество») по сути своей сообщества не составляет, ее компоненты разобщены, законспирированы и не имеют возможности, да и желания обмениваться накапливаемым опытом «отмывочных» операций.

В результате совокупного воздействия организационных и технических факторов деятельность по «отмыванию» денежных средств превратилась в самостоятельный, сверхприбыльный и быстро растущий теневой сектор, и ущерб, наносимый ею экономике (в материальном плане) и обществу в целом (в плане моральном), очевидно, существеннее, чем наблюдаемая и фиксируемая его часть. «Отмывочные» схемы присутствуют во многих экономических преступлениях, а в условиях нарастающей глобальной информатизации бороться с этими преступлениями можно только согласованными действиями в рамках международных организаций. К тому же в России нелегальная деятельность по ОД/ФТ опирается на традиции взяточниче-

ства, сложившуюся практику откатов, устойчивый настрой бизнеса на бегство капитала, отработанные приемы использования офшорных юрисдикций с целью завуалировать источники происхождения доходов и обеспечить уход от налогов [15]. Важным фактором, сдерживающим меры противодействия, остается уровень развития *информационного пространства* в России, не вполне достаточный для выполнения подобных масштабных задач [1].

В связи с этим механизмы контроля в кредитных организациях нуждаются в постоянном развитии, чтобы оказываться способными анализировать возрастающие объемы поступающей финансовой информации, своевременно выявлять в общем её потоке сведения об операциях, связанных с «отмыванием» нелегальных доходов, гарантировать экономическую безопасность банков, обеспечивать рациональное использование финансовых ресурсов. Представленный график (см. рис. 3) приводит нас к однозначному *выводу*, что свертывание международного сотрудничества в этой области ПОД/ФТ – верный путь к поражению в борьбе с организованной финансовой преступностью. Напротив, дальнейшая структурная оптимизация и повышение степени взаимной информационной открытости партнеров на всех уровнях позволит добиться существенных успехов в ограничении ОД/ФТ.

Рецензент: ***Марков Алексей Сергеевич****, доктор технических наук, доцент, профессор МГТУ им. Баумана, Главный редактор журнала «Вопросы кибербезопасности», г. Москва, Россия.*

E-mail: *a.markov@npo-echelon.ru*

Литература

1. Бегларян М. Е., Пичкуренко Е. А. Проблемы формирования информационно-правового пространства России // Экономика. Право. Печать. Вестник КСЭИ. 2014. № 3-4 (63-64). С. 68–73.
2. Бектенова Г. С. Риск как основной фактор, определяющий цену на рынке проектного финансирования в современном банковском менеджменте // Труды XVI Междунар. науч.-практ. конф. «Новая модель экономического роста на основе структурной модернизации в России» (22–23 апреля 2015 г.) / РЭУ им. Г. В. Плеханова. М. : РЭУ, 2015. С. 288–291.
3. Беркетов Г. А., Микрюков А. А., Федосеев С. В. Направления развития информационных технологий в экономической сфере // Труды Междунар. симпозиума «Надежность и качество» (25 мая – 2 июня 2011 г.), т. 1 / ПГУ. Пенза : ПГУ, 2011. С. 113–114.
4. Бондаренко Т. Г. Основные трудности банковской системы при переходе на международные стандарты финансовой отчетности // Известия Тульского гос. ун-та «Экономические и юридические науки». 2012. № 3. С. 315–323.
5. Ващекин А. Н. Применение математических методов теории нечетких множеств при моделировании принятия решений в экономической и правовой сфере // Экономика. Статистика. Информатика. Вестник УМО. 2013. № 6. С. 18–21.
6. Ващекин А. Н., Хрусталёв М. М. Исследование устойчивости экономико-математической модели неантагонистической игры субъектов оптового рынка // Автоматика и телемеханика. 2005. № 10. С. 161–174.
7. Ващекина И. В., Ващекин А. Н. Применение риск-ориентированного подхода при организации противодействия отмыванию нелегальных доходов в российской практике // Наука и практика. 2018. № 3 (31). С. 61–69.
8. Ващекина И. В. Деятельность банков в рамках национальных моделей концепции социальной ответственности // Вестник РЭУ им. Г. В. Плеханова. 2015. № 5(83). С. 59–65.
9. Ващекина И. В. Международное сотрудничество в области противодействия легализации преступных доходов и финансового терроризма на фоне внешних негативных воздействий // Международная торговля и торговая политика. 2018. № 2(14). С. 113–126.
10. Ващекина И. В. Российские кредитные организации в международной системе противодействия легализации (отмыванию) доходов и финансированию терроризма // Вестник РЭУ им. Г.В. Плеханова. 2018. № 5(101). С. 26–36.
11. Катаргин Н. В. Оценка рисков при произвольном распределении вероятности дохода и риска // Вестник научно-технического развития. 2015. № 4 (92). С. 12–19.
12. Кондратенко И. А., Ващекина И. В. Противодействие легализации доходов, полученных преступным путем, в кредитных организациях Российской Федерации // Наука и практика. 2017. № 1(25). С. 109–113.
13. Ловцов Д. А. Проблема эффективности международно-правового обеспечения глобального информационного обмена // Наука и образование: хозяйство и экономика, предпринимательство, право и управление. 2011. № 11(17). С. 24–31.
14. Терентьева Л. В. Концепция суверенитета государства в условиях глобализационных и информационно-коммуникационных процессов // Право: Журнал Высшей школы экономики. 2017. № 1. С. 187–200.
15. Vashchekin A. N. The development of new organization forms of wholesale trade enterprises in Russia // Экономика, статистика и информатика. Вестник УМО. 2015. № 2. С. 29–33.

INFORMATION INTERACTION IN THE SYSTEM OF LEGAL ORGANIZATIONS FOR COMBATING CRIMINAL INCOME "WASHING": RISK-ORIENTED APPROACH

Andrey Vashchekin, *Pn. D. in Economic, Docent, Professor of the Chair of Information Law, Informatics and Mathematics of the Russian State University of Justice, Russian Federation, Moscow.*
Email: *vaschekin@mail.ru*

Irina Vashchekina, *Pn. D. in Economic, Docent, associate Professor of the Chair of Information Law, Informatics and Mathematics of the Russian State University of Justice, Russian Federation, Moscow.*
Email: *vaschekina@mail.ru*

Abstract.
Purpose: *a study of information interaction in the system of countering the laundering of criminal proceeds and the financing of terrorism (AML / CFT), whose task is to carry out financial monitoring in order to prevent the functioning of the "shadow" sector of the economy, the formation of organized crime and the implementation of terrorist activities in the global community.*
Methods: *analytical and expert methods of system analysis and mathematical modeling.*
Results: the main levels of the AML / CFT system functioning are defined, the first of which is formed by international associations, the second by national AML / CFT structures, the third by separate financial and commercial organizations interacting with the first two levels and within the powers controlled by them. The Russian national AML / CFT system relies on the interaction of Rosfinmonitoring, the Bank of Russia and other organizations, the list of which is determined by Russian law. They ensure compliance of the activities of Russian credit organizations with the FATF recommendations, the Wolfsberg principles, interaction with EAG and Egmont, measures to reduce the Basel AML index of Russia.
The necessity of international information interaction in the fight against the laundering of illegal income as one of the tasks of ensuring the competitiveness of the domestic economy, creating a positive investment climate that enhances the international authority of the country as a whole and strengthens its political position, is substantiated. The use of a risk-based approach as a methodological basis in the organization of financial monitoring based on the development of foreign AML / CFT practices was recommended. It is proposed to conduct a risk assessment based on upgraded probabilistic methods and the method of fuzzy sets.

Keywords: *laundering of illegal incomes, information interaction, financial monitoring international associations, Russian organizations, risks, countermeasures, foreign policy crisis.*

References

1. Beglarian M. E., Pichkurenko E. A. Problemy formirovaniia informatsionno-pravovogo prostranstva Rossii, Ekonomika. Pravo. Pechat'. Vestnik KSEI, 2014, No. 3-4 (63-64), pp. 68-73.
2. Bektenova G. S. Risk kak osnovnoi faktor, opredeliaiushchii tsenu na rynke proektnogo finansirovaniia v sovremennom bankovskom menedzhmente, Trudy XVI Mezhdunar. nauch.-prakt. konf. "Novaia model' ekonomicheskogo rosta na osnove strukturnoi modernizatsii v Rossii" (22-23 aprelia 2015 g.), REU im. G. V. Plekhanova, M. : REU, 2015, pp. 288-291.
3. Berketov G. A., Mikriukov A. A., Fedoseev S. V. Napravleniia razvitiia informatsionnykh tekhnologii v ekonomicheskoi sfere, Trudy Mezhdunar. simpoziuma "Nadezhnost' i kachestvo" (25 maia -- 2 iiunia 2011 g.), t. 1, PGU, Penza : PGU, 2011, pp. 113-114.
4. Bondarenko T. G. Osnovnye trudnosti bankovskoi sistemy pri perekhode na mezhdunarodnye standarty finansovoi otchetnosti, Izvestiia Tul'skogo gos. un-ta "Ekonomicheskie i iuridicheskie nauki", 2012, No. 3, pp. 315-323.
5. Vashchekin A. N. Primenenie matematicheskikh metodov teorii nechetkikh mnozhestv pri modelirovanii priniatiia reshenii v ekonomicheskoi i pravovoi sfere, Ekonomika. Statistika. Informatika. Vestnik UMO, 2013, No. 6, pp. 18-21.
6. Vashchekin A. N., Khrustalev M. M. Issledovanie ustoichivosti ekonomiko-matematicheskoi modeli neantagonisticheskoi igry sub"ektov optovogo rynka, Avtomatika i telemekhanika, 2005, No. 10, pp. 161-174.
7. Vashchekina I. V., Vashchekin A. N. Primenenie risk-orientirovannogo podkhoda pri organizatsii protivodeistviia otmyvaniiu nelegal'nykh dokhodov v rossiiskoi praktike, Nauka i praktika, 2018, No. 3 (31), pp. 61-69.

8. Vashchekina I. V. Deiatel'nost' bankov v ramkakh natsional'nykh modelei kontseptsii sotsial'noi otvetstvennosti, Vestnik REU im. G. V. Plekhanova, 2015, No. 5(83), pp. 59-65.
9. Vashchekina I. V. Mezhdunarodnoe sotrudnichestvo v oblasti protivodeistviia legalizatsii prestupnykh dokhodov i finansovogo terrorizma na fone vneshnikh negativnykh vozdeistvii, Mezhdunarodnaia torgovlia i torgovaia politika, 2018, No. 2(14), pp. 113-126.
10. Vashchekina I. V. Rossiiskie kreditnye organizatsii v mezhdunarodnoi sisteme protivodeistviia legalizatsii (otmyvaniiu) dokhodov i finansirovaniiu terrorizma, Vestnik REU im. G.V. Plekhanova, 2018, No. 5(101), pp. 26-36.
11. Katargin N. V. Otsenka riskov pri proizvol'nom raspredelenii veroiatnosti dokhoda i riska, Vestnik nauchno-tekhnicheskogo razvitiia, 2015, No. 4 (92), pp. 12-19.
12. Kondratenko I. A., Vashchekina I. V. Protivodeistvie legalizatsii dokhodov, poluchennykh prestupnym putem, v kreditnykh organizatsiiakh Rossiiskoi Federatsii, Nauka i praktika, 2017, No. 1(25), pp. 109-113.
13. Lovtsov D. A. Problema effektivnosti mezhdunarodno-pravovogo obespecheniia global'nogo informatsionnogo obmena, Nauka i obrazovanie: khoziaistvo i ekonomika, predprinimatel'stvo, pravo i upravlenie, 2011, No. 11(17), pp. 24-31.
14. Terent'eva L. V. Kontseptsiia suvereniteta gosudarstva v usloviiakh globalizatsionnykh i informatsionno-kommunikatsionnykh protsessov, Pravo: Zhurnal Vysshei shkoly ekonomiki, 2017, No. 1, pp. 187-200.
15. Vashchekin A. N. The development of new organization forms of wholesale trade enterprises in Russia, Ekonomika, statistika i informatika. Vestnik UMO, 2015, No. 2, pp. 29-33.

ИНФОРМАЦИОННО-МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБОРОТА РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

*Ловцов Д. А., Богданова М. В., Лобан А. В. **

Ключевые слова: *результаты интеллектуальной деятельности (РИД), система управления оборотом РИД, система поддержки принятия решений, концептуально-логическая модель, факторы, формально-логическая структура, экономико-правовые механизмы, рентабельность, данные, фактор-множество, локальная информационная система, тезаурус.*

Аннотация.

Цель работы: формирование продуктивной теоретической базы создания и разработки эффективной национальной системы правового регулирования оборотом результатов интеллектуальной деятельности.

Метод: системный анализ существенных факторов предметной области правового регулирования оборотом результатов интеллектуальной деятельности (РИД), концептуально-логическое и математическое моделирование крупномасштабных информационно-аналитических систем.

Результаты: обоснована концептуально-логическая модель системы управления оборотом результатов интеллектуальной деятельности предприятий промышленности, определяющая основные организационно-функциональные компоненты и типы структурных связей (информационные, организационные, финансовые, фискальные) и позволяющая рационально планировать применение эффективных экономико-правовых механизмов; формализованы задачи оптимизации системы в целом и её основной функциональной подсистемы поддержки принятия управленческих организационно-правовых решений по регулированию оборота РИД; обоснована обобщенная формально-логическая структура процессов контроля оборота РИД, соответствующая требованиям ООН по стандартизации данных для международной торговли.

Предложено дополнить действующие национальные стандарты «национальным набором данных» о зарегистрированных РИД в упрощённом и стандартизированном форматах, рекомендуемых ООН.

DOI:10.21681/1994-1404-2018-4-15-23

В настоящее время в России большое внимание уделяется созданию экономически эффективной крупномасштабной системы правового регулирования оборотом результатов интеллектуальной деятельности (РИД) [6], одной из основных функциональных подсистем которой является распределённая информационно-аналитическая *система поддержки принятия организационно-правовых решений* (СППР) по регулированию оборота РИД. Данная система должна обеспечить эффективный многоагентный поиск и логическую обработку информации о состоянии «жизненного цикла» всех зарегистрированных РИД, в частности, на пространстве ЕврАзЭС [10] и в мире.

Разработанная [6, 7] обобщённая *концептуально-логическая модель* системы управления оборотом РИД предприятий промышленности, включая предприятия оборонно-промышленного комплекса (ОПК), содержит, в частности, следующие основные организационно-функциональные компоненты (рис. 1):

- создателей (авторов РИД), включая предприятия промышленности, авторские коллективы и отдельных авторов;
- источники финансирования создания РИД (собственников РИД);
- научно-технологический рынок;
- процесс оборота РИД.

В качестве основные типов структурных связей в модели представляется целесообразным рассматривать следующие:

* ***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, Россия.*

E-mail: dal-1206@mail.ru

Богданова Марина Валерьевна*, доктор экономических наук, доцент, отличник статистики Российской Федерации, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Россия.*

E-mail: bogdanovamv2009@yandex.ru

Лобан Анатолий Владимирович*, кандидат технических наук, старший научный сотрудник, доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Россия.*

E-mail: aloban@mail.ru

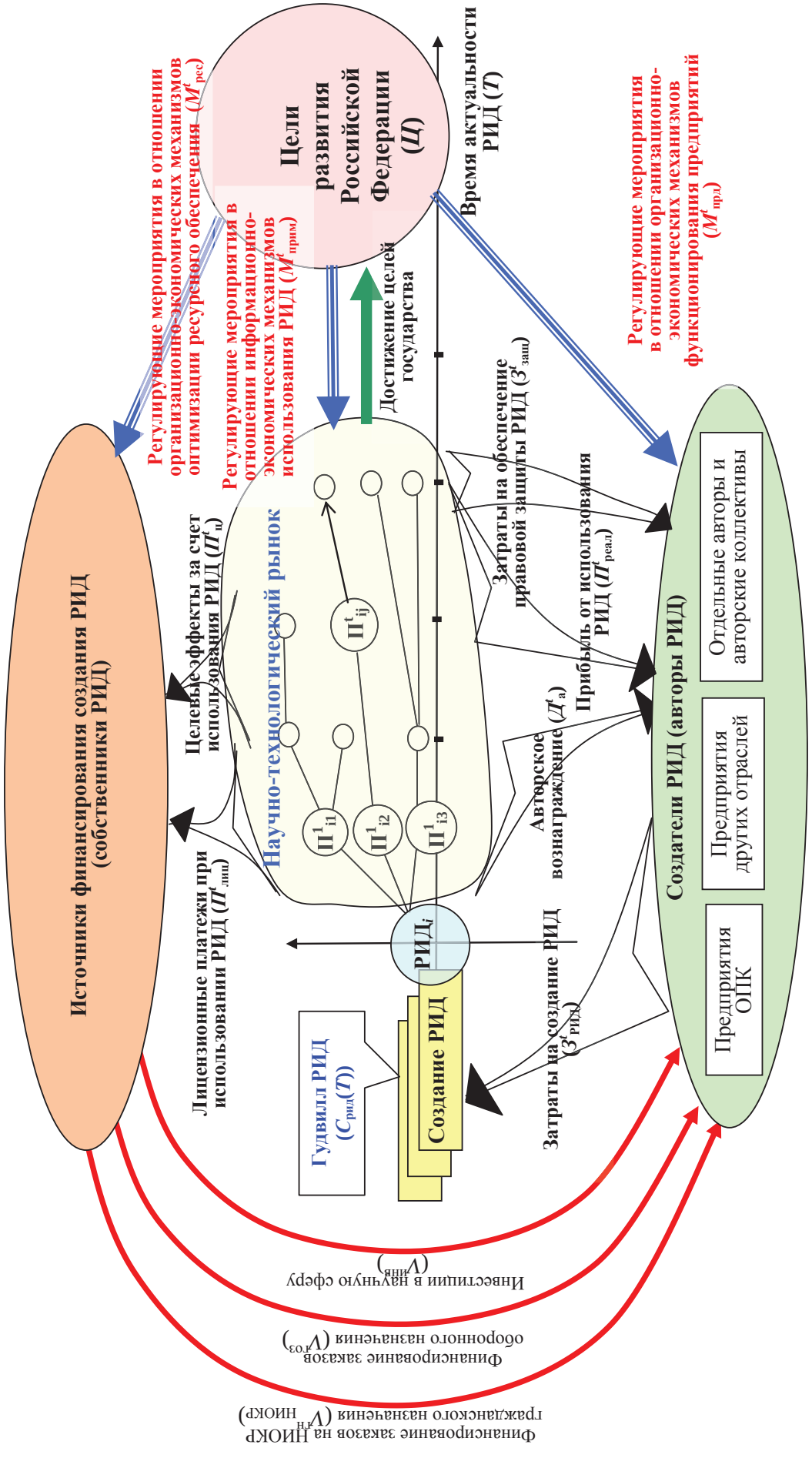

Рис. 1. Структура концептуально-логической модели системы управления оборотом результатов интеллектуальной деятельности предприятий промышленности

- *информационные*: цели развития Российской Федерации (***Ц***), целевые эффекты ($\boldsymbol{П}^t_{ц}$)за счёт использования РИД;
- *организационного управления*: совокупность целевых планов управленческих мероприятий по регулированию оборотом РИД в отношении экономико-правовых механизмов оптимизации ресурсного обеспечения ($\boldsymbol{М}^t_{рес}$), информационно-экономических механизмов использования РИД ($\boldsymbol{М}^t_{прим}$), экономико-правовых механизмов функционирования предприятий ($\boldsymbol{М}^t_{прд}$);
- *финансовые инвестиции*: финансирование заказов на НИОКР общегражданского назначения ($\boldsymbol{V}^{тн}_{НИОКР}$), финансирование госзаказов оборонного назначения ($\boldsymbol{V}^{гоз}$), инвестиции в научную сферу ($\boldsymbol{V}^{инв}$);
- *фискальные (денежные) операции*: авторское вознаграждение ($\boldsymbol{Д}^t_{а}$), лицензионные платежи при использовании РИД ($\boldsymbol{П}^t_{лиц}$), затраты на обеспечение правовой защиты РИД ($\boldsymbol{З}^t_{защ}$) [8, 11], затраты на создание РИД ($\boldsymbol{З}^t_{РИД}$), прибыль от использования РИД ($\boldsymbol{П}^t_{реал}$).

Концептуально-логическое моделирование системы управления оборотом РИД реализовано на основе системного анализа и учёта следующих основных факторов соответствующей предметной области оборота РИД [7]:

- Появление РИД, как правило, является одним из творческих результатов решения актуальных прикладных проблем, поэтому основная цель управления оборотом РИД должна определяться как создание условий для эффективного решения этих прикладных проблем.
- Значительная часть РИД имеет универсальный характер, т.е. их можно использовать для решения нескольких прикладных проблем. Следовательно, управление оборотом РИД будет экономически эффективным тогда, когда соответствующие прикладные проблемы будут решены с меньшими затратами различного рода ресурсов.
- Поскольку решение тех или иных прикладных проблем осуществляется в рамках мероприятий, определённых соответствующими целевыми программами и планами, то имеется возможность построить дерево целей, для достижения которых был создан соответствующий РИД.
- Создание РИД связано с затратами определённых финансовых ресурсов, поэтому их использование для решения прикладных проблем должно быть экономически эффективным, т.е. должно принести эффект, формализуемый соответствующими экономическими показателями.
- Поскольку РИД имеют информационную природу, управление их информационным обликом должно лежать в основе функционирования системы управления оборотом РИД.
- С учётом того, что процесс создания и использования РИД имеет протяжённость во времени, функционирование системы управления оборотом РИД должно охватывать все стадии этого процесса.
- Эффективность интеллектуальной деятельности определяется эффективностью деятельности государства в различных сферах, что предопределяет необходимость координации функционирования системы управления оборотом РИД с политикой Российской Федерации в политической, экономической, информационной, инновационной, социальной и других сферах.
- Ценность РИД существенно изменяется в зависимости от способа и времени начала использования, следовательно, при управлении оборотом РИД необходимо учитывать срок его актуальности и потенциальные направления реализации.
- Одни и те же РИД могут стать основой для создания разнообразных видов товарной продукции, реализация которых на рынке принесет экономические эффекты, что обусловливает необходимость их мультипликативного учёта.
- Источником появления РИД является творческая деятельность людей, как правило, работающих на предприятиях и организациях, что обусловливает возможность повышения эффективности управления оборотом РИД за счёт использования экономико-правовых механизмов, усиливающих мотивации участников творческого процесса.

Рассматриваемая концептуально-логическая модель (см. рис. 1) системы управления оборотом РИД предприятий промышленности свидетельствует о том, что для обеспечения экономической эффективности управления оборотом РИД применение экономико-правовых механизмов должно базироваться на *общеотраслевых принципах* (при необходимости модифицированных), дополненных *специфическими* принципами, т.е. учитывающими специфику предметной области [7]. При этом, поскольку на практике финансирование мероприятий, выполняемых для решения тех или иных прикладных проблем, осуществляет субъект, относительно которого эти проблемы решаются, то право собственности на РИД определяется этим субъектом. Это позволяет классифицировать все создаваемые в Российской Федерации РИД на две основные категории:

- созданные с использованием государственных средств (федерального и регионального уровней) и относительно которых Российская Федерация имеет долю прав собственности;
- созданные за счёт частных инвесторов, права распоряжения которыми государству не принадлежат.

Такое деление позволяет разграничить экономико-правовые механизмы (включая инвестиционно-инновационную деятельность; коммерциализацию РИД в процессе трансферта технологий; управление рисками при создании, распространении и внедрении РИД и др.), обеспечивающие эффективное управление оборо-

том РИД. Если в отношении РИД, созданных с использованием государственных средств, права собственности на которые полностью или частично принадлежат Российской Федерации, государство может использовать весь арсенал экономико-правовых механизмов для эффективного управления ими, то эффективное использование РИД, находящихся в собственности частных лиц (физических и юридических), государство может только стимулировать.

Повышение экономической эффективности системы управления оборотом РИД предприятий промышленности можно обеспечить на основе реализации стратегии $S^*_{РИД}$, содержащей рациональную, с точки зрения учёта интересов всех субъектов этого процесса, взаимосвязанную совокупность управленческих решений – планов управленческих мероприятий:

$$S^*_{РИД} = < M^*_{рес}, M^*_{прод}, M^*_{прим}, t >,$$

где: $M^*_{рес}$, $M^*_{прод}$, $M^*_{прим}$ – множество управленческих решений, реализуемых в отношении экономико-правовых механизмов оптимизации ресурсного обеспечения; в отношении экономико-правовых механизмов функционирования предприятий; в отношении информационно-экономических механизмов использования РИД, соответственно; *t* – интервал времени оборота РИД.

В качестве критерия экономической эффективности стратегии представляется целесообразным использовать максимум *рентабельности оборота* РИД:

$$R^{(t)}_{РИД}(S^*_{РИД}) \Rightarrow \max_{\{S\}},$$

где $\{S\}$ – множество допустимых управленческих решений (наборов планов управленческих мероприятий).

При этом одно из возможных формализованных выражений для рентабельности оборота РИД можно представить как отношение прибыли от реализации *i*-го РИД в *j*-м виде продукции в году *t* к затратам на его реализацию:

$$\sum_i \sum_j \sum_t (П^{лиц}_{i,j,t} + П^{ц}_{i,j,t}) > \sum_t (V^{ГН}_{НИОКР,t} + V^{ГОЗ}_t + V^{инв}_t),$$

где: $П^{лиц}_{i,j,t}$ – прибыль от реализации *i*-го РИД в *j*-м виде продукции в году *t*; $П^{ц}_{i,j}$ – затраты на реализацию *i*-го РИД в *j*-м виде продукции в году *t*.

В этом случае оптимизация системы управления оборотом РИД возможна при соблюдении следующих необходимых и достаточных условий:

1. Для хозяйствующих субъектов, финансирующих создание РИД, а также выступающих в качестве их собственников, должно выполняться следующее неравенство:

$$\sum_i \sum_j \sum_t (П^{лиц}_{i,j,t} + П^{ц}_{i,j,t}) > \sum_t (V^{ГН}_{НИОКР,t} + V^{ГОЗ}_t + V^{инв}_t), \quad (1)$$

где: $П^{лиц}_{i,j,t}$ – лицензионные платежи, в том числе в виде роялти и паушальных платежей, полученные за реализацию *i*-го РИД в *j*-м виде продукции в году *t*; $П^{ц}_{i,j,t}$ – стоимостная оценка целевых эффектов, полученных при реализации *i*-го РИД в *j*-м виде продукции в году *t*; $V^{ГН}_{НИОКР,t}$ – объёмы финансирования заказов на НИОКР гражданского назначения в году *t*; $V^{ГОЗ}_t$ – объёмы финансирования государственного заказа в соответствующем году *t*; $V^{инв}_t$ — объёмы инвестирования научной сферы в году *t*.

2. Для авторов РИД, являющихся их создателями, должно выполняться следующее неравенство:

$$\sum_i \sum_j \sum_t (Д_{i,j,t} + П_{i,j,t} - З^{защ}_{i,j,t}) > 0, \quad (2)$$

где: $Д_{i,j,t}$ – размер авторского вознаграждения, полученного в году *t*; $Д_{i,j,t}$ – прибыль от реализации *i*-го РИД в *j*-м виде продукции в году *t*; $П_{ijt}$ – затраты на обеспечение правовой защиты РИД в году *t*.

Физический смысл рассмотренных выражений сводится к следующему:

1. Ограничение (1) на формирование рациональной стратегии управления оборотом РИД предприятий промышленности с точки зрения хозяйствующих субъектов, финансирующих создание РИД и, как правило, выступающих в качестве их собственников, обусловлено необходимостью возврата средств, затраченных ими на решение соответствующих творческих и обеспечивающих задач. При этом для централизованных источников определяющей должна быть оценка целевых эффектов, полученных при реализации *i*-го РИД в *j*-м виде продукции в году *t*, для децентрализованных – размер соответствующих лицензионных платежей.

2. Необходимость экономической мотивации создателей РИД формализована соотношением (2), физический смысл которого заключается в том, что авторы должны стремиться к увеличению своих доходов, получаемых от созданной ими интеллектуальной продукции.

Определение и текущая коррекция стратегии $S^*_{РИД}$ в условиях возникающих в реальной обстановке ситуаций осуществляются в подсистеме поддержки принятия организационно-правовых решений (СППР) по регулированию оборота РИД. Создание эффективной СППР представляется целесообразным с учётом современных международных стандартов, в частности, с учётом Рекомендации № 34 СЕФАКТ ООН по упрощению и стандартизации данных для международной торговли[1], согласно которой товар должен пройти этапы сбора, определения, анализа и согласования данных. Полученный в результате этих этапов «набор данных» о товаре может стать основой для регулирования правоотношений автора РИД и пользователей на базе существующего законодательства.

[1] Рекомендация № 34 СЕФАКТ ООН (UN/CEFACT) – Упрощение и стандартизация данных для международной торговли. – http://www.unece.org/fileadmin/DAM/ cefact/recommendations/ rec34/ECE_TRADE_400_DataSimplificationand_Rec34R.pdf

В самом общем виде модель любого РИД может быть представлена упорядоченным множеством

$\Delta =< T, X, Y, Z, F, L >$ [2],

где *T* – множество моментов времени, в которые наблюдается РИД; *X, Y* – множество входных воздействий и выходных проявлений РИД, соответственно; *Z* – множество состояний «жизненного цикла» РИД; *F* – оператор переходов, отражающих механизм изменения состояния РИД под действием внутренних и внешних воздействий; *L* – оператор выходов, описывающий механизм формирования выходных проявлений как реакции РИД на внутренние и внешние воздействия. Операторы *F* и *L* реализуют отображения

$F : T \times X \times Z \to Z$;

$L : T \times X \times Z \to Y$.

С математической точки зрения определение любого из состояний РИД возможно только в том случае, если по выходным проявлениям $y_j (j = 1, n)$ при известных значениях входных воздействий $x_s (s = 1, l)$ удаётся зафиксировать оценки переменных состояния $z_r (r = 1, k)$. Такая задача характерна для ступени *сбора данных*[2] и в теории систем и управления известна как задача наблюдения.

Формально эта задача сводится к решению относительно $y(t)$ следующего уравнения:

$$L\{t, x(t), \hat{z}(t), r\} = \hat{y}(t),$$

где $\hat{y}(t)$ – некоторая реализация (точнее, часть реализации) выходного процесса-проявления, доступная регистрации с помощью тех или иных фиксирующих средств.

При полной наблюдаемости РИД всегда возможно определение его состояния по данным фиксации выходных проявлений. Задача отнесения наблюдаемого состояния РИД к одному из заданных видов решается на ступени *определения данных*[3] и относится к классу задач классификации. Решение этой задачи состоит в отыскании отображения классифицирования:

$$L\{t, x(t), \hat{z}(t), r\} = \hat{y}(t),$$

где *E* – множество заданных видов состояния РИД.

Каждому виду состояния РИД соответствует определённое подмножество его текущих состояний, объединённых некоторыми общими свойствами, т.е. таких состояний, о которых можно принять одно и то же решение. Нетрудно установить, что отдельные состояния, входящие в это подмножество, должны находиться в отношении *эквивалентности*. Отношением эквивалентности называется бинарное отношение $Q = Y \times Y$, обладающее свойствами рефлективности, симметричности и транзитивности [4].

Отношение эквивалентности задает разбиение множества *Y* возможных состояний РИД на непересекающиеся классы, т.е. осуществляет факторизацию этого множества. Обозначим получающееся при этом фактор-множество как Y / Q. С учётом данного обозначения операцию можно представить в виде отображения факторизации:

$\vartheta : Y \to Y / Q$,

которое по своему смыслу является наложением.

Разумно по существу рассматриваемой задачи потребовать, чтобы множество *E* видов состояний РИД и фактор-множество Y / Q находились во взаимно однозначном соответствии, т.е. чтобы отображение импликации $\chi : E \to Y / Q$ было взаимно однозначным.

Согласно известной теореме о гомоморфизме [1] для множеств, взаимная однозначность отображения достигается тогда, когда выполняется условие $\eta\chi = \vartheta$, а это возможно когда любой элемент $e_i \in E$ является «образом», по крайней мере, одного элемента $y \in Y$.

Физически это означает следующее: всякому наблюдаемому состоянию РИД должен быть поставлен в соответствие единственный вид его состояния, зафиксированный по выходным проявлениям РИД.

Способы разбиения множества *Y* на классы эквивалентности определяются соответствующими моделями РИД, вербальное описание которых содержит множество *D* авторских документов. Поэтому на практике *сбор* и *определение данных* о РИД является результатом отображения факторизации $\vartheta_{верб}$, имеющего вербальный, сопоставительный с документацией характер. При этом фактор-множество Y / Q можно рассматривать как результат, полученный с помощью тезауруса-классификатора, содержащего формализованный образ РИД как *информационной системы с тезаурусом* [2 – 5]:

$T_\phi =< D, \Pi, \varphi >$,

где Π – множество проверок, реализуемых для определения состояния РИД; $\varphi : \Pi \to 2^D$ – отображение сопоставления, ставящее в соответствие каждой проверке $\pi \in \Pi$ ответ из множества *D*.

Данные о РИД можно собрать в виде электронных таблиц баз данных. Как показано в Рекомендации № 34 СЕФАКТ ООН целесообразно от множества документов *D* перейти к *национальному набору данных* (ННД) о зарегистрированных РИД в упрощённом и стандартизированном форматах. После практического построения тезауруса-классификатора T_ϕ возникает возможность непосредственной реализации отображения классифицирования $\eta : Y \to E$, т.е. выработки решения о принадлежности РИД к одному из видов (классов).

Далее можно приступить к ступени *анализа* состояния РИД, заключающегося в реализации отображения оценивания $\psi : E \to S$, которое формально определенному виду состояния РИД $e \in E$ ставит в соответствие вполне конкретное решение об его истинном состоянии $s \in S$ с учётом вероятностных характеристик возможных ошибок при контроле, погрешностей выполняемых наблюдений проявлений РИД. Процесс

[2] Там же.

[3] Там же.

анализа данных заключается в выявлении схожих элементов для обеспечения полного понимания результата классифицирования.

На заключительной ступени *согласования* данных по результатам контроля производится уточнение сформированного фактор-множества Y/Q с помощью отображения идентификации:

$$\xi : S \to Y/Q.$$

Суть *задачи* заключается в консолидации перечня определённых и проанализированных данных в форме ННД с использованием процесса согласования. При согласовании учитываются стандарты[4], правила обмена данными, требования авторов РИД (в том числе по защите авторских прав [8, 11]) и др. На практике отображение идентификации реализуется через документы, т.е. $\xi_{верб}$ имеет вербальный, сопоставительный с документацией характер (рис. 2).

Такой подход позволяет использовать различные варианты архитектуры и моделирования данных, а также устранить риск ошибок, которые необходимо будет впоследствии выявить и устранить, особенно, если в ходе моделирования данных ставится задача обеспечить их оптимальное повторное использование в двусторонних и многосторонних проектах или операциях трансграничного обмена данными.

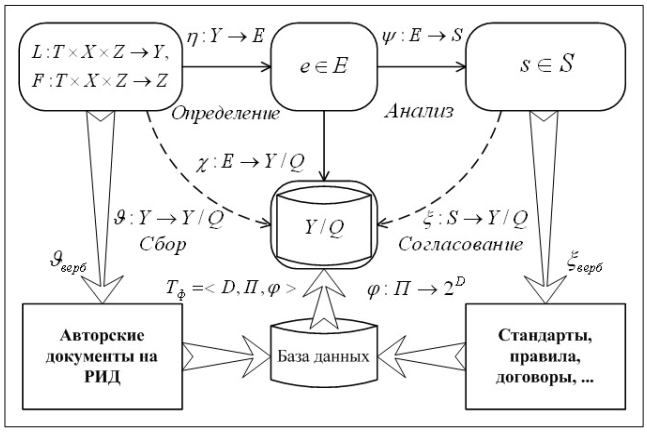

Рис. 2. Обобщенная формально-логическая структура процессов контроля оборота РИД

Приведенная формализация полностью согласуется с рекомендациями СЕФАКТ ООН и может быть положена в основу регулирования правоотношений авторов и пользователей РИД с целью более эффективного использования ресурсов для борьбы с незаконной торговлей и защиты авторских прав. ННД о совокупности существующих РИД облегчат соблюдение трейдерами[5] нормативных правовых требований за счёт сокращения времени, усилий и денежных затрат, необходимых для сбора, обобщения и представления данных в целях выполнения официальных формальностей.

Кроме того, созданный тезаурус-классификатор $T_\phi =< D, \Pi, \varphi >$ позволит выявлять случаи избыточности и дублирования данных. Вследствие этого процесс стандартизации приведет к сокращению общих потребностей в данных, а также к обеспечению таких свойств как *стабильность, непротиворечивость и предсказуемость* данных.

Страны ЕврАзЭС могут принять решение об объединении своих ННД в двусторонние или многосторонние наборы для использования в целях обмена данными в рамках торговых соглашений в соответствии с рекомендациями СЕФАКТ ООН.

Для создания систем, обеспечивающих эффективный поиск и логическую целенаправленную обработку информации о РИД на пространстве ЕврАзЭС, можно математически сформулировать и решить задачу синтеза структуры СППР поддержки принятия правовых решений в следующем обобщённом виде.

Пусть $S_1,\ldots,S_n$ – локальные информационные системы с тезаурусом, где $S_j = (T_j, D_j, \Pi_j, \varphi_j), j = \overline{1,n}$.

Соединим системы $S_1,\ldots,S_n$ в одну систему $S = (T, D, \Pi, \varphi)$ – СППР, базирующуюся на глобальном тезаурусе $T = \cup_j T_j$ [2, 3, 9]. Очевидно, что локальные информационные системы являются подсистемами СППР.

Ввиду того, что множество *D* документов СППР является объединением множеств $D = \cup D_j, j = \overline{1,n}$ документов локальных информационных систем, можно выразить ответ на вопрос к СППР как результат некоторых операций над ответами от локальных систем.

В СППР глобальный ответ на вопрос будет объединением локальных ответов, она выступает в роли центра сбора и обработки информации, т.е. обработки ответов на запросы управляющих органов.

Объём передаваемой информации на запрос из *j*-й локальной информационной системы равен оператору преобразования информации $G(\varphi_j(\bar{\pi})$ к виду, предназначенному для передачи по каналам связи.

Сформулируем *задачу распределения* РИД по локальным информационным подсистемам при множестве $\Pi = \{\pi_1, \pi_2, \ldots, \pi_r\}$ допустимых запросов в СППР, на которые ответы формируются последовательно без повторения запросов. Для удобства положим, что каждый запрос описывается одним дескриптором.

Требуется найти

$$\min \sum_j \sum_l c_{jl} x_{jl} + \sum_i \sum_j \sum_l b_{jl} G(\varphi_j^l(\bar{\pi}_i)) x_{jl}$$

при ограничениях

$$\sum_j x_{jl} = 1, \forall l \in L;$$

$$\sum_l x_{jl} \geq (\leq) N_j, \forall j \in \{1,2,\ldots,n\}.$$

где c_{jl} – обобщенная стоимость сбора информации об *l*-том РИД *j*-й локальной информационной системой;

[4] ГОСТ Р 56823-2015. Интеллектуальная собственность. Служебные результаты интеллектуальной деятельности (утв. Приказом Федеральным агентством по техническому регулированию и метрологии от 3 декабря 2015 г. № 2102-ст.) и др.

[5] От англ. trade – торговать, участвовать в торговле на финансовых рынках.

b_{jl} – обобщенная стоимость передачи единицы информации об *l*-том РИД в центр из *j*-й информационной локальной системы; x_{jl} – булева переменная, равна 1, если *l*-й РИД обслуживается *j*-й локальной информационной системой, и равна 0 в противном случае.

Первое ограничение требует обслуживания каждого РИД только одной информационной системой. *Второе* условие ограничивает количество РИД, подлежащих обслуживанию локальными подсистемами либо, напротив, требует, чтобы их было не меньше заданного числа.

Таким образом, рассмотрены результаты формализации и решения сложной актуальной задачи разработки информационно-математического обеспечения правового регулирования оборота результатов интеллектуальной деятельности как комплекса взаимосвязанных задач синтеза эффективной крупномасштабной системы правового регулирования оборота РИД и рациональной распределённой функциональной подсистемы поддержки принятия организационно-правовых решений по регулированию оборота РИД.

Литература

1. Винберг Э. Б. Курс алгебры. М. : Факториал Пресс, 2002. 544 с.
2. Дмитриев А. К., Мальцев П. А. Основы теории построения и контроля сложных систем. Л. : Энергоатомиздат, 1988. 192 с.
3. Лескин А. А., Мальцев П. А. Распределенные информационные системы на тезаурусе: препринт № 69. Л. : ЛИИАН, 1988.
4. Ловцов Д. А. Информационная теория эргасистем: Тезаурус. М. : Наука, 2005. 248 с.
5. Ловцов Д. А. Теория информационного права: базисные аспекты // Государство и право. 2011. № 11. С. 43–51.
6. Ловцов Д. А., Богданова М. В. Экономико-правовое регулирование оборота результатов интеллектуальной деятельности предприятий промышленности России // Экономика, статистика и информатика. Вестник УМО. 2013. № 1. С. 53–56.
7. Ловцов Д. А., Богданова М. В. Система управления оборотом результатов интеллектуальной деятельности оборонных предприятий // Труды XXXI Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (28–29 июня 2012 г.) в 5-и т. Т. 2 / РАО – Серпухов : Серп. воен. ин-т, 2012. С. 107–115.
8. 8. Ловцов Д. А., Галахова А. Е. Защита интеллектуальной собственности в сети Интернет // Информационное право. 2011. № 4. С. 13–20.
9. Ловцов Д. А., Лобан А. В. Синтез системы информационного обеспечения правового регулирования оборота результатов интеллектуальной деятельности // Труды IV Всеросс. науч.-практ. конф. «Современное непрерывное образование и инновационное развитие» (23 апреля 2014 г.) / ФГАУ «ФИРО». Серпухов : МОУ «ИИФ», 2014. С. 742–746.
10. Ловцов Д. А., Лобан А. В., Цимбал В. А. Система информационного обеспечения технического регулирования Таможенного Союза // Известия Института инженерной физики. 2013. № 1. С. 56–64.
11. Lovtsov D. A. Effective methods of protection of the intellectual activity results in infosphere of global telematics networks // Открытое образование. 2016. № 5. С. 85–88.

Рецензент: ***Запольский Сергей Васильевич,*** *доктор юридических наук, профессор, заслуженный юрист Российской Федерации, заведующий сектором административного и бюджетного права Института государства и права Российской академии наук, г. Москва, Россия.*

E-mail: *zpmoscow@mail.ru*

Литература

1. Королёв В. Т., Ловцов Д. А., Радионов В. В., Квачко В. Ю. Информатика и математика для юристов / Под ред. Д. А. Ловцова. – М.: Высшая школа, 2008. – 308 с.
2. Ловцов Д. А., Богданова М. В., Паршинцева Л. С. Правовая статистика преступности в современных условиях // Правовая информатика. – 2017. – № 4. – С. 40 – 48.
3. Ловцов Д. А., Верхоглядов А. А. Информационная безопасность судебных автоматизированных информационных систем: правовое регулирование и юрисдикция // Российское правосудие. – 2008. – № 8. – С. 55 – 64.
4. Ловцов Д. А., Ниесов В. А. Обеспечение единства судебной системы России в инфосфере: концептуальные аспекты // Российское правосудие. – 2006. – № 4. – С. 35 – 40.
5. Ловцов Д. А., Ниесов В. А. Правовая информатика в сфере электронного судопроизводства // Правовая информатика. – 2017. – № 3. – С. 23 – 34.
6. Ловцов Д. А., Ниесов В. А. Модернизация информационной инфраструктуры судопроизводства – ключевое направление оптимизации нагрузки на судебную систему // Российское правосудие. – 2014. – № 9. – С. 30 – 40.
7. Ловцов Д. А., Ниесов В. А. Развитие судебной системы России и создание единого информационного пространства – двуединая задача. // Российское правосудие. Спец. вып. 2012. С. 77 – 88.
8. Ловцов Д. А., Ниесов В. А. Актуальные проблемы создания и развития единого информационного

пространства судебной системы России // Информационное право. 2013. № 5. С. 13 – 18.
9. Ловцов Д. А., Ниесов В. А. Системные вопросы развития организационно-правового обеспечения электронного судопроизводства // Российское правосудие. – 2016. – № 51. – С. 64 – 78.
10. Ловцов Д. А. Проблемы правового регулирования электронного документооборота // Информационное право. – 2005. – № 2. – С. 28 – 31.
11. Ловцов Д. А., Шибаев Д. В. Семейство унифицированных правовых протоколов электронного документооборота в судебной системе // Российское правосудие. – 2011. – № 7. – С. 44 – 52.

INFORMATIVELY-MATHEMATICAL PROVIDING OF LEGAL REGULATION OF THE TURNOVER OF RESULTS OF INTELLECTUAL ACTIVITY

Dmitriy Lovtsov, *Dr. Sc. in Technology, Professor, Honored scientist of the RF, Deputy Director for research of Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Science; Head of the Chair of Information Law, Informatics and Mathematics of the Russian State University of Justice, Russian Federation, Moscow.*
E-mail: *dal-1206@mail.ru*

Marina Bogdanova, *Dr. Sc. in Economy, Associate Professor, Honored Statistic of the Russian Federation, Professor of the Chair of Information Law, Informatics and Mathematics of the Russian State University of Justice, Russian Federation, Moscow*
E-mail: *bogdanovamv2009@yandex.ru*

Anatoliy Loban, *PhD in Technology, Senior scientific specialist, Docent of the Chair of Information Law, Informatics and Mathematics of the Russian State University of Justice, Russian Federation, Moscow*
E-mail: *aloban@mail.ru*

Keywords: *results of intellectual activity (RIA), system for managing the turnover of RIA, the decision support system, informatively-mathematical providing, conceptual and logical model, factors, formal and logic structure, economic and legal mechanisms, profitability, data, factor-set, limited information system, thesaurus.*

Abstract.

Purpose of the article: formation of a productive theoretical basis for the creation and development of effective national system of legal regulation of the turnover of results of intellectual activity.

Method used: system analysis of significant factors in the subject area of legal regulation of the turnover of results of intellectual activity, conceptual and logical and mathematic modeling of large-scale information and analytical systems.

Results: the conceptual and logical model of system for managing the turnover of results of intellectual activity of industrial enterprises is substantiated, which determines the basic organized and functional components and types of structural links (informational, organizational, financial, fiscal) and makes it possible to rational planning the using of effectiveness economic and legal mechanisms; optimization tasks of system in hole and its basic functional subsystem of administrative organizational-legal decision support for regulating of the turnover of intellectual activity results are formalized; the generalized formal and logical structure of the processes controlling the turnover of results of intellectual activity, consistent with the requirements of the United Nations for the standardization of data for international trade is justified.

It is proposed to supplement the existing national standards with the "national data set" on registered results of intellectual activity in standardized and simplified formats recommended by the UN.

References

1. Vinberg E. B. Kurs algebry, M. : Faktorial Press, 2002, 544 pp.
2. Dmitriev A. K., Mal'tsev P. A. Osnovy teorii postroeniia i kontrolia slozhnykh sistem, L. : Energoatomizdat, 1988, 192 pp.
3. Leskin A. A., Mal'tsev P. A. Raspredelennye informatsionnye sistemy na tezauruse: preprint No. 69, L. : LIIAN, 1988.
4. Lovtsov D. A. Informatsionnaia teoriia ergasistem: Tezaurus, M. : Nauka, 2005, 248 pp.
5. Lovtsov D. A. Teoriia informatsionnogo prava: bazisnye aspekty, Gosudarstvo i pravo, 2011, No. 11, pp. 43-51.
6. Lovtsov D. A., Bogdanova M. V. Ekonomiko-pravovoe regulirovanie oborota rezul'tatov intellektual'noi deiatel'nosti predpriiatii promyshlennosti Rossii, Ekonomika, statistika i informatika. Vestnik UMO, 2013, No. 1, pp. 53-56.
7. Lovtsov D. A., Bogdanova M. V. Sistema upravleniia oborotom rezul'tatov intellektual'noi deiatel'nosti oboronnykh predpriiatii, Trudy XXKhI Vseross. nauch.-tekhn. konf. "Problemy effektivnosti i bezopasnosti funktsionirovaniia slozhnykh tekhnicheskikh i informatsionnykh sistem" (28-29 iiunia 2012 g.) v 5-i t., t. 2, RAO -- Serpukhov : Serp. voen. in-t, 2012, pp. 107-115.
8. Lovtsov D. A., Galakhova A. E. Zashchita intellektual'noi sobstvennosti v seti Internet, Informatsionnoe pravo, 2011, No. 4, pp. 13-20.
9. Lovtsov D. A., Loban A. V. Sintez sistemy informatsionnogo obespecheniia pravovogo regulirovaniia oborota rezul'tatov intellektual'noi deiatel'nosti, Trudy IV Vseross. nauch.-prakt. konf. "Sovremennoe nepreryvnoe obrazovanie i innovatsionnoe razvitie" (23 aprelia 2014 g.), FGAU "FIRO", Serpukhov : MOU "IIF", 2014, pp. 742-746.
10. Lovtsov D. A., Loban A. V., Tsimbal V. A. Sistema informatsionnogo obespecheniia tekhnicheskogo regulirovaniia Tamozhennogo Soiuza, Izvestiia Instituta inzhenernoi fiziki, 2013, No. 1, pp. 56-64.
11. Lovtsov D. A. Effective methods of protection of the intellectual activity results in infosphere of global telematics networks, Otkrytoe obrazovanie, 2016, No. 5, pp. 85-88.

РАЗРАБОТКА СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ДЛЯ ОЦЕНКИ РИСКОВ И УГРОЗ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

*Скворцова М. А., Терехов В. И.**

Ключевые слова: *информация, национальная безопасность, интеллектуальные методы, метод анализа иерархий, метод попарного сравнения, гибридная интеллектуальная система, системы поддержки принятия решений.*

Аннотация.

Цель: *развитие научно-методической базы теории систем поддержки принятия решения с применением гибридных интеллектуальных методов и с использованием неструктурированной входной информации*

Метод: *системный анализ современного состояния проблемы оценки рисков и угроз национальной безопасности и обоснование направлений и принципов её решения.*

Результаты: *рассмотрены требования основных нормативных правовых актов и документов в области национальной безопасности, определены основные недостатки в области разработки эффективных систем поддержки принятия решения; обосновано предложение по решению соответствующих основных проблем с учетом действующей стратегии национальной безопасности.*

Определена обобщенная структурная схема гибридной интеллектуальной системы оценки рисков и угроз. Представлены результаты работы авторского прототипа системы. Обоснованы выводы по дальнейшему улучшению системы и качества получаемых результатов. Сделано обоснованное предположение об использовании прогнозирования как направления дальнейшего применения и доработки системы.

DOI: 10.21681/1994-1404-2018-4-24-34

Введение

В последние годы интенсивно развивается рынок экспертных систем, систем поддержки принятия решений и гибридных интеллектуальных систем (ГИС) [1 – 4]. Так, например, ГИС использует преимущества традиционных средств и методов искусственного интеллекта, и, в то же время, преодолевает присущие им недостатки, способна решать задачи, которые до сих пор неудовлетворительно решались отдельными методами искусственного интеллекта. Кроме того, ГИС позволяет наиболее эффективно обрабатывать формализуемые и неформализуемые знания за счёт интеграции как традиционных методов логической обработки данных, так и искусственного интеллекта – экспертных и нечётких методов, искусственных нейронных сетей, генетических алгоритмов и др.

Используя системы, созданные на основе *гибридного* подхода, можно усовершенствовать уже существующие методы и алгоритмы и создавать более эффективные подходы к решению существующих проблем.

Одной из наиболее обсуждаемых тем в настоящее время является тема глобализации и безопасности экономических, политических, правовых и культурных процессов в современном мире. Суть этих процессов заключается в нарастающей унификации *информационных* и *коммуникационных технологий*, способов принятия решений, в формировании единых стереотипов мышления и поведения субъектов, действующих в экономическом, информационном, культурном пространстве. Объектами повышенного внимания являются религии, идеологии, естественные языки, языки программирования, национальные и региональные валюты, системы стандартов и международных договоров, узаконенные правила поведения и др. Стоит заметить, что в связи с быстро меняющейся мировой обстановкой, роль государства в безопасности страны становится размытой, так как на эти процессы начинают влиять большое количество факторов, которые государство не способно быстро отследить и изменить. При определённых условиях, рассматривая, каждую

* ***Скворцова Мария Александровна,*** *ассистент кафедры компьютерных систем и сетей Московского государственного технического университета им. Н. Э. Баумана, г. Москва, Россия.*

E-mail: mariya.gavrilovaa@ya.ru

Терехов Валерий Игоревич*, кандидат технических наук, доцент, заместитель заведующего кафедрой компьютерных систем и сетей Московского государственного технического университета им. Н. Э. Баумана, г. Москва, Россия.*

E-mail: terekchow@bmstu.ru

область подробнее, можно сформировать список *рисков*, которые могут привести к негативной или критической ситуации в сфере национальной безопасности и защите интересов страны [7, 8][1].

Гибридные интеллектуальные системы, при правильном проектировании способны проанализировать и оценить существующие риски в сфере национальной безопасности Российской Федерации, сформировать сценарии развития событий в сложившейся ситуации по оценке найденных рисков и дать рекомендации о мерах защиты.

Теоретическое обоснование

В литературе [7, 8, 12] много внимания уделяется системам автоматизации, но мало говорится, о теоретической, математической и технической стороне вопроса. Поэтому, прежде чем перейти к рассматриваемому предмету представляется целесообразным определить, что будет пониматься под гибридной интеллектуальной системой, риском и оценкой риска в определённых сферах.

В качестве области исследования в работе определены военно-политическая и социально-экономическая сферы, так как согласно Стратегии национальной безопасности[2] они является основополагающими при оценке рисков и проектировании документов, касающихся безопасности Российской Федерации. Однако очевидно, что модель предлагаемой системы можно использовать в любой сфере деятельности человека (государственной, военной, политической, правовой, экономической, социальной, информационной, техногенной, экологической и др.), будь то риски на предприятиях, либо риски, угрожающие жизнедеятельности человечества. При этом объектом данного исследования является *гибридная интеллектуальная система*, под которой, в дальнейшем, будем понимать информационную систему, использующую комбинацию традиционных методов обработки данных и интеллектуальных методов [5, 8][3].

Для проведения исследований в области оценки рисков национальной безопасности Российской Федерации, необходимо руководствоваться понятиями, описанными в действующих руководящих документах[4], где под риском понимается сочетание вероятности нанесения ущерба и тяжести этого ущерба, а под оценкой риска – общий процесс анализа и оценивания риска. Анализом риска является систематическое использование полученной из всех доступных источников информации для выявления опасностей и количественной оценки риска, а допустимым риском – риск, который в данной ситуации считают приемлемым при существующих общественных ценностях.

В нормативных документах и правовых актах[5] также используется понятие *стратегического* риска, которое описывается как событие с отрицательными последствиями, применимое к любой сфере деятельности. При этом стратегические риски классифицируются по следующим признакам: по масштабам реализации опасностей, по локализации источников опасностей, по сферам возникновения рисков и по сферам реализации этих рисков и опасностей. Основной *целью* является недопущение перехода от риска к вызову, а от вызова к угрозе, так как угроза является максимальным уровнем опасности для жизнедеятельности человека.

В иностранных публикациях[6], особое внимание уделяется сравнению понятий риска, опасности и угрозы, как однотипным понятиям, не имеющим сильных различий в понимании. Поэтому, в данном исследовании, под понятием риска понимается любая степень опасности (угроза, вызов или риск).

Изучая статистику отчётов различных российских и международных организаций, можно прийти к *выво-*

[1] См. также: Положение о системе независимой оценки рисков в области пожарной безопасности, гражданской обороны и защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера на территории Российской Федерации. Режим доступа: http://41.mchs.gov.ru/document/2912473 (дата обращения 01.12.2018); Федеральный закон «О стратегическом планировании в Российской Федерации». – URL: http://pravo.gov.ru/proxy/ips/docbody=&nd=102354386 (дата обращения 01.12.2018).

[2] Указ президента Российской Федерации «Стратегия национальной безопасности Российской Федерации до 2020 года». – URL: https://rg.ru/2009/05/19/strategia-dok.html (дата обращения 01.12.2018).

[3] См. также: Official site of Federation of European risk management associations. [Online]. Available: http://www.ferma.eu/ (дата обращения 01.12.2018); Global Trends: Paradox of Progress. [Online]. Available: https://www.dni.gov/ (дата обращения 01.12.2018); Official site of the Eurasian group on combating money laundering and financing of terrorism (EAG). [Online]. Available: http://www.eurasiangroup.org (дата обращения 01.12.2018); Официальный сайт глобальной политики. [Online]. Available: http://www.russiapost.su/ (дата обращения 01.12.2018); Прогноз социально-экономического развития РФ до 2030 года. – URL: http://economy.gov.ru/minec/activity/sections/macro/prognoz/doc20130325_06 (дата обращения 01.12.2018); Банк документов Президента РФ / URL: http://kremlin.ru/acts/bank (дата обращения 01.12.2018); Банк документов Правительства РФ по Стратегическому планированию в разных областях и сферах / URL: http://government.ru/govworks/625/events/ (дата обращения 01.12.2018); Документы стратегического планирования Российской Федерации URL: https://strategyrf.ru/rf/documents (дата обращения 01.12.2018).

[4] Положение о системе независимой оценки рисков в области пожарной безопасности, гражданской обороны и защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера на территории российской федерации. Режим доступа: http://41.mchs.gov.ru/document/2912473 (дата обращения 01.12.2018); ГОСТ Р 51898-2002. Аспекты безопасности. Правила включения в стандарты: сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[5] См., например: ГОСТ Р 51898-2002. Аспекты безопасности. Правила включения в стандарты: сочетание вероятности нанесения ущерба и тяжести этого ущерба; The IEEE website. [Online]. Available: http://www.ieee.org/ (дата обращения 01.12.2018); Федеральный закон «О стратегическом планировании в Российской Федерации» URL: http://pravo.gov.ru/proxy/ips/docbody=&nd=102354386 (дата обращения 01.12.2018); Федеральный закон «О безопасности» URL: https://rg.ru/2010/12/29/bezopasnost-dok.html (дата обращения 01.12.2018); SIPRI Yearbook 2017: Armaments, Disarmament and International Security // Oxford University Press. [Online]. Available: https://www.sipri.org/sites/default/files/2017-09/yb17-summary-eng.pdf (дата обращения 01.12.2018).

[6] The IEEE website. [Online]. Available: http://www.ieee.org/ (дата обращения 01.12.2018).

ду, что по любой сфере жизнедеятельности человека, имеется достаточное количество достоверной информации (законы, отчёты правительства, отчёты независимых экспертов и аудиторов, новостные источники). Каждая из этих организаций раз в год делает отчёт по текущей ситуации в мире и делится прогнозами с вероятными сценариями развития событий. Поэтому, очень важно понять, как определяют прогнозирование эксперты из Российской Федерации. Эксперты определяют прогнозирование как деятельность участников стратегического планирования по разработке научно-обоснованных представлений о рисках социально-экономического развития, об угрозах национальной безопасности Российской Федерации, о направлениях, результатах и показателях социально-экономического развития Российской Федерации, субъектов страны и муниципальных образований. Национальная безопасность Российской Федерации – это состояние защищённости личности, общества и государства от внутренних и внешних угроз, при котором обеспечивается реализация конституционных прав и свобод граждан Российской Федерации.

Структура системы поддержки принятия решений для оценки рисков и угроз

В настоящее время интеллектуальные системы, как правило, не разрабатываются отдельно, а встраиваются в виде модулей в традиционные информационные системы для решения задач, связанных с интеллектуальной обработкой данных и знаний.

На рис. 1 показана обобщённая структура системы поддержки принятия решений (СППР), как составной части гибридной интеллектуальной системы для оценки рисков на основе неструктурированной информации, разделённая на несколько основных модулей, работа которых взаимосвязана.

Модуль «Сбор и обработка неструктурированной информации». В данном модуле происходит сбор необходимой информации из неструктурированных источников, посредствам автоматических роботов. Далее информация проходит предобработку для последующей обработки, хранения и обучения ГИС. Необходимо отметить, что задача сбора информации из неструктурированных и слабоструктурированных источников не является объектом данного исследования. Все данные были получены с помощью специально написанных роботов, которые автоматически собирали информацию из заданных источников.

Модуль «Извлечение данных» предназначен для извлечения эталонных данных и эталонных моделей рисков для последующего обучения системы. Также извлечённые данные обрабатываются под шаблоны, которые необходимы для работы системы.

В *модуль «Интеллектуальный анализ данных»* входят подпрограммы, результат анализа которых выводится пользователю в формате отчёта, содержащего оптимальные решения.

Модуль «Оценка рисков на основе показателей» предназначен для проведения расчётов на основе оценок экспертов по множеству показателей с целью принятия решения о заблаговременной подготовке сценариев развития в анализируемой сфере при наступлении критической ситуации.

Модуль «Оценка рисков на основе событий» предназначен для оценки текущего состояния анализируемой сферы и определения рисков на основе событий, выделенных в потоке текстовых сообщений.

Модуль «Общая оценка рисков» предназначен для сравнения результатов работы функций, предназначенных для оценки обстановки в анализируемой сфере и формирования общего состояния с использованием метода анализа иерархий.

Рис. 1. Обобщённая структура СППР оценки рисков и угроз

Модели оценки рисков на основе полученной информации

Существует множество критериев, на основании которых оцениваются риски в различных сферах деятельности. К таким критериям можно отнести: множество сообщений, описывающих событие; вектор слов события; множество имен персон и организаций; вектор релевантности события темам и др. Так, например, при сопоставлении документов и событий определяется сходство между соответствующими компонентами их моделей с использованием различных мер близости.

Заключительные части эталонных ситуаций, признанных близкими к текущей, являются возможными сценариями развития текущей ситуации. Та из них, для которой вероятность аналогичности текущей ситуации максимальна, является наиболее вероятным сценарием.

В исследовании были определены три варианта развития ситуаций:

- по пессимистичному сценарию (нужно выбрать дальнейшее действие, которое необходимо предпринять);
- по наиболее вероятному сценарию (действие выбирается из заранее внесённых);
- по оптимистичному сценарию (указывается срок выполнения определённых действий).

Для определения приоритетности оптимистичного и пессимистичного сценариев, сформированных на основе эталонных ситуаций, используется метод анализа иерархий [3, 5, 6, 9, 10, 12, 13], позволяющий вычислить приоритет каждого из сценариев на основе набора критериев. Приоритетность критериев относительно цели вычисляется на основе попарных сравнений, выполняемых экспертами на этапе обучения гибридной системы (интеллектуального модуля).

Метод анализа иерархий (МАИ) разработан известным специалистом в области теории принятия решений Томасом Саати (*Thomas L. Saaty*). МАИ является методологической основой для решения задач выбора альтернатив посредством их многокритериального рейтингования, имеет строгое математическое обоснование. Под словом *рейтингование* подразумевается операция сравнения двух объектов и установление численного значения в соответствии с выбранной шкалой взаимного влияния. Т. Саати предположил, что модель ситуации принятия решения можно представить в виде многоуровневой декомпозиции проблемы на относительно небольшие группы.

В методе анализа иерархий рейтингование внутри кластера (группы) элементов осуществляется методом парных сравнений, что позволяет определить приоритеты среди всей совокупности, сравниваемых объектов. Для выявления приоритетов используется метод вычисления собственных векторов матрицы парных сравнений. Т. Саати предложил упрощённый вариант вычисления собственных векторов, используя значения близости оценок, как среднегеометрическую величину. При этом выявлять ошибочные суждения при парном сравнении элементов (объектов) кластера, Саати предложил с помощью процедуры согласования данных, которая основана на вычислении частного индекса согласования сравнений с последующим сравнением, полученного частного индекса, со среднестатистической величиной отклонения. Полученные данные позволяют принять или отклонить гипотезу о достоверности полученных данных.

Удобство МАИ заключается в том, что лицо, принимающее решение (ЛПР), может получить рейтинг альтернатив (вариантов решений), выраженных количественной оценкой. Причём, чем более предпочтительна альтернатива по избранному критерию, тем больше ее приоритет.

Формирование структуры модели принятия решения в МАИ достаточно трудоёмкий процесс. Вместе с тем процедуры расчётов рейтингов в МАИ просты, что выгодно отличает его от других методов принятия решений. Схема применения метода не зависит от предметной области, в которой принимаются решения. Основное преимущество МАИ заключается в том, что исследователь получает количественную оценку предпочтительности посредством рейтингования. Это способствует полному и адекватному выявлению предпочтений лица, принимающего решение.

Наиболее часто ЛПР, с помощью МАИ, решает поставленные задачи при следующих условиях:

1. имеется множество вариантов решения задачи или несколько сравниваемых объектов, при этом необходимо выбрать лучший вариант;
2. варианты решения зависят от определённых факторов (критериев), необходимо учесть зависимость каждого варианта решения от влияния множества показателей, которые принадлежат критериям;
3. данные, которые характеризуют критерии, часто не определены или не точны, а решение будет определённым в том случае, если будут определены рейтинги критериев.

При этом Т. Саати, предлагая методологию МАИ, исходил из того, что окончательное решение должен принять ЛПР, а точнее – индивидуум или группа индивидуумов, а целью ЛПР является снизить риск решения за счёт определения сравнительных характеристик для каждого критерия. С позиции ЛПР риск – это событие, связанное с опасным явлением или процессом, которое может произойти или не произойти. Исходя из этого ЛПР выдвигает, прежде всего, *цель,* к которой стремится при постановке задачи с многокритериальной оценкой альтернатив, а конечным результатом решения задачи является:

а) выбор наиболее подходящего варианта решения из нескольких;

б) получение количественного показателя для объекта, который сравнивается с аналогами;

в) распределение альтернатив в порядке их значимости с установкой весовых коэффициентов для каждой из них;

г) определение вероятности свершения события в будущем в зависимости от изменяющихся условий.

Таким образом, следует поставить задачу шире: необходима *методика* оценки природных и техногенных рисков, учитывающая указанные ограничения и сложности и отвечающая заданным требованиям.

Чтобы оценить эффективность методов, необходимо рассмотреть их множество, в соответствии с которым методы можно разделить на три основные группы:

1) статистические методы;

2) методы экспертных оценок;

3) методы моделирования.

Для того, чтобы использовать методы для оценки природных и техногенных рисков, необходимы уровни шкалы для оценки риска. Входными переменными могут служить значения трёх факторов риска на отрезке [0, 1], описанные лингвистическим *терм-множеством* (очень низкий, низкий, средний, высокий, очень высокий), представленными в таблице.

Приоритетность альтернатив относительно каждого критерия (определённого риска) вычисляется автоматически на основе характеристик сценариев. По итогам расчёта приоритета сценариев определяются наиболее оптимистичный и пессимистичный сценарии (рис. 2).

Таблица

Уровни шкалы при оценке факторов риска

Уровни шкалы	Риск	Наносимый ущерб
Очень низкий (от 0 до 0.2)	Событие практически никогда не происходит	Незначительные материальные потери и потери ресурсов, которые быстро восполняются
Низкий (от 0.2 до 0.4)	Событие случается редко	Более заметные потери материальных активов, существенное влияние на репутацию и ущемление интересов
Средний (от 0.4 до 0.6)	Событие вполне возможно при определённом стечении обстоятельств	Достаточные потери материальных активов или ресурсов, или достаточные урон репутации и интересов
Высокий (от 0.6 до 0.8)	Скорее всего, событие произойдёт при каком обстоятельстве	Значительные урон репутации и интересам, представляет сильную угрозу
Очень высокий (от 0.8 до 1)	Событие вероятнее всего произойдёт с большой вероятностью	Разрушительные последствия для этой сферы или всех сфер в совокупности

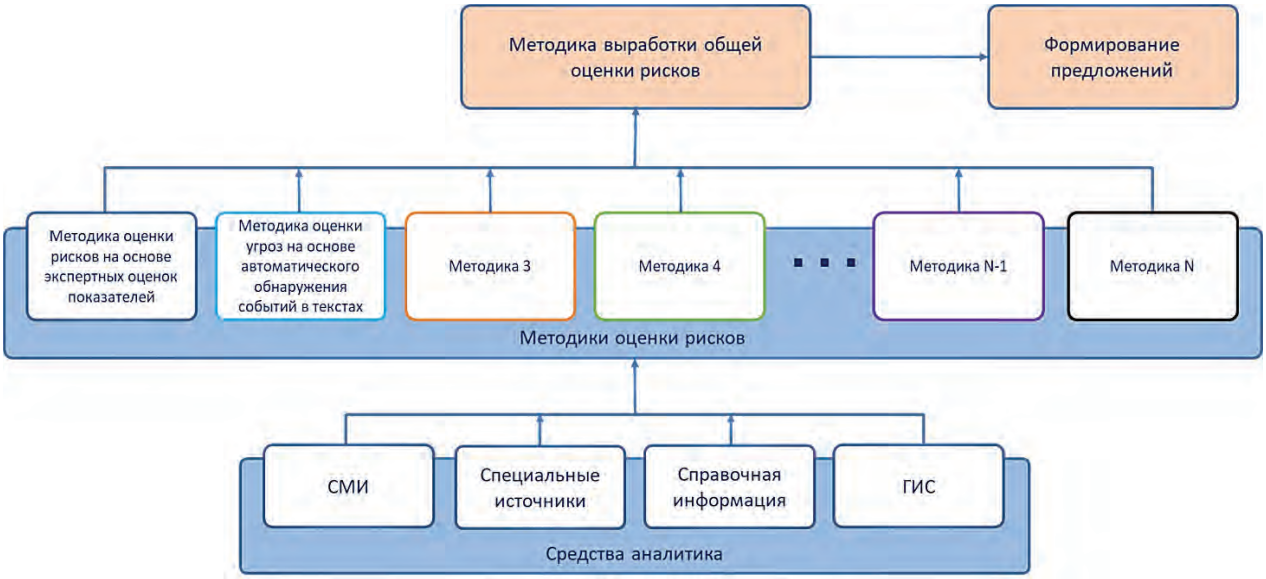

Рис. 2. Алгоритм вычисления оптимального сценария для формирования предложений

Анализ задачи обоснования варианта методики оценки возможных рисков и угроз показал, что она является слабоструктурированной, многокритериальной задачей оптимизации. Для решения таких задач предложено много математических методов. При этом в большинстве методов используется сложный математический аппарат, с помощью которого осуществляется логическая обработка данных, проверка их согласованности, адекватности для предложенной модели, проверка статистической надёжности результатов. Поэтому приходится проводить множество экспериментов и измерений, чтобы получить количественные оценки. Кроме того, часто приходится разделять задачу на несколько независимых модулей, осуществлять сбор данных и их сопряжение, что становится весьма громоздкой процедурой и требует много времени, ресурсов и сил.

Практическая реализация

В разработанном [11] прототипе системы в качестве исходных данных для анализа информации были использованы данные из неструктурированных или слабоструктурированных источников, состоящих из 40 сайтов и более 90 разделов по этим сайтам (федеральные и региональные сайты с открытыми данными, информационные агентства и новостные порталы, сайты с аналитической информацией и др.) – это более 600 *млн*. сообщений, собранных при помощи мониторинга ресурсов один раз в час.

Практические эксперименты для оценки рисков были проведены на полученных из неструктурированных источников данных следующими методиками: *методика* оценки рисков на основе событий, *методика* оценки рисков на основе показателей и общая *методика* оценки рисков национальной безопасности Российской Федерации.

В основу методики оценки рисков на основе событий лёг метод графов в котором скорость роста активности темы (события) определяет диаметр соответствующего узла, а скорость роста активности связи между темами – толщину соответствующего ребра. Как видно на рис. 3 информация о росте активности рисков по событиям и связей между ними выполняется построением графа, в котором узлы соответствуют темам, а ребра – связям между темами. Цвет узлов (рёбер) отражает скорость роста активности соответствующих рисков. Узлы и рёбра могут иметь три возможных цвета (в оригинальном изображении): зелёный (медленный рост активности темы/связи между темами); жёлтый (средний рост активности темы/связи между темами); красный (быстрый рост активности темы/связи между темами).

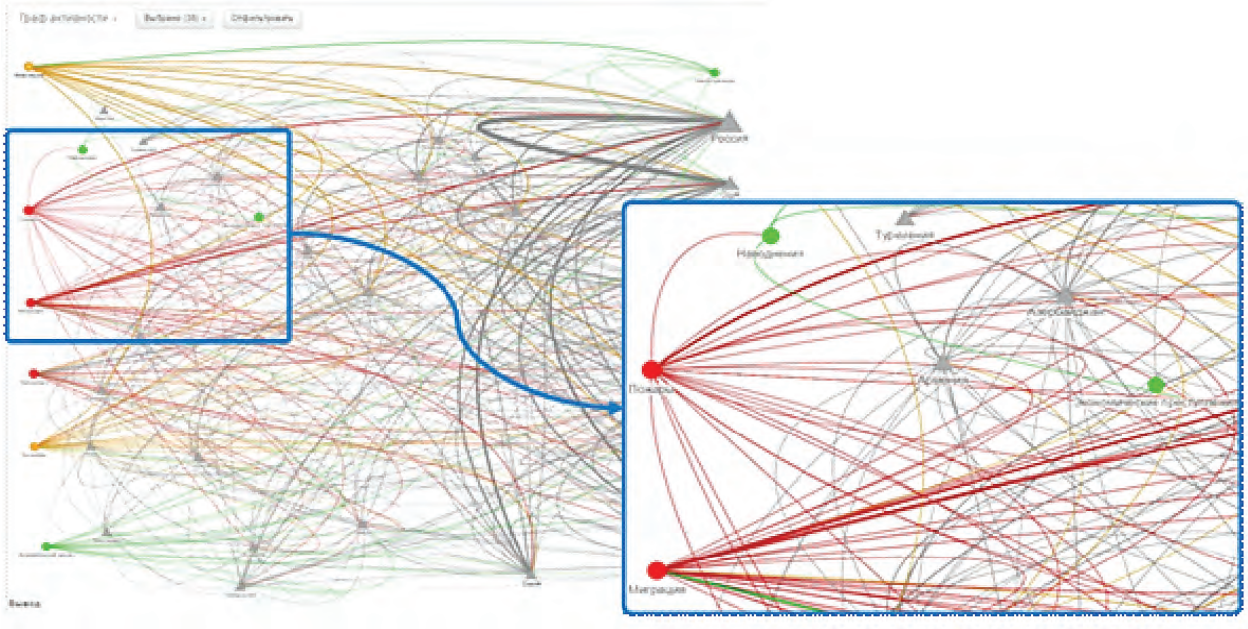

***Рис. 3. Отображение результатов работы методики оценки рисков на основе событий** (слева – **построение обобщённого графа,** справа – **увеличенная часть графа**)*

В основу методики оценки рисков на основе показателей взято вычисление среднего интервального показателя по каждой сфере жизнедеятельности, задание весов для групп показателей в диапазоне [0,1] и задание значений показателей в диапазоне [0,1]. Состояние обстановки относительно события, определяется в несколько этапов.

На первом этапе оператор (человек, отвечающий за введение данных в систему), либо эксперт, на основе экспертной оценки вводит необходимые значения показателей по всем сферам. Ввод значений показателей производится путём установки их значений в «1». После ввода значений показателей производится формирование отчётов, в котором выводятся значения по сферам показателей и интегральный показатель (рис. 4).

В основу общей методики оценки рисков был положен метод анализа иерархий и метод попарного сравнения. Особое внимание необходимо уделить оценке важности критериев между собой.

Рис. 4. Форма отчёта, содержащего форму для ввода показателя (слева) и таблицу по оценки рисков во всех сферах жизнедеятельности (справа)

Перед формированием отчёта по общей оценке рисков сначала необходимо заполнить таблицу численными значениями метода попарного сравнения, а затем по полученным результатам и проведённому анализу с помощью МАИ сформировать оценку с учётом введённых альтернатив. Все данные вводятся в систему согласно полученным от экспертов оценкам во всех сферах жизнедеятельности.

Результаты исследования

Реализация предложенной в статье ГИС является достаточно сложной и трудоёмкой научно-прикладной задачей, но при этом данная система будет чрезвычайно востребованной для оценки военно-политической обстановки в Российской Федерации, а также при оценке рисков национальной безопасности (рис. 5).

Основные же сложности *анализа* связаны с оценкой рисков и его факторов (угроз, возможного ущерба, уязвимостей) и вызваны следующими проблемами:

1) неполнота информации о составляющих риска и их неоднозначные свойства;

Для реализации предлагаемых подходов был проведён анализ и проработка методов, алгоритмов и программного обеспечения ГИС оценки рисков на основе неструктурированной информации. Полученные результаты позволили разработать *программное обеспечение*, которое может функционировать под различными программными платформами. Хранение данных организовано с помощью СУБД *PostgreSQL*. При создании интерфейсных компонентов программ использовались средства *web*-разработки, поэтому программы могут использоваться на различных программно-аппаратных платформах (стационарные устройства, планшеты, смартфоны и др.).

Заключение

Проведённое теоретико-экспериментальное исследование, показывает, что данная тема очень сложна, так как каждый процесс требует детальной и глубокой проработки. В задачах принятия стратегических решений часто приходится опираться скорее на опыт и интуицию специалистов, нежели на имеющиеся объективные данные. В этом случае результаты, полученные

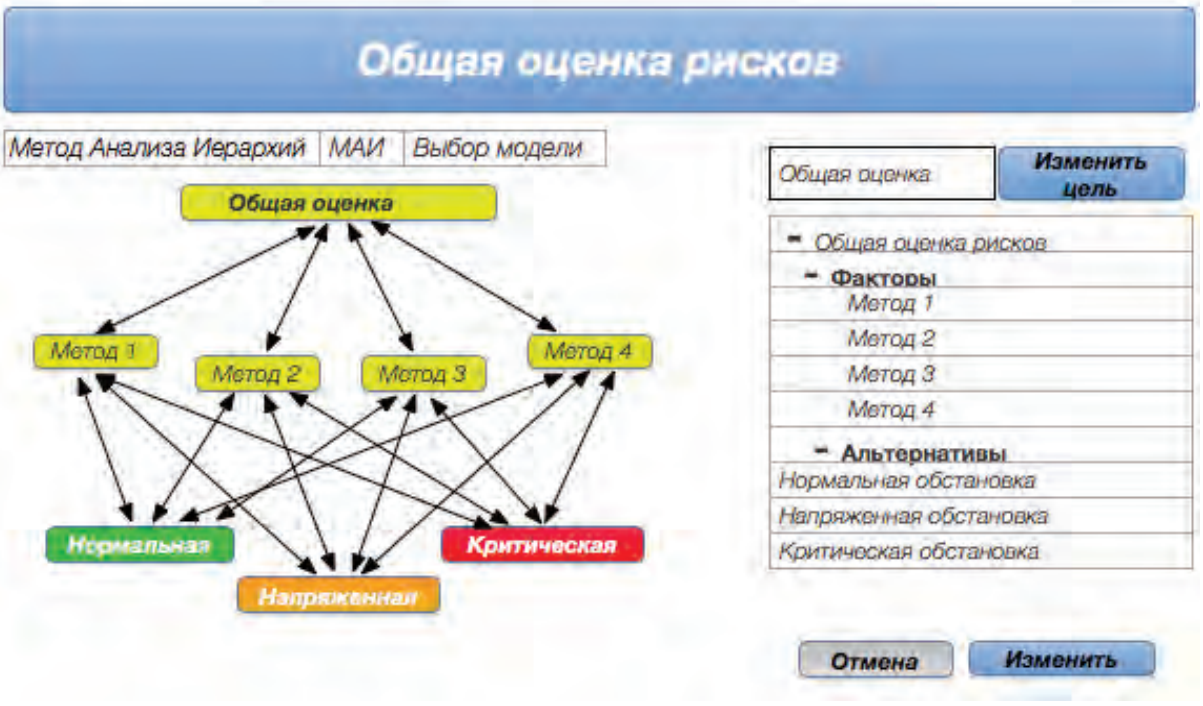

Рис. 5. Общая оценка рисков

2) сложность создания модели информационной системы и оценки её уязвимости;

3) длительность процесса оценки и быстрая потеря актуальности её результатов;

4) сложность агрегации данных из различных источников, в том числе статистической информации и экспертных оценок;

5) необходимость привлечения нескольких специалистов по анализу рисков для повышения адекватности оценок.

методом анализа иерархий, в сочетании с методом попарного сравнения могут быть более реалистичными, чем результаты, полученные другими формализованными методами.

Для получения более точных и качественных результатов по оценке рисков предлагается использование большего количества частных методик, которые будут охватывать как можно большее количество сфер человеческой жизнедеятельности.

Рецензент: ***Бетанов Владимир Вадимович,*** *доктор технических наук, профессор, член-корреспондент Российской академии ракетных и артиллерийских наук, начальник центра АО «Российские космические системы», г. Москва, Россия.*

E-mail: *vlavab@mail.ru*

Литература

1. Бетанов В. В., Ларин В. К. Концепция гибридной технологии баллистико-навигационного обеспечения наземно-космической связи в ГАС РФ «Правосудие» // Правовая информатика. 2018. № 2. С. 39 – 46.
2. Бетанов В. В., Ларин В. К. Построение эффективной экспертной системы баллистико-навигационного обеспечения наземно-космической связи в ГАС РФ «Правосудие» // Правовая информатика. 2017. № 3. С. 50 – 57.
3. Колесников А. В., Кириков И. А., Листопад С. В. Гибридные интеллектуальные системы с самоорганизацией: координация, согласованность, спор. М.: ИПИ РАН, 2014. 189 с.
4. Ловцов Д. А., Сергеев Н. А. Информационно-математическое обеспечение управления безопасностью эргатических систем. III. Экспертная информационная система // НТИ РАН. Сер. 2. Информ. процессы и системы. 2001. № 11. С. 23 – 30.
5. Тарасов В. Б. От многоагентных систем к интеллектуальным организациям: философия, психология, информатика. М.: Эдиториал УРСС, 2002. 352 с.
6. Черненький В. М. Алгоритмическая модель описания дискретного процесса функционирования системы // technomag.edu.ru: Наука и Образование: электронное научно-техническое издание. 2011. Вып. 12. URL http://technomag.edu.ru/doc/292997.html (дата обращения 01.12.2018).
7. Чечкин А.В. Интеллектуальная информационная система на основе радикального моделирования как инструментальное средство обеспечения комплексного развития // Нейрокомпьютеры: разработка, применение. 2015. № 5. С. 7 – 13.
8. Chernenkiy V., Gapanyuk Yu., Nardid A., Skvortsova M., Gushcha A., Fedorenko Y., Picking R. Using the metagraph approach for addressing RDF knowledge representation limitations // Internet Technologies and Applications. 2017. DOI: 10.1109/ITECHA.2017.8101909.
9. Pugh J.K., Stanley K.O. Evolving Multimodal Controllers with HyperNEAT // Proceedings of the Genetic and Evolutionary Computation Conference. New York, NY: ACM, 2013. 8 p.
10. Riza S., Murtuzayeva M. Application pair comparisons method to the investments distribution in parameters of ecological sustainability // Proceedings of the IV International Conference «Problems of Cybernetics and Informatics» (Sept. 2012). 2012. P. 1 – 3.
11. Skvortsova M., Terechov V., Grout V. Hybrid Intelligent System for Risk Assessment based on Unstructured Data // Proceedings of the 2017 IEEE Russia Section Young Researchers in Electrical and Electronic Engineering Conference. 2017. P. 560 – 564. DOI: 10.1109/ElConRus.2017.7910616.
12. Xiao X., Zhang H., Hasegawa O. Density Estimation Method Based on Self-Organizing Incremental Neural Network and Error Estimation // Proceedings of the Neural Information Processing: 20th International Conference. Daegu, Korea. 2013. P. 43–50.
13. Xu SW-J., Dong Y-C., Xiao W-L. Is It Reasonable for Saaty's Consistency Test in the Pairwise Comparison Method?" // Proceedings of the ISECS International Colloquium on Computing, Communication, Control, and Management (3 – 4 Aug. 2008). Vol. 3. 2008. P. 294 – 298.

DEVELOPMENT OF A DECISION SUPPORT SYSTEM FOR THE ESTIMATION OF RISKS AND THREATS OF NATIONAL SAFETY

Maria Skvortsova, *Research Assistant of the Computer systems and networks Chair of Bauman Moscow State Technical University, Moscow, Russia.*
E-mail: *mariya.gavrilovaa@ya.ru*

Valery Terekhov, *Ph.D., Associate Professor, Deputy Chief of the Computer systems and networks Chair of Bauman Moscow State Technical University, Moscow, Russia.*
E-mail: *terekchow@bmstu.ru*

Abstract.

Improving of scientific and methodical base of the theory of decision support systems using hybrid intelligent methods and using unstructured input information.

Methods: *system analysis of the current state of problem of assessing risks and threats to national security and the justification of the directions and principles for its decision.*

Results: *the main normative legal acts and documents in the field of national security are considered, the main shortcomings in the development of effective decision support systems are identified; the proposed solution to the main problems, taking into account the national security strategy.*

A generalized structural diagram of a hybrid intelligent risk and threat assessment system is defined. The results of the prototype system are presented. Conclusions on further improvement of the system and the quality of the results are substantiated. The substantiated assumption is made about the use of forecasting, as a way of further use and refinement of the system.

References

1. Betanov V. V., Larin V. K. Kontseptsiia gibridnoi tekhnologii ballistiko-navigatsionnogo obespecheniia nazemno-kosmicheskoi sviazi v GAS RF "Pravosudie", Pravovaia informatika, 2018, No. 2, pp. 39-46.
2. Betanov V. V., Larin V. K. Postroenie effektivnoi ekspertnoi sistemy ballistiko-navigatsionnogo obespecheniia nazemno-kosmicheskoi sviazi v GAS RF "Pravosudie", Pravovaia informatika, 2017, No. 3, pp. 50-57.
3. Kolesnikov A. V., Kirikov I. A., Listopad S. V. Gibridnye intellektual'nye sistemy s samoorganizatsiei: koordinatsiia, soglasovannost', spor, M. : IPI RAN, 2014, 189 pp.
4. Lovtsov D. A., Sergeev N. A. Informatsionno-matematicheskoe obespechenie upravleniia bezopasnost'iu ergaticheskikh sistem. III. Ekspertnaia informatsionnaia sistema, NTI RAN, ser. 2, Inform. protsessy i sistemy, 2001, No. 11, pp. 23-30.
5. Tarasov V. B. Ot mnogoagentnykh sistem k intellektual'nym organizatsiiam: filosofiia, psikhologiia, informatika, M. : Editorial URSS, 2002, 352 pp.
6. Chernen'kii V. M. Algoritmicheskaia model' opisaniia diskretnogo protsessa funktsionirovaniia sistemy, technomag. edu.ru: Nauka i Obrazovanie: elektronnoe nauchno-tekhnicheskoe izdanie, 2011, vyp. 12, URL: http://technomag.edu.ru/doc/292997.html (data obrashcheniia 01.12.2018).
7. Chechkin A.V. Intellektual'naia informatsionnaia sistema na osnove radikal'nogo modelirovaniia kak instrumental'noe sredstvo obespecheniia kompleksnogo razvitiia, Neirokomp'iutery: razrabotka, primenenie, 2015, No. 5, pp. 7-13.
8. Chernenkiy V., Gapanyuk Yu., Nardid A., Skvortsova M., Gushcha A., Fedorenko Y., Picking R. Using the metagraph approach for addressing RDF knowledge representation limitations, Internet Technologies and Applications, 2017. DOI: 10.1109/ITECHA.2017.8101909.
9. Pugh J.K., Stanley K.O. Evolving Multimodal Controllers with HyperNEAT, Proceedings of the Genetic and Evolutionary Computation Conference. New York, NY: ACM, 2013. 8 p.
10. Riza S., Murtuzayeva M. Application pair comparisons method to the investments distribution in parameters of ecological sustainability, Proceedings of the IV International Conference "Problems of Cybernetics and Informatics" (Sept. 2012), 2012. P. 1-3.
11. Skvortsova M., Terechov V., Grout V. Hybrid Intelligent System for Risk Assessment based on Unstructured Data, Proceedings of the 2017 IEEE Russia Section Young Researchers in Electrical and Electronic Engineering Conference, 2017. P. 560-564. DOI: 10.1109/EIConRus.2017.7910616.

12. Xiao X., Zhang H., Hasegawa O. Density Estimation Method Based on Self-Organizing Incremental Neural Network and Error Estimation, Proceedings of the Neural Information Processing: 20th International Conference. Daegu, Korea, 2013. R. 43-50.
13. Xu SW-J., Dong Y-C., Xiao W-L. Is It Reasonable for Saaty's Consistency Test in the Pairwise Comparison Method?", Proceedings of the ISECS International Colloquium on Computing, Communication, Control, and Management (3-4 Aug. 2008). Vol. 3. 2008. P. 294-298.

ВЫЯВЛЕНИЕ ПОТЕНЦИАЛЬНО ОПАСНЫХ АБОНЕНТОВ ЧАСТНЫХ ВИРТУАЛЬНЫХ СЕТЕЙ

Голосов П. Е., Зелюкин Н. Б. *

Ключевые слова: *компьютерные сети, анализ, классификация, методика, сетевой трафик, IPsec.*

Аннотация.

Цель*: рассмотреть вопрос безопасности в VPN-сетях. Этот вопрос поднимается в связи с широким и неуклонно растущим рынком VPN-услуг, а также их повсеместным применением для защиты чувствительных данных. В условиях шифрования передаваемых данных традиционные методики анализа поведения абонентов не работают, таким образом, необходимы иные подходы к обеспечению безопасности и предотвращению атак на частные виртуальные сети.*

Метод: *информационный анализ, моделирование и функционально-логическая классификация.*

Результат: *разработана методика классификации абонентов VPN-сетей. Методика предполагает дополнительный анализ служебного трафика и основана на том, что передаваемая служебная информация зависит от настроек, характерных для абонента, самого абонента и особенностей используемого оборудования. Анализируя эту информацию можно классифицировать трафик и выделять в нем группы VPN-сессий, использующий нестандартное оборудование и/или настройки и требующие более подробного аудита.*

Был проведен экспериментальный анализ тестовой записи трафика, в процессе которого были выявлены IPsec-абоненты, использующие нестандартные реализации IPsec-протокола, и представляющие потенциальную угрозу безопасности корпоративной VPN-сети.

DOI:10.21681/1994-1404-2018-4-35-42

Введение

На сегодняшний день компьютерные технологии проникли практически во все сферы деятельности человека. Электронный документооборот вытесняет традиционный бумажный, общение между людьми постепенно переносится в сеть [2]. Использование компьютерных сетей упрощает и ускоряет процесс передачи информации на дальние расстояния. Также наблюдается постоянное удешевление стоимости передачи 1 *Гб* трафика. Все эти факторы делают Интернет чрезвычайно привлекательным средством для передачи информации.

Однако сеть Интернет не является доверенной, т.е. нет никаких гарантий, что передаваемые данные не будут прочитаны, изменены или их передача не будет заблокирована. В связи с этим возникла потребность в защите передаваемых данных [7 – 10], что дало толчок развитию класса технологий *VPN* (*Virtual Private Network*) – виртуальная защищенная сеть. В основе *VPN* сетей лежит понятие *туннель* – виртуальное соединение типа точка-точка, защищающее данные при передаче через него. Слово «виртуальное» включено сюда для того, чтобы подчеркнуть, что соединение не является постоянным, а создается и существует только во время передачи данных.

По данным сайта *www.statista.com* более 30% пользователей Интернета в таких крупных странах, как Индия и Китай, используют *VPN*-сети (рис. 1). При этом ежедневно к услугам *VPN*-сетей прибегают около 40% из пользователей. Спрос на услуги *VPN* неуклонно растет, о чем свидетельствуют оценочная стоимость рынка и её прогнозы.

* ***Голосов Павел Евгеньевич,*** *кандидат технических наук, декан факультета информационных технологий и анализа данных Российской академии народного хозяйства и государственной службы при Президенте РФ, г. Москва, Россия.*

E-mail: golosov-pe@ranepa.ru

Зелюкин Николай Борисович, *младший научный сотрудник Российской академии народного хозяйства и государственной службы при Президенте РФ, г. Москва, Россия.*

E-mail: zelyukin-nb@universitas.ru

Рис. 1. Диаграмма удельной доли числа VPN-пользователей ряда стран

Вместе с развитием технологий VPN возникла проблема анализа угроз безопасности сетей [12][1], ведь обычные инструменты, полагающиеся на анализ поведения абонентов и передаваемых ими данных в условиях сквозного шифрования точка-точка не работают. По данным на начало 2018 г., около 30% пользователей *VPN*-сетей пользуются виртуальными сетями для удаленного доступа к рабочему месту. Компрометация передаваемых данных в этом случае может нанести финансовый вред организации, а злоумышленнику – обогатиться. На рис. 2 представлены оценки объемов рынка *VPN*-услуг до 2022 г.

Вместе с ростом популярности виртуальных сетей появляются средства для их анализа и поиска уязвимостей. Например, утилита *Ike-scan* предназначена для формирования и отсылки служебных *IPsec*-пакетов с разными параметрами и разбора ответа[2].

Таким образом, в то время как пользовательские данные защищены шифрованием в *VPN*-сетях, сами виртуальные сети становятся объектом интереса со

Рис. 2. Динамика роста объемов рынка VPN-услуг на среднесрочную перспективу

стороны злоумышленников. Вместе с тем, растущий рынок услуг только подогреет их интерес в будущем и стимулирует развитие инструментов компрометации

[1] *См. также:* Moore W., Papgiannaki D. Toward the Accurate Identification of Network Applications, 2005. - URL http://www.cl.cam.ac.uk/~awm22/publications/moore2005toward.pdf (дата обращения 06.12.2018); Kim H., Fomenkov M., Barman D., Faloutsos M., Lee K. Internet traffic classification demystified: myths, caveats, and the best practices, 2008. – URL http://www.caida.org/publications/ papers/2008/classification_demystified/classification_demystified.pdf (дата обращения 06.12.2018); Маркин Ю., Санаров А. Обзор современных инструментов анализа сетевого трафика. – URL http://www.ispras.ru/preprints/docs/prep_27_2014.pdf (дата обращения 04.11.2018).

[2] Методическое пособие. IPsec. «Методы и средства защиты информации», ПетрГУ, 2006. – URL http://dfe.karelia.ru/koi/posob/security/index.html#0 (дата обращения 4.11.2018).

VPN-шлюзов. Все это свидетельствует об актуальности исследований в области безопасности *VPN*-сетей.

При анализе безопасности автоматизированной информационной системы (АИС) под *угрозой* будем понимать возможное событие, которое может привести к нанесению ущерба чьим-либо интересам [6]. Классификацию угроз целесообразно проводить по следующим базовым признакам:

1. По природе возникновения:
   a. естественные угрозы, не связанные с деятельностью человека, например, стихийные бедствия;
   b. искусственные угрозы, например, хакерские атаки.
2. По положению источника угроз:
   a. вне контролируемой зоны АИС;
   b. в пределах контролируемой АИС, например, подслушивающие устройства, хищение носителей;
   c. Непосредственно в АИС, например, активность вирусов.
3. По степени преднамеренности воздействия:
   a. угрозы, вызванные некомпетентностью персонала;
   b. преднамеренные действия злоумышленника.
4. По непосредственному источнику угроз:
   a. природная среда;
   b. человек, например, подкупленный сотрудник;
   c. санкционированные программно-аппаратные средства;
   d. несанкционированные программно-аппаратные средства [10, 11].
5. По степени зависимости от активности АИС:
   a. независимо от активности АИС;
   b. только в процессе обработки данных.
6. По степени воздействия на АИС:
   a. пассивные угрозы, при реализации которых структура и работоспособности АИС не меняется, например, копирование конфиденциальных данных;
   b. Активные угрозы, при которых меняется структура АИС, например, внедрение *троянских* программ [11].
7. По способы доступа к ресурсам АИС:
   a. доступ с использованием стандартных интерфейсов АС, например, доступ при помощи украденного пароля;
   b. доступ с использованием недокументированных возможностей АИС.
8. По месту расположения информации, хранимой и обрабатываемой АИС:
   a. информация на внешних запоминающих устройствах;
   b. информация, находящаяся в оперативной памяти АИС;
   c. информация, циркулирующая в каналах связи;
   d. информация на устройствах вывода, например, снимок монитора сотрудника на скрытую камеру.

Кратко классификатор признаков, релевантных целям работы, представлен в таблице.

Таблица

Признаки и группы классификации угроз

№	Признак классификации	Классификационная группа
	Природа возникновения	Искусственные угрозы
	Положение источника угрозы	Вне АС
	Преднамеренность воздействия	Преднамеренные
	Непосредственный источник угрозы	Несанкционированные программно-аппаратные средства
	Активность АИС	Требующие активной АИС
	Степень воздействия	Пассивные и активные
	Способ доступа к ресурсам	Использование недокументированных возможностей АИС
	Расположение информации	Каналы связи

В качестве метода классификации абонентов корпоративных *IPsec*-сетей можно использовать метод, основанный на анализе служебной информации в *VPN*-трафике. Классификация позволяет выявить аномалии в используемом оборудовании и/или программном обеспечении, и выделить среди среднестатистических пользователей тех, кто может использовать нестандартные реализации клиентов для анализа корпоративной виртуальной сети.

Постановка задачи. В данной работе произведена попытка классификации абонентов *VPN*-сетей на основе анализа их сетевого трафика. Поскольку основным предназначением *VPN*-технологий является обеспечение *конфиденциальности* [5] передаваемых данных, то полезная нагрузка появляется на транзитных узлах в зашифрованном виде, что делает невозможным ее анализ. В таких условиях возможно построить *систему анализа и классификации* на основе исследования служебной информации *VPN*-протоколов, без доступа к полезной нагрузке абонентов.

Методика классификации

В основу методики положен тот факт, что стандарты, относящиеся к *VPN*-сетям (*Ike*[3], *Isakmp*[4], *Pptp*[5], *Ssl* [6] и др.) оставляют для разработчиков программного обеспечения (ПО) некоторую свободу в реализации, приводящую к различиям в формируемом сетевом трафике. Эти различия могут выражаться в различной структуре, порядке следования, содержании сообщений, а также в реакции на различные события.

Другой составляющей, влияющей на видимую часть трафика, формируемого VPN-оборудованием, является его *настройка*. Настройка оборудования (программного обеспечения) могут заниматься как неподготовленные пользователи самостоятельно, так и специально предназначенные для этого сетевые администраторы. Также возможен случай, когда оборудование специально не настраивается, производится его минимальная подстройка для работы в сети, а основная масса настроек задается производителем. Если количество параметров для настройки в программной реализации протокола велико, то различия в настройках в этих трех случаях с большей вероятностью проявят себя, что также даст возможность для анализа и классификации абонентов с целью выявления нарушителей.

Отличия в реализации ПО и его настройках позволяют построить достаточно обширное множество классификационных признаков и произвести по ним классификацию абонентов. Данные признаки проявляют себя как особенности структуры, порядка, содержания передаваемых сообщений. Некоторые признаки будут иметь уникальные для каждого абонента значения (например, *IP*-адрес абонента в случае использования адреса из глобального пространства адресов), другие будут выборками из некоторого ограниченного множества значений (например, используемые абонентами алгоритмы шифрования) [1, 3, 4].

Анализировать трафик предлагается по следующим направлениям:

1. Явные идентификаторы абонентов. Например, *x*509-сертификат используемый для идентификации, должен содержать имя абонента.
2. Нестандартные расширения протоколов. Стандарты *VPN* технологий, часто закладывают в протоколы возможность расширения, чем пользуются производители оборудования.

Недостаточная детализация в описании протокола. Для различных VPN протоколов в документах, описывающих требования к реализации, присутствуют места, оставляющие для разработчика возможность импровизации. Эти приводит к различиям как структуры и наполнения пакетов, так и различному поведению ПО, что выражается в посылке/непосылке разных сообщений в ответ на одинаковый запрос или событие.

3. Различия в настройке одной и той же версии ПО. Заданные сетевым администратором настройки оборудования могут иметь видимые при анализе шифрованного трафика проявления, выражающиеся различиям в формате и содержании сообщение *VPN*-сетей.

Метод классификации абонентов VPN-сетей

Анализ и классификация *VPN*-абонентов подразумевает применение на разных этапах специального программного обеспечения, позволяющего в автоматизированном режиме анализировать сетевой трафик и составлять базу данных классификационных признаков. Работу метода можно разделить на несколько этапов:

1. *Подготовительный этап*. На подготовительном этапе производится подробный анализ всех стандартизирующих документов, относящихся к протоколам, абонентов которых предполагается классифицировать. Источником информации о возможной реализации являются:

- Документы *RFC*[7] – наиболее доверенный источник информации по протоколам *VPN*.

[3] Kaufman C., Hoffman P., Nir Y., Eronen P. The Internet Key Exchange (IKE). IETF RFC 5996, September 2010. – URL https://www.ietf.org/rfc/rfc5996.txt (дата обращения 06.12.2018).

[4] Maughan D., Schertler M., Turner J. Internet Security Association and Key Management Protocol. IETF RFC 2408, November 1998. – URL https://www.ietf.org/rfc/rfc2408.txt (дата обращения 06.12.2018).

[5] Hamzeh K., Pall G., Verthein W., Taarud J., Little W., Zorn G.. Point-to-point tunneling protocol. IETF RFC 2337, July 1999. – URL https://www.ietf.org/rfc/rfc2637.txt (дата обращения 14.01.2018).

[6] Freier A., Karlton P., Kocher P. The Secure Sockets Layer Protocol Version 3.0. IETF RFC 6101, August 2011. – URL http://www.rfc-base.org/txt/rfc-6101.txt (дата обращения 06.12.2018).

[7] *Requests for Comments* (с англ. – «требования к обсуждению») играют роль международных технико-правовых стандартов, принятых стандартизирующей международной организацией *IETF* (*Internet Engineering Task Force* — Инженерный совет Интернета) [5].

- Исходные коды прошивок оборудования и программного обеспечения (в случае их наличия).
- Исходные коды программного обеспечения для анализа сетевого трафика (например, открытого ПО *Wireshark*[8]).
- Исследование сетевого трафика, содержащего исследуемые протоколы при помощи различного программного обеспечения (например, *Wireshark*).

Для найденных признаков производится их анализ и устанавливается, возможно ли отслеживать значения этих свойств в сетевом трафике. При отсутствии такой возможности признак отбрасывается. Для всех остальных признаков выявляются условия, при которых их значения характеризуют абонентов.

2. *Настройка СПО*. После предварительного этапа производится настройка программного комплекса для анализа трафика. Все выбранные признаки получают программную реализацию и добавляются в систему анализа.
3. *Анализ сетевого трафика*. После создания программной реализации сборщиков классификационных признаков и интеграции их в систему анализа трафика производится анализ сетевого трафика. Анализ может производиться как в режиме реального времени, так и в отложенном. Результаты работы комплекс записывает в базу данных. В базе данных содержится информация по всем VPN сессиям, относящимся к выбранным для анализа протоколам. Сюда входят адреса абонентов, идентификаторы сессий, а также значения классификационных признаков, встретившихся в сессии.
4. *Предварительная обработка результатов анализа сетевого трафика*. После получения базы данных с классификационными признаками необходима ее предварительная обработка. Данный этап включает в себя отбор значимых сессий, т.е. сессий, в которых встречались классификационные признаки. Также может производиться анализ адресов абонентов на принадлежность их глобальному сегменту сети Интернет или же локальным сегментам.
5. *Анализ полученных результатов*. После отбора значимых реализаций *VPN*-протоколов производится классификация абонентов по значениям классификационных признаков.

Среди анализируемых реализаций признаков могут встречаться не стандартизированные значения, редкие значения, а также значения, противоречащие стандартам. При нахождении значений, противоречащим стандартам, стоит произвести дополнительный анализ, действительно ли является сессия, в которой появился данный признак, реализацией исследуемого протокола *VPN*.

Данная классификация позволит разделить абонентов, на тех, кто использует широко распространённое оборудование и программное обеспечение, тех, кто использует «нишевое» (теневого рынка) оборудование, а также выделить частные реализации *VPN*-протоколов.

Анализ абонентов IPsec-сетей

Классификацию абонентов будем проводить на примере протокола *IPsec*. Выбор протокола не случаен и обусловлен несколькими факторами:

- широкое распространение в сети Интернет;
- хорошая документированность;
- внутреннее «разнообразие» протокола – в нем используется много типов пакетов, сообщений, поддерживаются несколько схем выработки криптографических ключей, защиты данных. Данное свойство позволяет снимать большое количество «метрик» с трафика.

Анализ стандартов, относящихся к протоколу *IPsec* (порядка десятка документов) выявил несколько типов «вариативных» мест протокола, служащих источником классификационных признаков:

- места в протоколе, непосредственно указывающие на оборудование и используемую версию программного обеспечения. Сюда, прежде всего, относится номер версии протокола, указываемый в пакетах *Isakmp*, а также вендорные последовательности в *VendorID* сообщениях;
- разнообразные прямые идентификационные признаки самих абонентов, например, имена абонентов, их реальные *IP*-адреса (в случае, если используется туннельный режим и стороннему наблюдателю они неизвестны), сертификаты абонентов;
- косвенные признаки, позволяющие идентифицировать оборудование и версию программного обеспечения, такие как использование типов нагрузок с номерами из раздела для частного использования. Например, использование нагрузки *Cisco Fragmentation* (*Next Payload* = 243) хотя и не является стандартным, но широко распространено и позволяет с высокой долей вероятности угадать производителя оборудования;
- характеристики реализации протокола (под реализацией протокола будем понимать сеанс связи с его использованием), зависящие от настроек оборудования и программного обеспечения. Сюда входят такие признаки, как используемые сервисы защиты, алгоритмы шифрования, хэш-функции;
- точки реализации, помеченные ключевым словом *SHOULD* или *SHOULD NOT*. Хотя стандарты дают настоятельные рекомендации по поводу реализации некоторых аспектов, производители оборудования иногда их игнорируют. Например, все реализации стандарта *Ikev*1 должны поддерживать агрессивный режим обмена;

[8] https://www.wireshark.org/

- для некоторых аспектов проведения, в которых возможны несколько адекватных поведений программного обеспечения, стандарты указывают один из возможных путей реализации при помощи ключевого слова *MAY*. В таких местах производитель строго не ограничен и на основе реализованного варианта поведения можно судить о производителе оборудования или его настройках. Примером может служить поддержка дополнительных алгоритмов шифрования, не указанных как обязательных к реализации;
- места, предполагающие вариативность, но не описанные стандартом. Например, порядок атрибутов *Transform* нагрузки стандартом *Ikev*1 не ограничен, поэтому их порядок может отличаться для разных реализаций.

Классификационные признаки IPsec

Протокол *IPsec* состоит из трех основных протоколов – *Isakmp*, *ESP*[9], *AH*[10]. В свою очередь каждый из них описывается несколькими *RFC* и может иметь несколько версий. Будем изучать следующие версии протоколов и связанные с ними *RFC*:

- Для *Isakmp* – общая структура и поведение (*RFC* 2408), реализация Ike версии 1 (*RFC* 2409) и реализация Ike версии 2 (*RFC* 4306);
- Для *ESP* – *RFC* 2406 – общая структура;
- *AH* – *RFC* 4302.

В перечисленный список вариативных мест протоколов не включены места, влияющие только на внутренне состояние сторон, без каких-либо видимых снаружи проявлений.

Всего после изучения стандартов и поиска в них мест, влияющих на формируемый трафик, было выделено:

- 63 признака для протокола *Isakmp*;
- 8 признаков, относящихся к *Ike v*1 специализации *Isakmp*;
- 20 признаков, относящихся к *Ike v*2 специализации *Isakmp*;
- 4 признака в *Esp*;
- 2 признака в *AH*.

Эксперимент

Для отобранных классификационных признаков была выполнена *программная* реализация модулей системы анализа для их отбора. В качестве базы данных для записи значений признаков была выбрана *SQLite* база данных. Выбор обусловлен простотой построения запросов к базе данных для предварительного этапа анализа отобранных признаков.

В качестве эксперимента был проанализирован трафик из глобального сегмента интернета. Объем анализируемых данных составил около 60 *Гб*. Были собраны данные на ~650000 *IPsec*-соединений. Среди этих абонентов были как абоненты локальных сетей, так и имеющие адреса из глобального пространства *IP*-сетей.

В процессе предварительного анализа собранных данных были отфильтрованы признаки, вообще не встретившиеся в трафике, а также признаки, имеющие одинаковое значение для всех найденных абонентов (пустое значение и просто значения считались разными значениями).

Среди всего массива данных о сессиях были также отброшены записи, не содержащие реализаций признаков. Всего из первоначальных 97 характерных признаков после предварительной фильтрации осталось 25 признаков

Последующий анализ производился экспертным способом и позволил выявить порядка нескольких абонентов, в сетевом трафике которых были выявлены отклонения от стандартов и/или редкое оборудование. Данные абоненты можно отнести к категории «подозрительных» и на регулярной основе производить их аудит.

Заключение. Таким образом, в статье представлена методика анализа абонентов *VPN*-сетей и их классификации. Методика позволяет классифицировать абонентов виртуальных сетей без доступа к зашифрованным данным. Данная классификация предоставляет возможность поиска «странных» сессий, имеющих отклонение от стандартов, что может быть признаком *нестандартного* оборудования и/или программного обеспечения. Данной оборудование может использоваться злоумышленниками для анализа безопасности *VPN*-сервисов, являющихся достаточно чувствительной зоной в любой корпоративной сети.

Был произведен анализ применимости методики к семейству протоколов *IPsec*. Составлен список классификационных признаков абонентов *IPsec*-сетей. Приведены результаты экспериментальной проверки работоспособности методики.

Рецензент: ***Зайцев Александр Владимирович,*** *доктор технических наук, профессор, член-корреспондент РАЕН, лауреат Благодарности Президента РФ, профессор Московского авиационного института (Национального исследовательского университета), г. Москва, Россия.*

E-mail: *ug253@mail.ru*

[9] S. IP Encapsulating Security Protocol. IETF RFC 4303, December 2005. – URL https://tools.ietf. org/html/rfc4303 (дата обращения 06.12.2018).

[10] S. IP Authentication Header. IETF RFC 4302, December 2005. – URL https://tools.ietf.org/html/ rfc4302 (дата обращения 06.12.2018).

Литература

1. Бельфер Р. А., Богомолова Н. Е. Аутентификация в сетях передачи данных на базе виртуальных каналов // Труды Междунар. науч.-техн. конф. (3 – 7 декабря 2012 г.)/ МИРЭА. Ч. 6. М.: МИРЭА, 2012. С. 34 – 37.
2. Голоскоков Л. В. Теория сетевого права. М.: МПСУ, 2012. 216 с.
3. Каганов В. Ю., Королев А. К., Крылов М. Н., Машечкин И. В., Петровский М. И. Методы активной аутентификации на основе анализа динамики работы пользователей с клавиатурой // Информатика и её применение. 2013. Т. 7, вып. 3. С. 40 – 55.
4. Куликова О. В. Методы и средства аутентификации в задачах обеспечения информационной безопасности в корпоративных системах // Безопасность информационных технологий. 2010. № 3. С. 85 – 91.
5. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере: Монография. М.: РГУП, 2016. 316 с.
6. Ловцов Д. А. Информационная теория эргасистем: Тезаурус. М.: Наука, 2005. 248 с.
7. Ловцов Д. А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3 – 7.
8. Ловцов Д. А., Галахова А. Е. Защита интеллектуальной собственности в сети Интернет // Информационное право. 2011. № 4. С. 13 – 20.
9. Ловцов Д. А. Effective methods of protection of the intellectual activity results in infosphere of global telematics networks // Открытое образование. 2016. № 5. С. 85 – 88.
10. Ловцов Д. А., Ермаков И. В. Защита информации от доступа по нетрадиционным информационным каналам // НТИ РАН. Сер. 2. Информ. процессы и системы. 2006. № 9. С. 1 – 9.
11. Ловцов Д. А., Ермаков И. В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // НТИ РАН. Сер. 2. Информ. процессы и системы. 2005. № 2. С. 1 – 7.
12. Турский А., Панов С. Защита информации при взаимодействии корпоративных сетей в Internet // Экономика и производство. 1999. № 10-12. URL: http://elvis.ru/upload/iblock/7ca/7cae87c4173012693a637873a66c 19ca.pdf (дата обращения 06.12.2018).

DETECTING POTENTIALLY HAZARDOUS SUBSCRIBERS OF PRIVATE VIRTUAL NETWORKS

Pavel Golosov, *Ph.D. (Technology), Dean of the Faculty of Information Technology and Data Analysis of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Moscow, Russian Federation.*
E-mail: *golosov-pe@ranepa.ru*

Nikolai Zeliukin, *Junior Researcher at the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Moscow, Russian Federation.*
E-mail: *zelyukin-nb@universitas.ru*

Keywords: *dangerous subscribers, analysis, classification, technique, network traffic, IPsec.*

Abstract.
Purpose: *discussion of VPN networks security. This issue is raised due to wide and steady growing of VPN services marker, as well as their widespread use for protecting sensitive data. In terms of encrypting the transmitted data, traditional methods of analyzing the behavior of network users do not work, thus, other approaches are needed to ensure security and prevent attacks on private virtual networks.*
Method: *information analysis, modeling and function and logical classification.*
Result: *the technique of classification of VPN-nets users was proposed. This technique suggests some additional analysis of service traffic and is based on dependency between user's settings & equipment and service traffic, formed by this equipment. Analyzing this service information one can classify network traffic and allocate groups of VPN sessions, using non-standard equipment and/or settings and requiring more detailed audit.*
An experimental analysis was performed on test traffic record, during which some abnormal IPsec sessions were detected, formed by non-standard IPsec implementations, potentially endangering corporate network security.

References

1. Bel'fer R. A., Bogomolova N. E. Autentifikatsiia v setiakh peredachi dannykh na baze virtual'nykh kanalov, Trudy Mezhdunar. nauch.-tekhn. konf. (3-7 dekabria 2012 g.), MIREA, ch. 6, M. : MIREA, 2012, pp. 34-37.
2. Goloskokov L. V. Teoriia setevogo prava, M. : MPSU, 2012, 216 pp.
3. Kaganov V. Iu., Korolev A. K., Krylov M. N., Mashechkin I. V., Petrovskii M. I. Metody aktivnoi autentifikatsii na osnove analiza dinamiki raboty pol'zovatelei s klaviaturoi, Informatika i ee primenenie, 2013, t. 7, vyp. 3, pp. 40-55.
4. Kulikova O. V. Metody i sredstva autentifikatsii v zadachakh obespecheniia informatsionnoi bezopasnosti v korporativnykh sistemakh, Bezopasnost' informatsionnykh tekhnologii, 2010, No. 3, pp. 85-91.
5. Lovtsov D. A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere: Monografiia, M. : RGUP, 2016, 316 pp.
6. Lovtsov D. A. Informatsionnaia teoriia ergasistem: Tezaurus, M. : Nauka, 2005, 248 pp.
7. Lovtsov D. A. Obespechenie informatsionnoi bezopasnosti v rossiiskikh telematicheskikh setiakh, Informatsionnoe pravo, 2012, No. 4, pp. 3-7.
8. Lovtsov D. A., Galakhova A. E. Zashchita intellektual'noi sobstvennosti v seti Internet, Informatsionnoe pravo, 2011, No. 4, pp. 13-20.
9. Lovtsov D. A. Effective methods of protection of the intellectual activity results in infosphere of global telematics networks, Otkrytoe obrazovanie, 2016, No. 5, pp. 85-88.
10. Lovtsov D. A., Ermakov I. V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam, NTI RAN, ser. 2. Inform. protsessy i sistemy, 2006, No. 9, pp. 1-9.
11. Lovtsov D. A., Ermakov I. V. Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme, NTI RAN, ser. 2. Inform. protsessy i sistemy, 2005, No. 2, pp. 1-7.
12. Turskii A., Panov S. Zashchita informatsii pri vzaimodeistvii korporativnykh setei v Internet, Ekonomika i proizvodstvo, 1999, No. 10-12, URL: http://elvis.ru/upload/iblock/7ca/7cae87c4173012693a637873a66c 19ca.pdf (data obrashcheniia 06.12.2018).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПРАВОВЫЕ АСПЕКТЫ

*Карцхия А. А., Севостьянов В. Л.**

Ключевые слова: *право информационной безопасности, информация, киберпреступность, защита информации, правонарушения в информационной сфере, цифровые технологии, цифровые права, цифровизация права, информационно-коммуникационные технологии, стратегия развития.*

Аннотация.

Информационная безопасность является одним из основных направлений деятельности в связи с развитием информационно-коммуникационных технологий и является наиболее актуальным вопросом в сфере правового регулирования.

Применение цифровых технологий приводит к изменению характера правоприменительной практики, обеспечивающей не только защиту прав граждан, но и безопасность (физическую и сохранность персональных данных) всех участников «цифрового» оборота информации и данных в киберпространстве. Возрастание роли информационной безопасности, связано также с появлением новых видов правонарушений в информационной сфере.

Важная роль в обеспечении информационной безопасности России отводится определению приоритетных направлений и механизмов реализации государственной политики Российской Федерации в области международной информационной безопасности в целях противодействия основным угроз в этой области. В этой связи, представляется исключительно актуальным и важным инициатива по разработке концепции стратегии кибербезопасности Российской Федерации, проект которой в настоящее время предложен к обсуждению в Совете Федерации Федерального Собрания РФ.

Стремительное увеличение оборота разнообразной информации (включая коммерческую информацию, информацию о новых технологиях, информацию в составе баз данных), глобализация доступа к ней и появление новых средств ее формирования, распространения и использования актуализировали вопросы сохранности и легального использования массивов информации. Информационная безопасность выходит за рамки потребностей отдельных обладателей и выступает уже в качестве одного из направлений национальных стратегий развития.

Цель работы: *совершенствование научно-методических теоретических и правовых основ информационной безопасности.*

Метод исследования: *комплексный теоретико-сравнительный анализ действующего законодательства России и зарубежных стран в совокупности с анализом практики правоприменения.*

Результаты*: показаны особенности правового регулирования информационной безопасности в российском и зарубежном законодательстве, выявлены направления и общие тенденции правового регулирования информационной безопасности.*

DOI: 10.21681/1994-1404-2018-4-43-49

Как показывают исследования последних лет, основой современного мирового развития служат инновации, которые являются движущей силой общего роста [1]. В современных условиях для повышения капитализации и получения конкурентных преимуществ бизнеса применяются новые цифровые промышленные технологии, которые в совокупности определяются термином «Индустрия 4.0» и формируют новую, четвертую мировую технологическую революцию – «цифровую революцию» [2,3].

«Цифровая революция» выражается в создании и бурном развитии современных цифровых, информационно-коммуникационных IT-технологий, их широкое использование в различных сферах деятельности, формировании «цифровой» экономики, «цифровизации» системы права. Можно сказать, что совокупность совместно применяемых современных цифровых, IT-технологий, включающих, в частности, Интернет вещей

* ***Карцхия Александр Амиранович,*** *кандидат юридических наук, профессор РГУ нефти и газа (НИУ) им. И.М. Губкина, г. Москва, Россия.*

E-mail: arhz50@mail.ru

Севостьянов Валерий Леонидович, *кандидат технических наук, ученый секретарь некоммерческого партнерства экспертов Федерального Собрания РФ «Парламентский Центр «Наукоемкие технологии, интеллектуальная собственность», г. Москва, Россия.*

E-mail: valery.sewostyanov@yandex.ru

(Internet of Things), искусственный интеллект и современную робототехнику (AI & robotics), большие данные (Big data) и аналитику, облачные вычисления (Cloud computing), цифровое моделирование и дополненная реальность (augmented reality & simulation), аддитивное производство (additive manufacturing), создают технологический фундамент «цифровой экономики», новых социальных и общественных отношений в цифровом пространстве.

В таких условиях «цифровизации» общественных отношений, предпринимательской деятельности и государственного управления сфера права преобразуется («форматируется») под влиянием современных цифровых технологий, что находит отражение, как отмечают исследователи феномена цифровизации права [4,5,6,7,8], во множестве новых правовых явлений, связанных с субъектами и объектами правового регулирования, спецификой правоотношений в цифровой реальности, осмысления понятия и содержания цифровых прав и т.д.

Информационные и коммуникационные технологии, как указывается в Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы[1] (далее – Стратегия), стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

Российское законодательство Федеральным законом от 27.07.2006 №149-ФЗ (редакция от 31.12.2017) «Об информации, информационных технологиях и о защите информации»[2] устанавливает, что информация, являясь объектом публичных, гражданских или иных правовых отношений, может свободно использоваться и передаваться любым лицом, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения. Законом также закреплено право на доступ к информации и определены общие требования о защите информации и ответственности за правонарушения в сфере информации, информационных технологий и защиты информации, а также установлены правила ограничения доступа к информации в сети Интернет, включая распространение информации с нарушением исключительных прав на фильмы, в том числе кинофильмы, телефильмы. Предусмотрен в законе и порядок ограничения доступа в информационно-коммуникационных сетях (включая Интернет) к информации, распространяемой с нарушением закона, в которой содержаться призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях.

Информационная безопасность является одним из основных направлений деятельности в связи с развитием информационно-коммуникационных технологий. Так, в целях формирования информационного пространства знаний в п.26 Стратегии ставится ряд задач, в частности в сфере информационной безопасности, а именно:

- обеспечить создание и развитие систем нормативно-правовой, информационно-консультативной, технологической и технической помощи в обнаружении, предупреждении, предотвращении и отражении угроз информационной безопасности граждан и ликвидации последствий их проявления;
- совершенствовать механизмы ограничения доступа к информации, распространение которой в Российской Федерации запрещено федеральным законом, и ее удаления;
- совершенствовать механизмы законодательного регулирования деятельности средств массовой информации, а также средств обеспечения доступа к информации, которые по многим признакам могут быть отнесены к средствам массовой информации, но не являются таковыми (интернет-телевидение, новостные агрегаторы, социальные сети, сайты в сети «Интернет», мессенджеры);
- принять меры по эффективному использованию современных информационных платформ для распространения достоверной и качественной информации российского производства.

Кроме этого, Стратегия предусматривает, что для устойчивого функционирования информационной инфраструктуры Российской Федерации необходимо обеспечить технологическую и производственную независимость и информационную безопасность, а для защиты данных в Российской Федерации необходимо также совершенствовать нормативно-правовое регулирование в сфере обеспечения безопасной обработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение) и применения новых технологий, уровень которого должен соответствовать развитию этих технологий и интересам общества.

Обеспечение информационной безопасности как принципиальный момент соблюдении национальных интересов Российской Федерации, как отмечается в Доктрине информационной безопасности Российской Федерации[3], подразумевает, в том числе, укрепление механизмов правового регулирования отношений в области охраны интеллектуальной собственности и создание условий для соблюдения установленных федеральным законодательством на доступ к конфиденциальной информации, а также противодействие угрозам информационной безопасности.

[1] Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»//СЗ РФ, 15.05.2017, N 20, ст. 2901.

[2] Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"// СЗ РФ, 31.07.2006, N 31 (1 ч.), ст. 3448… 23.07.2018, N 30, ст. 4546.

[3] Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»// СЗ РФ, 12.12.2016, N 50, ст. 7074.

Путь цифровой трансформации также требует фундаментальной перестройки подходов частного бизнеса и государства к взаимодействию, принятию решений, стимулированию инноваций и формированию законодательной среды, где у каждого участника системы – своя значимая роль. Развитие инфраструктуры, снижение стоимости обработки, хранения и передачи данных подводят человечество к порогу нового, наиболее масштабного этапа цифровой революции. В отличие от предыдущего, который характеризовался быстрым проникновением Интернета в жизнь потребителей, современный этап отличает быстрое и расширяющееся использование в самых разнообразных областях деятельности более широкого спектра цифровых сервисов, продуктов и систем. Сегодня вполне обоснованно говорится о слиянии онлайн- и офлайн-сфер, о появлении киберфизического мира и формировании объективно нового явления, получившего название «Индустрия 4.0», которое характеризуется созданием и интеграцией принципиально новых революционных цифровых технологий.

Цифровые технологии оказывают сильное влияние на управленческие структуры, включая государственные органы управления. Они помогают сделать государственные услуги более доступными для потребителей – рядовых граждан, пользователей интернет-услуг и онлайн коммуникаций [9,10,11,12,15]. Правительства развитых стран развивают амбициозные программы по созданию и совершенствованию цифровых сервисов для различных государственных услуг. В России это программа Открытое правительство, функционирующее на основе Концепции открытости федеральных органов исполнительной власти[4].

В зарубежной практике примером может служить принятый правительством Великобритании в 2013 году и дополненный в 2016 году Свод практических правил (Technology Code of Practice)[5], который устанавливает стандарты (базовые правила) для взаимоотношений государственных структур с компаниями и физическими лицами при разработке, внедрении, а также продаже новых технологий.

Формирование киберпространства и использование в нем новых технологий на базовом принципе распределенного (децентрализованного) реестра (*blockchain tech)* привело к созданию принципиально нового правового инструментария: умные контракты, электронно-цифровые подписи, базовые технологические стандарты и правила и др. Новые цифровые технологии используются при ведении официальных государственных реестров, объектов недвижимости или реестров нормативных правовых актов, а также в таких сфера правоприменения как сбор налогов, в сфере учета и выдаче документов, оказания государственных услуг. Цифровые технологии получили широкое применение в промышленном интернете, в управлении сложными технологическими процессами и структурами.

Применение цифровых технологий, на наш взгляд, может привести к изменению характера правоприменительной практики, обеспечивающей не только защиту прав граждан, но и безопасность (физическую и сохранность персональных данных) всех участников «цифрового» оборота информации, данных в киберпространстве.

Информационная безопасность является наиболее актуальным вопросом в сфере правового регулирования. В докладе Европола за 2017 год «Оценка угроз организованной преступности в Интернете» [12] выделены особо опасные сферы киберпреступлений, к которым, в частности, относятся: разработка вредоносных компьютерных программ и средств (разработка «программ-вымогателей», банковские трояны и другие вредоносные программы (malware), организация DDoS-атак и ботов); кибератаки на критическую инфраструктуру экономики и государства (электростанции, транспортные узлы, объекты промышленности, объекты в системе Интернет-вещей и др.); интернет-контент, касающийся сексуальной эксплуатации детей; террористическая активность в Интернете; мошенничество с банковскими картами и безналичными платежами; интернет-торговля оружием, наркотиками иными запрещенными товарами, незаконная торговля людьми); он-лайн оборот контрафактной продукции и использование известных товарных марок (брэндов) в нелегальных интернет-приложениях; мошенничество и кражи в отношении криптовалют, а также использование криптовалют (Bitcoin, Monero, Ethereum, Zcash) в киберпреступлениях и «отмывании» незаконных денежных средств; преступное шифрование данных; использование социальной инженерии в кибермошенничестве; трансграничный характер киберпреступности.

Как отмечается в докладе Европейского агентства сетевой и информационной безопасности (European Union Agency For Network And Information Security-ENISA) за 2018 год [13] угрозы и риски, связанные с устройствами, системами и услугами Интернета вещей, многообразны и быстро развиваются. Интернет вещей оказывает все большее влияние на безопасность и частную жизнь граждан, а сами виды угроз в отношении Интернета вещей чрезвычайно многообразны.

Появление и использования новых цифровых активов (криптовалют, токенов и др.), повышение доступности цифровых финансовых услуг создают новые риски для «отмывания» доходов преступной и террористической деятельности, а также финансирование такой незаконной деятельности. Поэтому Межправительственная организация «Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ)» призывает к скоординированным усилиям всех стран, направленным на предотвращение использования виртуальных активов в преступных и террористических целях [14].

Возрастание роли информационной безопасности, связано и с появлением новых видов правонарушений

[4] [Электронный ресурс]URL: www.open.gov.ru

[5] Technology Code of Practice,UK (2016). URL: http://www.gov.uk

в информационной сфере. В частности, в интернет-банкинге – кража денежных средств с банковских счетов с использование программных средств-эксплойтов (компьютерные программы, использующие уязвимости программного обеспечения для проведения атак на вычислительные системы и электронные устройства, например, смартфоны и др.). Киберсквоттинг (захват доменных имен), т.е. регистрация доменного имени, частично сходного с уже зарегистрированным, или тождественного по написанию с иным средством индивидуализации (товарным знакам). Брэндсквотинг – регистрация на определенной территории товарного знака, ранее не зарегистрированного, с целью продажи его заинтересованным лицам.

Манипулирование рынком также является негативным явлением при использовании информации в экономической деятельности. В связи с этим в российском законодательстве в ст.5 Федеральный закон от 27.07.2010 N 224-ФЗ (редакция от 03.07.2016) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», а также в статье 185.3 УК РФ манипулирование рынком признается преступлением, которое выражается в умышленном распространении через средства массовой информации, в том числе через электронные, информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц (включая сеть «Интернет») заведомо ложных сведений, в результате которого цена, спрос, предложение или объем торгов финансовым инструментом, валютой или товаром отклонились от уровня или поддерживались на уровне, существенно отличающемся от того уровня, который сформировался бы без распространения таких сведений.

К самостоятельным составам преступлений в сфере информационной безопасности можно отнести мошенничество с платежными и кредитными картами (статья 159.3 УК РФ) и мошенничество в сфере компьютерной информации (статья 159.6 УК РФ). Уголовный кодекс РФ (ст.272-274 УК РФ) предусматривает уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации (не только ЭВМ или их сети), за создание, распространение или использование вредоносных компьютерных программ, а также за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации (информационно-телекоммуникационных сетей). Мошенничеством в сфере компьютерной информации признается и совершение посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, а также целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

В соответствии со ст. 15.2 и 15.3 ст.15.3 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» предусмотрена ответственность провайдеров, информационных посредников, а также администраторов доменного имени или физического лица, фактически использующего доменное имя в виде ограничения доступа к информационным ресурсам за нарушение авторских и смежных прав в информационно-телекоммуникационных сетях, включая сеть «Интернет» в случае распространения без разрешения правообладателя или иного законного основания, а также нарушения порядка ограничения доступа к информации, содержащей призывы к массовым беспорядкам.

Вместе с тем, информационная безопасность – это еще и безопасность персональных данных в цифровой экосистеме и массивах больших данных, базах персонифицированного учета и рассылки сообщений, сохранение тайны личной переписки в социальных сетях и мессенджерах. В соответствии со ст. 15.8 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» владельцам «анонимайзеров» и VPN-сервисов запрещается предоставлять возможность использования этих сервисов на территории Российской Федерации для получения доступа к заблокированным в установленном законом порядке информационным ресурсам.

Сохранность персональных данных и защита частной жизни – один из актуальных аспектов информационной безопасности в свете появления новых серьезных киберугроз. Особый правовой режим установлен Федеральным законом от 27.07.2006 N 152-ФЗ (редакция от 31.12.2017) «О персональных данных»[6] для такой специфической информации как персональные данные. В частности, в законе предусматривается порядок получения и обработки персональных данных и биометрических данных физических лиц.

Во многих странах в настоящее время уже имеется действующее законодательство, связанное с обеспечением информационной безопасности в информационно-коммуникационных сетях, применяются собственные стратегии информационной безопасности.

Проблемы информационной безопасности выходят на первый план и в национальных стратегиях других стран. В частности, в феврале 2013 года Еврокомиссия утвердила Стратегию кибербезопасности в Европе (EU Cyber Security Strategy). Стратегия устанавливает общие минимальные требования к сетевой и информа-

[6] Собрание законодательства РФ, 31.07.2006, N 31 (1 ч.), ст. 3451.

ционной безопасности между государствами-членами; определяет согласованную линию на профилактику, обнаружение и смягчения последствий и механизмов киберугроз, а также предусматривает повышение уровня готовности и участия в общей стратегии частного бизнеса.

По недавним оценкам органов государственного контроля Великобритании затраты на борьбу с киберпреступностью обходятся стране ежегодно в сумме от 18 до 27 млрд. фунтов стерлингов. Такая ситуация в информационно-коммуникационной среде вынуждает правительства многих стран принимать активные контрмеры по защите государственных и частных интересов в киберпространстве, включая разработку нового законодательства в этой сфере.

Аналогичные законы по защите информации существуют в США, к примеру Digital Millennium Copyright Act (1998) – Закон об авторском праве в цифровую эпоху. Примечательно, что законодатели США в современной практике законотворчества расширяют принцип экстерриториальности действия права США практически по всему миру. В частности, в марте 2018 г. принят закон о правомерном использовании данных за рубежом (Clarifying Lawful Overseas Use of Data Act, «CLOUD Act» 2018)[7] , который позволяет правоохранительным органам США получать в упрощенном порядке доступ к информации граждан, хранящейся на серверах за границей, на территории другой страны, если на это был выдан ордер американским судом. Явное нарушение права на частную жизнь, тем не менее, получил одобрение и поддержку у таких гигантов интернет-индустрии, как Google, Apple, Microsoft,Facebook and Oath [16].

В мае 2018 г. во всех странах Евросоюза стал обязательным к исполнению новый правовой акт ЕС о защите персональных данных (General Data Protection Regulation, GDPR)[8].

Стремительное увеличение оборота разнообразной информации (включая коммерческую информацию, информацию о новых технологиях, информацию в составе баз данных), глобализация доступа к ней и появление новых средств ее формирования, распространения и использования актуализировали вопросы сохранности и легального использования массивов информации. Информационная безопасность выходит за рамки потребностей отдельных обладателей и выступает уже в качестве одного из направлений национальных стратегий развития.

В этой связи, представляется исключительно актуальным и важным инициатива по разработке концепции стратегии кибербезопасности Российской Федерации, проект которой в настоящее время предложен к обсуждению в Совете Федерации Федерального Собрания РФ.

Запущенный процесс «цифровизации» продолжает бурно развиваться, стимулируя новые изменения и технологические новации, которые, в свою очередь, ставят непростые проблемы правового характера в цифровой экосистеме. Особую актуальность приобретают вопросы по защите прав интеллектуальной собственности, обеспечением публичных (национальных) и частных (коммерческих) интересов правообладателей. На первый план выходит задача создания эффективной защиты интеллектуальной собственности в киберпространстве и обеспечение сохранности государственной, служебной и коммерческой тайны в глобальной информационно-коммуникационной среде.

Решением этой задачи может стать создание более эффективной модели Интернета, которая могла гарантировать суверенитет, безопасность и соблюдение принципов международного общежития в сочетании с соблюдением норм о неприкосновенности частной жизни, непосредственно связано с эффективностью охраны и защиты интеллектуальной собственности в киберпространстве [17]. В частности, целесообразно сосредоточить нормы о защите прав в киберпространстве в одном законе, например, в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Важная роль в обеспечении информационной безопасности России отводится определению приоритетных направлений и механизмов реализации государственной политики Российской Федерации в области международной информационной безопасности в целях противодействия основным угроз в этой области. Международное сотрудничество в сфере кибербезопасности сейчас развивается на двусторонней основе между Россией и другими государствами. Поэтому особенно важно результативно проводить работу по принятию международной конвенции по кибербезопасности в рамках ООН. В этом направлении в ноябре 2018 г. Российская Федерация добилась поддержки Комитета Генеральной Ассамблеи ООН, который одобрил российский проект резолюции по разработке общеобязательных международных норм безопасности в киберпространстве.

Рецензент: ***Полякова Татьяна Анатольевна****, доктор юридических наук, профессор, Главный научный сотрудник, заведующая сектором информационного права ИГП РАН, г. Москва, Россия.*

E-mail: *polyakova_ta@mail.ru*

[7] URL: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/congress-enacts-the-clarifying-lawful-overseas-use-of-data-cloud-act-reshaping-us-law-governing-crossborder-access-to-data/CD82F8379A94BCF3B48C532ABD67E23B.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Литература

1. Global Innovation Index 2017: Innovation Feeding the World. Cornell University, INSEAD, the World Intellectual Property Organization (WIPO). Geneva, 2017. URL: www.wipo.int/edocs/.
2. Digitalization for All Future-Oriented Policies for a Globally Connected World.G20, 2017. URL: https://www.b20germany.org/fileadmin/ user_upload/ documents/B20/ B20_ Digitalization_Policy_ Paper_2017.pdf; OECD Digital Economy Outlook 2017. OECD, 2017. URL: https://doi.org/10.1787/ cc76d818/.
3. Networks of «Things». NIST Special Publication 800-183. U.S. Department of Commerce, July 2016. URL: https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-183.pdf
4. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права, N 1, 2018. С. 85-102.
5. Понкин И.В., Редькина А.И. Искусственный интеллект и право интеллектуальной собственности // Интеллектуальное право. Авторское право и смежные права. № 2, 2018. С. 35-44.
6. Новоселова Л.А. «Токенизация» объектов гражданского права // Хозяйство и право, 2017, № 12. С 29–44;
7. Карцхия А.А. Цифровые технологии – правовой аспект // ИС. Промышленная собственность, № 10, 2018. С.17-26.
8. Добрынина Т.В., Севостьянов В.Л. Гражданское общество активизирует мониторинг правоприменительной практики в сфере коммерциализации интеллектуальной собственности. / Сборник научных, методических и аналитических материалов XI Международного форума «Интеллектуальная собственность – XXI век». Издание Торгово-промышленной палаты РФ, 2018 г., с.44-48.
9. Карцхия А.А. «Облачные» технологии: российское и зарубежное законодательство и практика правоприменения // Мониторинг правоприменения. № 2, 2018. С.36-41.
10. Карцхия А.А. Цифровизация в праве и правоприменении // Мониторинг правоприменения. № 1, 2018. С.36-40.
11. Bliznets, I., Kartskhiya, A., & Smirnov, M. (2018). Technology Transfer in Digital Era: Legal Environment. Journal of History Culture and Art Research, 7(1), 354-363. DOI: http://dx.doi.org/10.7596/taksad.v7i1.1466.
12. Internet organized Crime Threat Assessment (IOCTA) 2017. European Union Agency for Law Enforcement Cooperation (Europol), 2017. pp. 10—12. URL: www.europol. europa.eu .
13. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. European Union Agency For Network And Information Security, November 2017. www.enisa.europa.eu. P.11-12.
14. FATF (2012-2018). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF 2012-2018, Paris, France, URL: www.fatf-afi.org .
15. Карцхия А.А. Цифровая революция: новые технологии и новая реальность // Правовая информатика. 2017. №1. С.13-19.
16. President signs overseas data access bill into law. URL: www.engadget.com/ 2018/03/24/cloud-act-law .

INFORMATION SECURITY: LEGAL ASPECTS

Aleksandr Kartskhiia, *Ph.D. (Law), Professor at Gubkin Russian State University of Oil and Gas, Moscow, Russian Federation.*
E-mail: *arhz50@mail.ru*

Valerii Sevost'ianov, *Ph.D. (Technology), Academic Secretary of the Not-For-Profit Partnership of Experts of the Federal Assembly of the Russian Federation "Parliamentary Centre 'Science-Intensive Technologies, Intellectual Property'", Moscow, Russian Federation.*
E-mail: *valery.sewostyanov@yandex.ru*

Keywords: *right to information security, information, cybercrime, information protection, offences in the information sphere, digital technologies, digital rights, digitalisation of law, information and communication technologies, development strategy.*

Abstract.

Information security is one of the main lines of activity related to the development of information and communication technologies and the most topical issue in the sphere of legal regulation.

Using digital technologies leads to changes in the nature of law enforcement practice ensuring not only the protection of citizens' rights but also the security (physical security as well as integrity of personal data) of all participants of the 'digital' circulation of information and data in the cyberspace. The growth of the role of information security is also related to the

appearance of new types of offences in the information sphere.

An important role in ensuring Russia's information security goes to identifiying of priority lines and mechanisms of implementation of the government policy of the Russian Federation in the field of international information security with a view to combating the main threats in this field. In view of this, the initiative for developing a conception of cyber-security of the Russian Federation whose draft is currently submitted for discussion in the Federation Council of the Federal Assembly of the Russian Federation is deemed extremely topical and important.

Rapid growth of circulation of various kinds of information (including commercial information, information on new technologies, information contained in databases), globalisation of access to it and appearance of new means for its forming, distribution and use, made the issues of integrity and legal use of information files even more topical. Information security goes beyond the scope of the needs of individual owners and stands in as one of the lines of the national development strategies.

Purpose of the paper: improving the research and methodological, theoretical and legal foundations of information security.

Method of study: complex theoretical and comparative analysis of the current laws of the Russia and foreign countries combined with an analysis of law enforcement practice.

Results obtained: features of legal regulation of information security in Russian and foreign laws are shown, general lines and trends of legal regulation of information security are identified.

References

1. Global Innovation Index 2017: Innovation Feeding the World. Cornell University, INSEAD, the World Intellectual Property Organization (WIPO). Geneva, 2017. URL: www.wipo.int/edocs/.
2. Digitalization for All Future-Oriented Policies for a Globally Connected World.G20, 2017. URL: https://www.b20germany.org/fileadmin/user_upload/ documents/B20/ B20_ Digitalization_Policy_Paper_2017.pdf; OECD Digital Economy Outlook 2017. OECD, 2017. URL: https://doi.org/10.1787/ cc76d818/.
3. Networks of "Things". NIST Special Publication 800-183. U.S. Department of Commerce, July 2016. URL: https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-183.pdf
4. Khabrieva T.Ia., Chernogor N.N. Pravo v usloviiakh tsifrovoi real'nosti, Zhurnal rossiiskogo prava, No. 1, 2018, pp. 85-102.
5. Ponkin I.V., Red'kina A.I. Iskusstvennyi intellekt i pravo intellektual'noi sobstvennosti, Intellektual'noe pravo. Avtorskoe pravo i smezhnye prava, No. 2, 2018, pp. 35-44.
6. Novoselova L.A. "Tokenizatsiia" ob"ektov grazhdanskogo prava, Khoziaistvo i pravo, 2017, No. 12, pp. 29-44.
7. Kartskhiia A.A. Tsifrovye tekhnologii -- pravovoi aspekt, IS. Promyshlennaia sobstvennost', No. 10, 2018, pp. 17-26.
8. Dobrynina T.V., Sevost'ianov V.L. Grazhdanskoe obshchestvo aktiviziruet monitoring pravoprimenitel'noi praktiki v sfere kommertsializatsii intellektual'noi sobstvennosti, Sbornik nauchnykh, metodicheskikh i analiticheskikh materialov XI Mezhdunarodnogo foruma "Intellektual'naia sobstvennost' -- XXI vek". Izdanie Torgovo-promyshlennoi palaty RF, 2018 g., pp. 44-48.
9. Kartskhiia A.A. "Oblachnye" tekhnologii: rossiiskoe i zarubezhnoe zakonodatel'stvo i praktika pravoprimeneniia, Monitoring pravoprimeneniia, No. 2, 2018, pp. 36-41.
10. 10. Kartskhiia A.A. Tsifrovizatsiia v prave i pravoprimenenii, Monitoring pravoprimeneniia, No. 1, 2018, pp. 36-40.
11. Bliznets, I., Kartskhiya, A., & Smirnov, M. (2018). Technology Transfer in Digital Era: Legal Environment. Journal of History Culture and Art Research, 7(1), 354-363. DOI: http://dx.doi.org/10.7596/taksad.v7i1.1466.
12. Internet organized Crime Threat Assessment (IOCTA) 2017. European Union Agency for Law Enforcement Cooperation (Europol), 2017, pp. 10-12. URL: www.europol.europa.eu .
13. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. European Union Agency For Network And Information Security, November 2017. www.enisa.europa.eu. P. 11-12.
14. FATF (2012-2018). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF 2012-2018, Paris, France, URL: www.fatf-afi.org .
15. Kartskhiia A.A. Tsifrovaia revoliutsiia: novye tekhnologii i novaia real'nost', Pravovaia informatika, 2017, No. 1, pp. 13-19.
16. President signs overseas data access bill into law. URL: www.engadget.com/ 2018/03/24/cloud-act-law .

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ В ПРАВОВОЙ СФЕРЕ

Федосеев С. В. *

Ключевые слова*: цифровая трансформация, правовая информация, информационно-телекоммуникационные технологии, наука о данных, категории данных, экосистема больших данных, процесс Data science, области применения Data science.*

Аннотация.

Цель: *обоснование методических подходов к решению задач эффективной обработки больших объемов данных в правовой сфере.*

Метод*: логическое моделирование правовых отношений и информационных связей в правовой сфере и системный анализ взаимосвязи предметной области правовой сферы и основных объектов и методов технологии больших данных.*

Результаты*: обоснована необходимость цифровой трансформации и перехода на новые информационные технологии в правовой сфере, создания и развития инфраструктуры обработки больших данных; выполнен анализ предметной области Data science и больших данных, категорий данных в Data science; рассмотрена экосистема больших данных и data science; исследованы этапы процесса Data science; определены области применения Data science и больших данных.*

DOI: 10.21681/1994-1404-2018-4-50-58

В правовой сфере общественно-производственной деятельности важное значение имеет использование *статистической* информации, которая является результатом логической обработки очень больших динамически изменяющихся массивов разнообразных статистических данных и позволяет принимать обоснованные управленческие решения (правовые предписания), а также выявлять и анализировать тенденции развития систем правового регулирования и позитивного права [4, 6, 10, 16]. В связи с этим осуществляется, в частности, целенаправленная системная модернизация и совершенствование электронной обработки правовой и судебной статистики в крупномасштабных системах информационно-аналитической поддержки правовой сферы (типа ГАС РФ «Правосудие») [14].

Особое значение использование статистической информации имеет в сфере правотворчества, так как оно способствует обеспечению своевременности разработки и принятия соответствующих нормативных правовых актов, а также их совершенствованию. Общий объём и сложность обрабатываемой правовой и судебной информации стремительно растут, поэтому становится очевидной невозможность обеспечения требуемых качества и скорости обработки данных с использованием традиционных информационных технологий.

Необходимость «цифровой трансформации» [12] деятельности государственных органов и перехода на новые (нетрадиционные, новаторские) информационные технологии обусловлена положениями ряда нормативных правовых актов и документов (*Концепция Федеральной целевой программы «Развитие судебной системы Российской Федерации на* 2013 – 2020 *годы»; Концепция цифровой трансформации органов и организаций прокуратуры Российской Федерации до* 2025 *года; программа «Цифровая экономика Российской Федерации до* 2024 *года»; Стратегия развития информационного общества в Российской Федерации до* 2024 *года; Стратегия научно-технологического развития Российской Федерации; Прогноз научно-технологического развития Российской Федерации на период до* 2030 *года* и др.). В нормативных правовых актах и документах значительное внимание уделяется применению *новых* информационно-телекоммуникационных технологий в различных областях деятельности, и, в частности, созданию и развитию инфраструктуры обработки больших данных. Большие данные (*big data*) являются

* ***Федосеев Сергей Витальевич****, кандидат технических наук, доцент, доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Россия.*

E-mail: fedsergvit@mail.ru

также одним из важнейших компонентов глобальной стратегии «Индустрия 4.0»[1].

Технологии больших данных применяются в правовой сфере еще недостаточно широко, поэтому представляется целесообразным выявить прагматические характеристики технологий и компонентов экосистемы больших данных, а также определить предназначение соответствующих различных групп инструментальных средств [10] с целью широкого эффективного их внедрения.

1. Предметная область *Data science* и больших данных

Под обобщающим термином «большие данные» (*big data*) принято понимать любые наборы данных, достаточно большие и сложные для того, чтобы их можно было обработать традиционными средствами переработки данных (например, реляционными системами управления базами данных – РСУБД). Более конкретно можно определить, что термин «большие данные» применяется для обозначения структурированных и неструктурированных данных очень больших объёмов и значительного многообразия, эффективно обрабатываемых горизонтально масштабируемыми программными инструментами [10].

Справедливо признается, что широко распространённые РСУБД являются универсальным инструментом. Однако в случае обработки больших данных РСУБД в большинстве случаев уже не удовлетворяют новым требованиям.

Характеристики больших данных обычно обозначают «четырьмя *V*» [5]:

- объем (*Volume*) – величина физического объёма данных в наборе;
- многообразие (*Variety*) – возможность одновременной обработки различных типов структурированных и частично структурированных данных;
- скорость *(Velocity)* – скорость генерирования (прироста) данных, скорость обработки и получения новых результатов;
- достоверность (*Veracity) – характеристика, определяющая* насколько точны данные.

Эти четыре свойства отличают большие данные от данных, встречающихся в традиционных средствах управления данными. Соответственно, привносимые ими изменения проявляются почти во всех аспектах: сборе данных, хранении и обслуживании данных, поиске, обмене, передаче и визуализации. Кроме того, большие данные требуют применения специализированных средств извлечения информации.

В настоящее время принято различать *data science* и большие данные, при том, что обе эти дисциплины развиваются на базе статистики и традиционных подходов в управлении данными [15].

Data science (наука о данных) – раздел информатики [13], изучающий проблемы анализа, обработки и представления данных в цифровой форме. *Data science* объединяет методы по обработке данных в условиях больших объёмов и высокого уровня параллелизма, статистические методы [9 – 11], методы интеллектуального анализа данных и приложения искусственного интеллекта для работы с данными, а также методы проектирования и разработки баз данных [2].

Следует заметить, что наряду с методами статистической обработки данных [1, 9 – 11], в *data science* широко используются методы, заимствованные из *Computer science* (организация вычислений и построение алгоритмов), а также методы машинного обучения [3, 18].

Категории данных в Data science. В *Data science* и области больших данных используется различные типы данных, для каждого из которых требуются свои инструменты и методы. Основные категории данных: структурированные; неструктурированные; на естественном языке; машинные; графовые; аудио, видео и графика; потоковые.

Структурированные данные зависят от модели данных и хранятся в фиксированных полях внутри записи. Соответственно, структурированные данные удобно хранить в таблицах, в базах данных или файлах *Excel*.

Язык структурированных запросов *SQL (Structured Query Language)* является основным средством управления и обращения с запросами к данным, хранящимся в базах данных. Иногда встречаются структурированные данные, которые достаточно трудно сохранить в традиционной реляционной базе данных (один из примеров – иерархические данные).

Неструктурированные данные трудно поставить в соответствие какой-либо конкретной модели данных, потому что их содержимое зависит от контекста и поэтому имеет переменный характер.

Данные на естественном языке составляют особую разновидность неструктурированных данных. Обработка таких данных достаточно сложна, потому что она требует знания, как лингвистики, так и специальных методов *data science*. Достижения в области обработки данных на естественном языке связаны с успехами в распознавании сущностей, в распознавании тематических областей, в анализе текстов. Однако, модели, адаптированные для одной предметной области, не могут быть эффективно применены в других областях. Задача распознавания смысла произвольного фрагмента текста по-прежнему является трудноразрешимой, даже при использовании самых современных методов.

К *машинным данным* относится информация, автоматически генерируемая компьютером, процессом, приложением или устройством без вмешательства человека. Машинные данные становятся одним из основных источников информации. Это связано, прежде

[1] Ожидаемая четвёртая промышленная революция – массовое внедрение киберфизических систем в производство.

всего, с развитием промышленного Интернета (*Интернета вещей*[2]).

Анализ машинных данных вследствие очень больших объемов и скоростей в значительной степени зависит от инструментов, обладающих высокой масштабируемостью.

Примеры машинных данных: журналы вебсерверов, записи детализации звонков, журналы сетевых событий и телеметрии. Машинные данные хорошо укладываются в структуру классической базы данных.

Термин *графовые данные* связан с понятием графа из математической теории графов, при этом под графом понимается математическая структура для моделирования попарных отношений между объектами. В графовых или сетевых данных особое внимание уделяется связям или смежности объектов. Графовые структуры данных используют узлы, ребра и свойства для представления и хранения графических данных. Графовые данные естественным образом подходят для представления социальных сетей, а их структура позволяет вычислять такие специфические метрики, как влияние участников и кратчайший путь между двумя людьми. Одной из типовых задач для графовых данных является анализ нескольких перекрывающихся графов, построенных на одних и тех же узлах.

Для хранения графовых данных используются *графовые базы данных*, а для построения запросов к ним специализированные языки запросов. Решение задач с графовыми данными имеет специфические проблемы, связанных с их высокой вычислительной сложностью.

Аудио, видео и графика – категория данных, предъявляющая высокие требования к системам хранения данных по объему размещаемой информации и к эффективности применяемых алгоритмов обработки данных.

Потоковые данные формально не являются отдельной категорией данных и могут быть отнесены к любой из перечисленных выше категорий. Однако их отличительная черта состоит в том, что эти данные поступают в систему при возникновении некоторых событий или несут в себе информацию о некотором процессе в реальном масштабе времени.

Экосистема больших данных и *data science* может быть разделена на отдельные компоненты по технологиям с похожими целями и функциональностью.

2. Экосистема больших данных и *data science*

В настоящее время существует много различных технологий и инструментальных средств, используемых для обработки больших данных [2, 7, 10, 15]. Именно эти технологии и инструментальные средства, находящиеся в состоянии постоянного совершенствования и обновления, и составляют экосистему[3] больших данных и *data science* (рис. 1.).

Проведем анализ компонентов экосистемы больших данных и различных технологий, рассмотрим различные группы инструментальных средств и определим их предназначение.

Распределенные файловые системы. Распределенная файловая система похожа на обычную файловую систему, но в отличие от последней она функционирует на нескольких серверах сразу. Используя эти системы, можно выполнять почти все те же действия, что и в обычных файловых системах.

В основе любой файловой системы лежат такие действия, как *запись*, *хранение*, *чтение* и *удаление* данных, а также реализация средств безопасности файлов. Распределенные файловые системы имеют такую же функциональность и обладают при этом рядом важных преимуществ:

- они способны хранить файлы, размер которых превышает размер диска отдельного компьютера;
- файлы автоматически реплицируются на нескольких серверах для создания избыточности или выполнения параллельных операций, при этом все сложности технической реализации этих действий незаметны для пользователя;
- распределенная файловая система легко масштабируется: пользователь не ограничен объемом памяти или дискового пространства одного сервера.

Важной характеристикой файловой системы является возможность ее *масштабирования*. Ранее масштабирование осуществлялось переводом всех систем на сервер с бо́льшим объёмом памяти и дискового пространства и более быстрым процессором (*вертикальное* масштабирование). В настоящее время в распределенных системах появляется возможность дополнительного использования соседнего по уровню сервера с унифицированными характеристиками (*горизонтальное* масштабирование). Благодаря такой возможности потенциал масштабирования становится практически безграничным.

Наиболее популярной распределенной файловой системой является *Hadoop File System (HDFS)*. Она представляет собой реализацию *Google File System* с открытым кодом. Эта система чаше всего применяется на практике. Существуют также и другие распределенные файловые системы: *Red Hat Cluster File System*, *Ceph File System*, *Tachyon File System* и др.

Технологии распределенного программирования. После того, как данные сохранены в распределенной файловой системе, следует процесс их использования. Важнейшим аспектом работы с распределенной файловой системой является то, что более рациональным является не перемещение данных к программе, а наоборот – перемещение программы к данным.

[2] Программа «Цифровая экономика Российской Федерации», утв. Распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р – URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf, http://government.ru/docs/28653/ (Дата обращения 19.11.2018 г.)

[3] Там же.

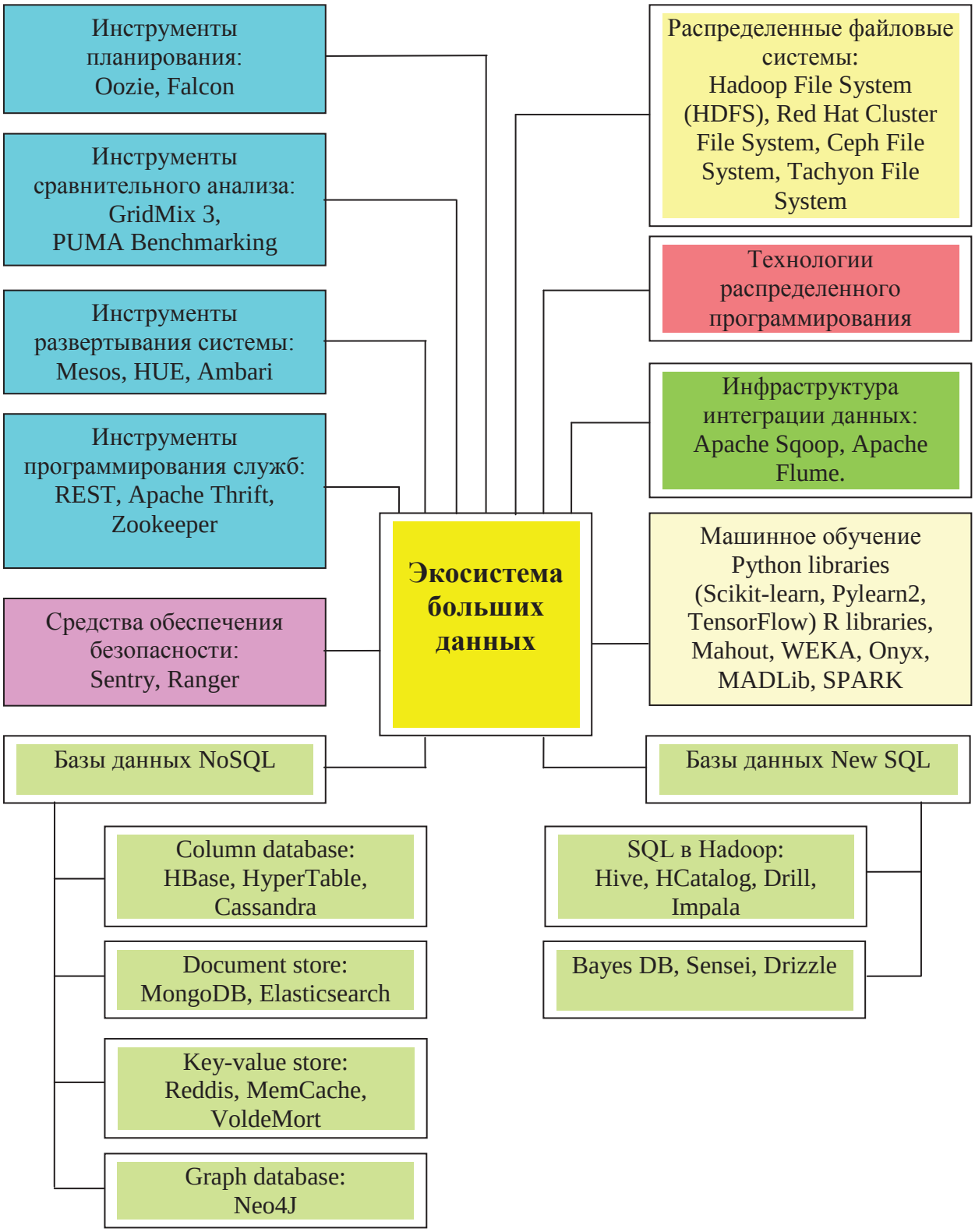

Рис. 1. Экосистема больших данных и data science

Дополнительными технологическими сложностями, присущими распределенному программированию, являются: перезапуск сбойных заданий, синхронизация субпроцессов, учет консистентности данных. В большинстве случаев эти сложности успешно преодолеваются с помощью существующих инструментальных средств, которые значительно упрощают работу с распределенными данными.

Инфраструктура интеграции данных. После создания распределенной файловой системы возникает необходимость добавления данных или перемещения данных из одного источника в другой. В подобных случаях используются такие инфраструктуры интеграции данных, как *Apache Sqoop* и *Apache Flume*.

Инфраструктуры машинного обучения. Инфраструктуры машинного обучения находят свое применение при анализе данных и извлечении из них скрытой информации. На этой стадии используются методы не только из области машинного обучения, но также из статистики и прикладной математики.

В современных условиях необходимо анализировать огромные объемы данных. Для решения этих задач применяются специализированные библиотеки и процедуры. Так, например, для высокоуровневого языка программирования *Python* [3] наиболее популярной библиотекой машинного обучения является *Scikit-learn*. Используются также и другие библиотеки: *Pylearn2* и *TensorFlow* – библиотека *Python* для машинного обучения, предоставленная компанией *Google*.

Базы данных. Для хранения огромных объемов данных требуется программное обеспечение, специализирующееся на управлении этими данными и формировании запросов к ним. Традиционно в этой области использовались реляционные базы данных – такие, как *Oracle SQL, MySQL. Sybase IQ* и др. [19]. Во многих случаях эти базы данных продолжают оставаться предпочтительным решением. Однако у традиционных баз данных существуют *недостатки*, которые затрудняют их применение в системах обработки больших данных и усложняют их масштабирование: их память и вычислительный ресурс не масштабируются за пределы одного узла; в традиционных базах данных отсутствуют средства обработки потоковых, графовых и неструктурированных категорий данных.

Попытки ликвидировать эти недостатки привели к появлению новых типов баз данных, объединенных в категорию баз данных *NoSQL*. Следует заметить, что «*No*» в названии этой категории означает «не только». Базы данных *NoSQL* обладают большей функциональностью, лишены недостатков традиционных баз данных и обеспечивают возможность почти неограниченного масштабирования данных.

Существующие разновидности баз данных можно разделить на следующие типы:

- *столбцовые базы данных (column database)* – данные организуются в столбцы, что позволяет алгоритмам существенно повышать скорость обработки запросов; табличные структуры продолжают играть важную роль в обработке данных;
- *хранилища документов (document store)* – хранилища документов, не использующие таблицы, но хранящие полную информацию о документе; их особенностью является чрезвычайно гибкая схема данных;
- *хранилища «ключ-данные» (key-value store)* – данные не хранятся в таблицах; каждому отдельному значению ставится в соответствие ключ, а не «координаты» этого значения в таблице; такое решение обеспечивает хорошее масштабирование, но затрудняет разработку базы данных;

SQL в Hadoop – пакетные запросы в *Hadoop* пишутся на *SQL*-подобном языке, во внутренней реализации которого используется инфраструктура отображения-свертки (*Map-reduce*);

обновленный SQL (New SQL) – этот тип сочетает масштабируемость баз данных *NoSQL* с преимуществами реляционных баз данных; используется интерфейс *SQL* и реляционная модель данных.

Графовые базы данных (graph database). Табличный формат представления данных является оптимальным не для всех задач. Некоторые задачи могут быть более естественно представлены с помощью графовых моделей, а используемые ими данные – размещены в графовых базах данных.

Инструменты планирования. Инструменты планирования упрощают автоматизацию повторяющихся операций и запуск заданий по событиям (например, при появлении нового файла в папке). Эти инструментальные средства имеют аналоги в традиционных программах, но разрабатываются специально для больших данных. Например, такие инструменты могут запускать задачу *Map-reduce* при появлении нового набора данных в каталоге.

Инструменты сравнительного анализа. Этот класс инструментов разработан для оптимизации установки больших данных за счет предоставления стандартизированных *профилей*. Профили строятся на основании представительного множества операций с большими данными. С использованием этих инструментов решаются задачи сравнительного анализа и оптимизации инфраструктуры больших данных.

Инструменты развертывания системы. Подготовка инфраструктуры больших данных – достаточно сложная задача. Инструменты развертывания системы применяются при развертывании новых приложений в кластерах больших данных. Они в значительной степени автоматизируют установку и настройку компонентов больших данных.

Инструменты программирования служб. Инструменты программирования служб обеспечивают доступ к приложениям и моделям больших данных, как к сервису. Примером такого рода являются *REST*-службы (*Representational State Transfer*). Эти службы используются, например, для передачи данных веб-сайтам.

Средства обеспечения безопасности. В процессе обработки больших данных необходимо обеспечить точное *управление доступом* к используемым данным, причем целесообразно сделать это на уровне, общем для всех приложений, а не на уровне каждого отдельного приложения. Средства безопасности больших данных позволяют создать централизованную и высокоточную систему управления доступом к данным.

3. Процесс *Data science*

Наиболее часто для описания процесса *data science* используется *структурный* подход [8], который при реализации проекта позволяет получить требуемый результат при минимальных издержках. Кроме того, он позволяет рационально организовать коллективную работу над проектом и обеспечивает наличие точно определенного плана исследований и сроков его выполнения.

Типичный процесс *data science* состоит из шести последовательно выполняемых этапов (рис. 2.).

Этап 1. Процесс начинается с определения *цели* исследования. Основным результатом первого этапа является проектное задание, которое должно включать следующее [17]: четко сформулированную цель исследований; предназначение проекта; предварительное описание методики анализа; планируемые к использованию ресурсы; обоснование практической реализуемости проекта; предполагаемые результаты проекта.

Этап 2. Выполняется сбор данных. Исходные данные могут храниться во многих форматах: от простых текстовых файлов до таблиц баз данных. Прежде всего, следует оценить актуальность и качество данных, которые могут определяться местом их хранения. Данные могут храниться в *базах данных*, *витринах данных* (*data marts*), *складах данных* (*data warehouses*) и *озерах данных* (*data lakes*).

Базы данных предназначены, прежде всего, для хранения данных, тогда как *склады* данных – для чтения и анализа этих данных. *Витрины* данных представляют собой вариант склада данных, ориентированный на обслуживание конкретного пользователя. Если в складах и витринах данные хранится в уже обработанном виде, то в *озерах* данных они содержатся в исходном, необработанном формате.

Этап 3. Подготовка данных. Данные, полученные на предыдущем этапе, требуют специальной обработки, предназначенной для обнаружения и устранения различных дефектов и возможных ошибок, для объединения данных из разных источников и их преобразования.

Это очень важный этап, так как на проверку и очистку данных затрачивается значительная часть времени проекта (в некоторых случаях – до 80%). Его результаты определяют успешное последующее применение моделей и сокращают время на исправление аномальных результатов. На данном этапе данные из низкоуровневой формы преобразуются в данные, которые могут напрямую использоваться в применяемых моделях. Этот этап включает три шага:

- *очистка данных* – удаление некорректных значений из источника данных и устранение расхождений между источниками;
- *интеграция данных* – объединении информации из нескольких источников;
- *преобразование данных* – преобразование данных в подходящий формат для использования в моделях.

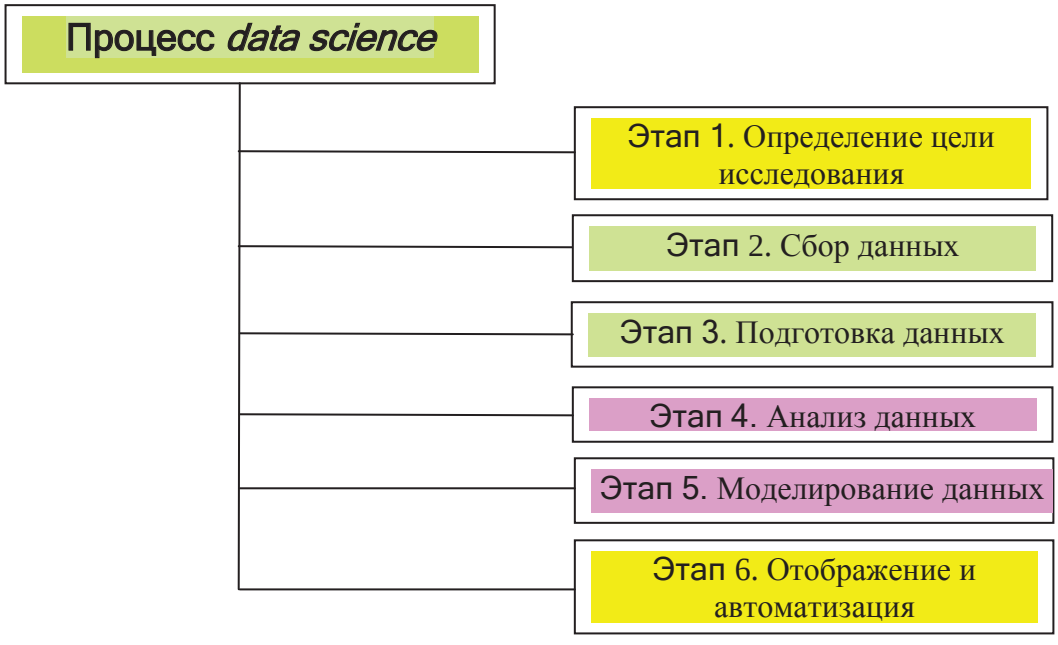

Рис. 2. Структура процесса data science

Очистка данных представляет собой часть (подпроцесс) общего процесса *data science*, направленную на устранение следующих типов ошибок в данных.

Ошибки ввода данных, которые обусловлены человеческим фактором и сбоями средств вычислительной техники или оборудования. В частности, это ошибки, возникающие при передаче данных и в фазах извлечения, преобразования и загрузки (*ETL – Extract-Transform-Load*). Если количество классов в анализируемых переменных невелико, то обнаружение таких ошибок может осуществляться посредством группировки данных с подсчетом значений.

Избыточные пробелы (Whitespaces) – такая ошибка обычно трудно обнаруживается и приводит, например, к несовпадению ключей при работе с таблицами реляционной базы данных.

Невозможные значения – ошибка в данных, устраняемая проверкой разумности (*sanity checks*), в ходе которой значения проверяются на соответствие физическим или теоретическим критериям возможности и невозможности.

Выброс (*outlier*) – заметно отклоняющийся результат наблюдений, который обусловлен иной логикой или иным порождающим процессом, в сравнении с другими результатами. Основной способ поиска выбросов основан на использовании статистических методов.

Отсутствующие значения. Если переменная может быть описана устойчивым законом распределения, то можно восстановить отсутствующие значения на основании этого закона распределения.

Разные единицы измерения. Это ошибки, проявляющиеся при слиянии наборов данных, когда необходимо обращать внимание на соответствие единиц измерения. Проблема решается простым преобразованием.

Разные уровни агрегирования. Ошибки такого рода обнаруживаются достаточно легко и устраняются согласованием наборов данных.

Интеграция данных. Данные поступают из нескольких разных источников и могут быть представлены в разных формах, размерах, типах и структурах: от баз данных и файлов *Excel* до текстовых документов.

Существуют различные способы интеграции данных. В случае обработки данных в табличных структурах применяется две основные операции, комбинирующие информацию из разных источников данных.

Первая операция – *соединение* (*joining*): расширение наблюдений из одной таблицы информацией из другой таблицы.

Вторая операция – *дополнение*: наблюдения из одной таблицы просто добавляются в другую таблицу.

Преобразование данных. После очистки и интеграции данных следующей задачей является преобразование данных в форму, удобную для их моделирования. Для решения этой задачи следующие подходы: *сокращение количества переменных* и *использование вспомогательных переменных*.

Излишнее количество переменных осложняет работу с моделями данных и резко увеличивает время обработки, особенно в тех случаях, когда алгоритмы моделей связаны с полным или направленным перебором. Существуют специальные методы сокращения количества переменных с минимальной потерей информации. Одним из таких приемов является декомпозиция исходной задачи на несколько подзадач, каждая из которых имеет существенно сокращенный набор переменных.

Переход к вспомогательным переменным применяется в моделировании данных и часто используется в экономических расчетах. Вспомогательные переменные принимают только одно из двух значений (*true* – 1 или *false* – 0) и используются для обозначения присутствия (или отсутствия) однозначного эффекта, объясняющего наблюдение.

Этап 4. Выполняется анализ данных. Выявляются закономерности и отклонения, исследуются взаимозависимости между переменными. При этом используются методы компьютерного анализа данных, методы статистической обработки данных, корреляционно-регрессионный анализ и анализ временных рядов [1, 11]. Этот этап часто обозначается *EDA* (*Exploratory Data Analysis* – исследовательский анализ данных).

Этап 5. Выполняется построение модели (моделирование данных) с целью построения прогнозов исследуемых процессов, проведения классификации рассматриваемых объектов, оптимизации структуры систем или процедуры управления ими. Этот этап отличается от предыдущего бо́льшей целенаправленностью, нацеленностью на конкретный результат.

В ходе моделирования используются методы и модели из области статистики, машинного обучения, решения оптимизационных задач, постановки статистического эксперимента и др. Построение модели является итеративным процессом, в ходе которого выбирается наиболее приемлемая модель. Процесс построения большинства моделей включает следующие основные шаги: выбор метода моделирования; выполнение модели; диагностика и сравнение моделей.

Этап 6. Демонстрируются полученные результаты и проводится автоматизация процесса анализа, что дает возможность использовать, при необходимости, разработанные модели в другом рабочем процессе.

Следует заметить, что описанный процесс *data science* не обязательно имеет линейный характер, и последовательное продвижение от начального этапа к конечному встречается редко. Такой подход годится не для всех типов проектов и не является единственно возможным. На практике часто приходится возвращаться назад, к предыдущим этапам, для внесения определенных изменений и пересмотра отдельных вопросов, повторять различные этапы. Этим определяется итеративный характер процесса *data science*.

Представленный процесс *data science* в наибольшей степени подходит для сложных проектов *data science* с большим количеством ресурсов. Альтернативой последовательному процессу с итерациями является гибкая (*agile*) модель проекта. Гибкие методологии также

могут быть использованы для реализации проектов *data science*. Однако на практике в большинстве случаев предпочтение отдается более формальному структурному подходу.

4. Области применения Data science и больших данных

В качестве отдельных прикладных задач, актуальных для правовой сферы, можно выделить следующие: поиск ценной информации при выполнении аналитических разработок; многоаспектный анализ преступности в современных условиях [9]; выявление случаев финансового мошенничества и других видов преступной деятельности; сбор информации об потенциально опасных абонентах сети Интернет телематической сети ГАС РФ «Правосудие»; личностная аналитика (people analytics), изучение неформальных связей; глубокий анализ текстовых документов; противодействие «цифровой преступности» [16] и др. в соответствии с Концепцией формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов[4].

Таким образом, количество направлений потенциального применения *Data science* и больших данных в правовой сфере и, в частности, в едином информационном пространстве судебной системы [12], достаточно велико.

Рецензент: ***Марков Алексей Сергеевич,*** *доктор технических наук, доцент, профессор МГТУ им. Баумана, главный редактор журнала «Вопросы кибербезопасности», г. Москва, Россия.*

E-mail: *a.markov@npo-echelon.ru*

Литература

1. Агеев Ю. Д., Кавин Ю. А., Павловский И. С., Федосеев С. В. Анализ данных. Казань : Бук, 2018. 308 с.
2. Брюс Э., Брюс П. Практическая статистика для специалистов Data Science. СПб. : Изд-во «БХВ-Петербург», 2018. 304 с.
3. Вандер Плас Дж. Python для сложных задач. Наука о данных и машинное обучение. СПб. : Изд-во «Питер», 2018. 576 с.
4. Ващекин А. Н., Ващекина И. В. Информационное право: прикладные задачи и математические методы // Информационное право. 2017. № 3. С. 17–21.
5. Дэви С., Арно М., Мухамед А. Основы data science и Big Data/Python и наука о данных. СПб. : Питер, 2017. 336 с.
6. Ларина Е. С., Овчинский В. С. Искусственный интеллект. Большие данные. Преступность. М. : Изд. дом «Книжный мир», 2018. 416 с.
7. Лесковец Ю., Раджараман А., Ульман Дж. Д. Анализ больших наборов данных. М. : Изд-во «ДМК Пресс», 2016. 498 с.
8. Ловцов Д. А. Информационная теория эргасистем: Тезаурус. М. : Наука, 2005. 248 с.
9. Ловцов Д. А., Богданова М. В., Паршинцева Л. С. Правовая статистика преступности в современных условиях // Правовая информатика. 2017. № 4. С. 40–48.
10. Ловцов Д. А., Богданова М. В., Паршинцева Л. С. Пакеты прикладных программ для многоаспектного анализа судебной статистической информации // Правовая информатика. 2017. № 1. С. 28–36.
11. Ловцов Д. А., Богданова М. В., Паршинцева Л. С. Основы статистики / Под ред. Д. А. Ловцова. М. : РГУП, 2017. 160 с.
12. Ловцов Д. А., Ниесов В. А. Системная модернизация «цифрового» судопроизводства в России // Государство и право в новой информационной реальности: Сб. науч. тр. / Отв. ред. Е. В. Алферова, Д. А. Ловцов. М. : ИНИОН РАН, 2018. С. 22–29.
13. Ловцов Д. А., Федичев А. В. Место и роль правовой информатики в системе информационно-правовых знаний // Правовая информатика. 2017. № 1. С. 5–12.
14. Ловцов Д. А., Черных А. М. Модернизация системы судебной статистики на основе новой геоинформационной технологии // Правовая информатика. 2016. № 1. С. 7–14.
15. Марц Н., Уоррен Дж. Большие данные. Принципы и практика построения масштабируемых систем обработки данных в реальном времени. М. : Изд. дом «Вильямс», 2018. 368 с.
16. 16. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения. М. : ИНФРА-М, 2018. 227 с.
17. Федосеев С. В., Беркетов Г.А., Микрюков А.А. Подходы к проектированию программного комплекса как к интеллектуальной системе // Труды XII Междунар. науч.-прак. конф. «Инновации на основе информационных коммуникационных технологий» (1–10 октября 2015 г.) / ВШЭ. Сочи: МИЭМ, 2015. С. 248–250.
18. Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных. М. : Изд-во «ДМК Пресс», 2015. 400 с.
19. Чаллавала Ш., Лакхатария Д., Мехта Ч., Патель К. MySQL 8 для больших данных. М. : Изд-во «ДМК Пресс», 2018. 226 с.

[4] Эта концепция разработана во исполнение Указа Президента РФ от 1 июля 1994 г. № 1390 «О совершенствовании информационно-телекоммуникационного обеспечения органов государственной власти и порядке их взаимодействия при реализации государственной политики в сфере информатизации»).

THE USE OF BIG DATA MODERN TECHNOLOGIES IN LEGAL SPHERE

Sergey Fedoseev, *Ph.D., associate Professor of the Chair of Information Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russia.*
E-mail: *fedsergvit@mail.ru*

Keywords: *digital transformation, legal information, information and telecommunication technologies, big data, data science, data categories, big data ecosystem, data science process, applications of Data science and big data.*

Abstract.
Purpose: *substantiation of methodological approaches to solving problems of effective processing of large amounts of data in the legal sphere.*
Method: *logical modeling of legal relations and information relations in the legal sphere. System analysis of the relationship between the subject area of the legal sphere and the main objects and methods of big data technology.*
Results: *the necessity of digital transformation and transition to new information technologies in the legal sphere, creation and development of big data processing infrastructure; the analysis of the data science and big data domain, data categories in Data science; the big data ecosystem and data science; the stages of the Data science process; the application areas of Data science and big data.*

References

1. Ageev Iu. D., Kavin Iu. A., Pavlovskii I. S., Fedoseev S. V. Analiz dannykh, Kazan' : Buk, 2018, 308 pp.
2. Brius E., Brius P. Prakticheskaia statistika dlia spetsialistov Data Science, SPb. : Izd-vo "BKhV-Peterburg", 2018, 304 pp.
3. Vander Plas Dzh. Python dlia slozhnykh zadach. Nauka o dannykh i mashinnoe obuchenie, SPb. : Izd-vo "Piter", 2018, 576 pp.
4. Vashchekin A. N., Vashchekina I. V. Informatsionnoe pravo: prikladnye zadachi i matematicheskie metody, Informatsionnoe pravo, 2017, No. 3, pp. 17-21.
5. Devi S., Arno M., Mukhamed A. Osnovy data science i Big Data/Python i nauka o dannykh, SPb. : Piter, 2017, 336 pp.
6. Larina E. S., Ovchinskii V. S. Iskusstvennyi intellekt. Bol'shie dannye. Prestupnost', M. : Izd. dom "Knizhnyi mir", 2018, 416 pp.
7. Leskovets Iu., Radzharaman A., Ul'man Dzh. D. Analiz bol'shikh naborov dannykh, M. : Izd-vo "DMK Press", 2016, 498 pp.
8. Lovtsov D. A. Informatsionnaia teoriia ergasistem: Tezaurus, M. : Nauka, 2005, 248 c.
9. Lovtsov D. A., Bogdanova M. V., Parshintseva L. S. Pravovaia statistika prestupnosti v sovremennykh usloviiakh, Pravovaia informatika, 2017, No. 4, pp. 40-48.
10. Lovtsov D. A., Bogdanova M. V., Parshintseva L. S. Pakety prikladnykh programm dlia mnogoaspektnogo analiza sudebnoi statisticheskoi informatsii, Pravovaia informatika, 2017, No. 1, pp. 28-36.
11. Lovtsov D. A., Bogdanova M. V., Parshintseva L. S. Osnovy statistiki, pod red. D. A. Lovtsova, M. : RGUP, 2017, 160 pp.
12. Lovtsov D. A., Niesov V. A. Sistemnaia modernizatsiia "tsifrovogo" sudoproizvodstva v Rossii, Gosudarstvo i pravo v novoi informatsionnoi real'nosti: sb. nauch. tr., otv. red. E. V. Alferova, D. A. Lovtsov, M. : INION RAN, 2018, pp. 22-29.
13. Lovtsov D. A., Fedichev A. V. Mesto i rol' pravovoi informatiki v sisteme informatsionno-pravovykh znanii, Pravovaia informatika, 2017, No. 1, pp. 5-12.
14. Lovtsov D. A., Chernykh A. M. Modernizatsiia sistemy sudebnoi statistiki na osnove novoi geoinformatsionnoi tekhnologii, Pravovaia informatika, 2016, No. 1, pp. 7-14.
15. Marts N., Uorren Dzh. Bol'shie dannye. Printsipy i praktika postroeniia masshtabiruemykh sistem obrabotki dannykh v real'nom vremeni, M. : Izd. dom "Vil'iams", 2018, 368 pp.
16. Russkevich E. A. Ugolovnoe pravo i "tsifrovaia prestupnost'": problemy i resheniia, M. : INFRA-M, 2018, 227 pp.
17. Fedoseev S. V., Berketov G.A., Mikriukov A.A. Podkhody k proektirovaniiu programmnogo kompleksa kak k intellektual'noi sisteme, Trudy XII Mezhdunar. nauch.-prak. konf. "Innovatsii na osnove informatsionnykh kommunikatsionnykh tekhnologii" (1-10 oktiabria 2015 g.), VShE, Sochi : MIEM, 2015, pp. 248-250.
18. Flakh P. Mashinnoe obuchenie. Nauka i iskusstvo postroeniia algoritmov, kotorye izvlekaiut znaniia iz dannykh, M. : Izd-vo "DMK Press", 2015, 400 pp.
19. Challavala Sh., Lakkhatariia D., Mekhta Ch., Patel' K. MySQL 8 dlia bol'shikh dannykh, M. : Izd-vo "DMK Press", 2018, 226 pp.

РАЗВИТИЕ КОНЦЕПЦИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА

*Чубукова С. Г.**

***Ключевые слова**: информационное общество, информационные технологии, информационная безопасность, информационное законодательство, информационный суверенитет.*

Аннотация.

Цель: определить основные направления развития концепции правового регулирования международного информационного обмена.

Метод: системный анализ концепции правового регулирования международного информационного обмена и информационного законодательства Российской Федерации.

Результат: стратегической задачей России становится полномасштабное вхождение в глобальное информационное общество в качестве его полноправного участника при сохранении политической независимости, национальной самобытности и культурных традиций. Решение этой задачи требует разработки единой концепции правового регулирования международного информационного обмена. В работе рассмотрены специальные принципы международного информационного обмена, проблема определения информационного суверенитета государства, проблемы системы субъектов международного информационного обмена и их правового статуса, проблема признания электронных документов и электронных подписей физических и юридических лиц иностранных государств.

Положения данной концепции должны найти отражение при разработке нового федерального закона об участии России в международном информационном обмене.

DOI: 10.21681/1994-1404-2018-4-59-65

Международное сотрудничество в области информационного обмена – одна из важнейших составляющих государственной политики в *информационной сфере* [8, 10], непременное условие формирования международного информационного пространства как основы создания глобального информационного общества.

Общие вопросы международного информационного обмена в рамках развития глобального информационного общества освещены в таких программных документах как Хартия глобального информационного общества[1], Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии»[2], Тунисская программа для информационного общества[3].

В рамках СНГ, БРИКС, ШОС, ЕАЭС, Европейского сообщества, Союзного государства с Республикой Беларусь Россия активно участвует в работе различных международных организаций. Межгосударственный обмен информацией осуществляется, главным образом, в рамках двух или многосторонних межгосударственных соглашений. Так на 19-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ 26 марта 2002 года принят Модельный закон о международном информационном обмене[4].

Важность выстраивания системы международного информационного обмена подтверждает и тот факт, что одним из первых законов информационного законодательства Российской Федерации стал Федеральный закон «Об участии в международном информационном обмене».[5] Целью данного Федерального закона было создание условий для эффективного участия России в международном информационном обмене в рамках

[1] Хартия Глобального информационного общества // Дипломатический вестник. 2000. № 8. С. 51 – 56.

[2] Декларация принципов. Построение информационного общества – глобальная задача в новом тысячелетии. // URL: http://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата обращения: 05.12.2018).

[3] Тунисская программа для информационного общества // URL: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (дата обращения: 05.12.2018).

[4] Модельный закон «О международном информационном обмене» (принят постановлением Межпарламентской Ассамблеи государств - участников СНГ от 26 марта 2002 г. № 19-7) // Информационный бюллетень Межпарламентской Ассамблеи государств-участников СНГ. 2002. № 29.

[5] Федеральный закон от 4 июля 1996 г. «Об участии в международном информационном обмене» // СЗ РФ. 1996. № 28. Ст. 3347 (*утратил силу*).

* ***Чубукова Светлана Георгиевна,*** *кандидат юридических наук, доцент, почетный работник высшего профессионального образования Российской Федерации, доцент кафедры информационного права и цифровых технологий Московского государственного юридического университета имени О. Е. Кутафина (МГЮА), г. Москва, Россия.*

E-mail: sgchubukova@msal.ru

единого мирового информационного пространства, защита интересов Российской Федерации, субъектов Российской Федерации и муниципальных образований, физических и юридических лиц при международном информационном обмене.

Однако геополитический передел мира, глобализация мировой экономики, переоценка идеологических ценностей, развитие информационно-телекоммуникационных технологий потребовали переосмысления современной *системы международного информационного обмена* [1]. В связи с этими глобальными тенденциями Федеральный закон «Об участии в международном информационном обмене» утратил силу. Кроме того, установленные в нем требования были применимы только к физическому перемещению информации и информационных ресурсов на материальных носителях через таможенную границу Российской Федерации и не обеспечивали адекватного правового регулирования международного информационного обмена в рамках трансграничной сети Интернет [13].

Как результат, сегодня в российском законодательстве отсутствует нормативный акт, реализующий целостную концепцию правового регулирования международного информационного обмена. В разрозненных нормах федеральных законах речь идет о международном сотрудничестве на основе соблюдения общепризнанных принципов и норм международного права. Очевидно, что приведение указанных норм в целостную систему невозможно без разработки *единой концепции правового регулирования* участия России в международном информационном обмене.

Важность этой работы определяется задачами, поставленными в Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы[6], которая в числе основных национальных интересов называет повышение роли России в мировом гуманитарном и культурном пространстве, и подтверждает необходимость укреплять информационный обмен между государствами.

В основе международного информационного обмена лежат общепризнанные принципы международного права, которые являются императивными и имеют универсальный характер в любых международных отношениях. Они закреплены в уставе ООН, в Декларации о принципах международного права: принцип уважения прав и основных свобод человека, принцип сотрудничество между государствами; принцип добросовестного выполнения международных обязательств и другие. Однако очевидно, что специфику правового регулирования информационных отношений должны определять специальные принципы [8 – 10], которые и надлежит разработать в рамках концепции международного информационного обмена.

Учитывая особенности международного информационного обмена, в зависимости от содержания можно выделить несколько групп специальных принципов международного информационного обмена:

1) системообразующие принципы международного информационного обмена: комплексность правового воздействия на отношения в сфере международного информационного обмена путем сочетания экономических, организационно-административных и общественно-политических механизмов, позволяющих целенаправленно мотивировать деятельность субъектов на достижение целей международного информационного обмена; обеспечение свободы получения и распространения информации для всех субъектов информационных отношений; установление баланса прав и законных интересов человека, общества и государства в сфере международного информационного обмена;

2) международные принципы создания информационного общества, которые определены Окинавской хартией глобального информационного общества, Декларацией принципов «Построение информационного общества – глобальная задача в новом тысячелетии», Тунисской программой для информационного общества: применение информационно-телекоммуникационных технологий в целях развития личности, общества и государства; обеспечение каждому возможности иметь доступ к знаниям; развитие доступной информационной и коммуникационной инфраструктуры, ликвидация цифрового разрыва; предоставление государственных и негосударственных услуг в электронном виде.

3) принципы, связанные с правом любого человека на доступ к информации как к важнейшему стратегическому ресурсу развития: обеспечение доступности, достоверности, полноты и своевременности информации, ограничение доступа к информации исключительно на основании закона с целью защиты прав и законных интересов других лиц;

4) принципы, связанные с обеспечение информационной безопасности субъектов международного информационного обмена[7] [11].

Одной из важнейших задач, решаемых в концепции международного информационного обмена, должно стать определение соотношения национальных и глобальных (наднациональных) интересов в рамках разработки понятия и направлений реализации *суверенитета Российской Федерации в информационном пространстве*.

Утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646 новая Доктрина информационной безопасности основными направлениями обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства определяет защиту суверенитета Россий-

[6] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

[7] Организационное и правовое обеспечение информационной безопасности: Учебник / Под ред. Т. А. Поляковой, А. А. Стрельцова. М.: Юрайт, 2016. 324 с.

ской Федерации в информационном пространстве посредством осуществления самостоятельной и независимой политики, направленной на реализацию национальных интересов в информационной сфере[8].

В условиях трансграничности информационного пространства все чаще звучат утверждения, что суверенитет государств в его традиционном понимании размывается, а государственные границы постепенно превращаются в фикцию. Государства не всегда могут контролировать киберпространство и противодействовать противоправным действиям в сети Интернет. Это дает основание некоторым исследователям говорить, что государственный суверенитет не распространяется на информационные сети, а *киберпространство* представляет собой некое вненациональное саморегулирующееся сообщество пользователей [5, 14]. Указанные дискуссии подтверждают необходимость дальнейшего изучения правовой наукой вопросов, связанных с изменением содержания понятия государственного суверенитета, обусловленным процессами глобализации, межгосударственной интеграции и развития информационно-телекоммуникационных трансграничных технологий и сетей.

Несмотря на то, что большинство ученых рассматривают правовой суверенитет как единое и неделимое понятие, которое охватывает все сферы государственной деятельности, в том числе и информационную сферу, в последнее время все шире развивается дискуссия по поводу введения понятия *«информационный суверенитет»*.

Так, необходимость обеспечения информационного суверенитета, т. е. формирования и проведения политики, исходя из интересов национальной безопасности России, содержится в Концепции развития рынка ценных бумаг в Российской Федерации[9]. В Концепции формирования информационного пространства СНГ одной из важнейших проблем формирования информационного пространства государств-участников СНГ названо обеспечение каждым из них собственной информационной безопасности и защиты своего информационного суверенитета. Для своевременного решения этих вопросов каждое государство-участник СНГ осуществляет своевременный мониторинг «противоречий» в информационной политике и угроз своему информационному суверенитету[10].

В Концепции внешней политики Российской Федерации[11], утвержденной Указом Президента РФ от 30 ноября 2016 г. № 640, отмечено, что «на передний план, наряду с военной мощью, выдвигаются такие важные факторы влияния государств на международную политику, как экономические, правовые, технологические, информационные» (п. 8). Россия, согласно данной Концепции, принимает необходимые меры для обеспечения национальной и международной информационной безопасности, противодействия угрозам государственной, экономической и общественной безопасности, исходящим из информационного пространства, для борьбы с терроризмом и иными криминальными угрозами с применением информационно-телекоммуникационных технологий, противодействует их использованию в военно-политических целях, не соответствующих нормам международного права, включая действия направленные на вмешательство во внутренние дела государств или представляющие угрозу международному миру, безопасности и стабильности, добивается выработки под эгидой ООН универсальных правил ответственного поведения государств в области обеспечения международной информационной безопасности (п. 28).

Ряд ученых также поддерживают идею необходимости выделения *информационного суверенитета* [3, 6]. В частности, информационный суверенитет определяется как верховенство государственной власти и возможность национального (или государственно-правового) регулирования определенного информационного пространства [3].

В докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (Семидесятая сессия Генеральной Ассамблеи ООН, 22 июля 2015 года, A/70/174)[12] было отмечено, что государственный суверенитет и международные нормы и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием информационных и коммуникационных технологий (ИКТ), а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории.

В апреле 2017 года Министерство связи и массовых коммуникаций Российской Федерации в целях повышение безопасности сети «Интернет», обеспечение гарантий прав и свобод ее пользователей, равноправного международного сотрудничества в управлении сетью разработало новую концепцию конвенции ООН (или концепция безопасного функционирования и раз-

[8] Указ Президента РФ от 5 декабря 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[9] Указ Президента РФ от 1 июля 1996 г. № 1008 (ред. от 16.10.2000) «Об утверждении Концепции развития рынка ценных бумаг в Российской Федерации». // СЗ РФ. 1996. № 28. Ст. 3356; СЗ РФ. 2000. № 43. Ст. 4233.

[10] Решение о Концепции формирования информационного пространства Содружества Независимых Государств (Москва, 18 октября 1996 г.) // Информационный вестник Совета глав государств и Совета глав правительств СНГ «Содружество». 1996. № 4. С. 87.

[11] Указ Президента Российской Федерации от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации» // URL: http://publication.pravo.gov.ru/Document/View/0001201612010045?index=1&rangeSize=1 (дата обращения: 15.07.2017)

[12] Доклад Группы правительственных экспертов ООН. 22 июля 2015 г., A/70/174 // [Электронный ресурс]. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (дата обращения: 05.12.2018).

вития сети Интернет)[13]. Указанная концепция вводит понятие сетевого суверенитета и предлагает общие принципы международного сотрудничества по управлению сетью «Интернет».

Сетевой суверенитет определен как возможность безусловной реализации полномочий государства в отношении объектов информационной инфраструктуры национального сегмента сети Интернет, которыми государство обладает в силу суверенитета и которые осуществляет в целях реализации суверенной власти. Государства осуществляют управление сетью Интернет на основе суверенного равенства, признания сетевого суверенитета, устойчивого развития, защиты от трансграничного влияния, обеспечения безопасности и укрепления мер по обеспечению безопасного функционирования сети Интернет. Государства сохраняют национальный суверенитет в информационной сфере сети Интернет, гарантируют своим гражданам защиту в своей юрисдикции [15], обеспечивают управление, стратегическую устойчивость и защиту национального сегмента сети Интернет.

Очевидно, что государственный суверенитет сложное и многоплановое явление, которое в информационной сфере обогащается новым содержанием, которое должно найти отражение в концепции правового регулирования международного информационного обмена.

Другой важной задачей является определение *субъектов международного информационного обмена* и закрепление в законодательстве их правового статуса.

До настоящего времени российским ведомством, обладающим необходимой компетенцией в решении вопросов, связанных с развитием телекоммуникаций, информационной инфраструктуры, универсальных информационных услуг, является Министерство связи и массовых коммуникаций РФ, которое представляет интересы России, в установленном порядке взаимодействуя с органами государственной власти иностранных государств и международными организациями в сфере информационного обмена. В то же время области интересов нашего государства гораздо шире интересов одного ведомства. Сегодня отсутствует всеобъемлющая концепция участия России в деятельности международных организаций в сфере международного информационного обмена, которая отражает интересы всех заинтересованных государственных ведомств и организаций, частных компаний, организаций и граждан, и которая лежала бы в основе реализации механизмов межведомственной координации международного сотрудничества в области развития информационного общества.

Также до конца не решена проблема *признания электронных документов и электронных подписей физических и юридических лиц иностранных государств*.

Так в статье 7 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[14] законодатель установил презумпцию юридической силы электронного документа, подписанного электронной подписью, сертификат ключа проверки которой выдан в соответствии с нормами иностранного государства и международными стандартами.

Основным международным стандартом в данной области является рекомендация Европейской экономической комиссии ООН в отношении функциональной совместимости подписанных цифровых документов[15], в которой отмечено, что многообразие стандартов электронных подписей способно затруднить в техническом или юридическом отношении подтверждение подписанных цифровых документов получателем. В некоторых случаях это может непосредственным образом влиять на способность организаций и государственных органов без риска для себя обмениваться цифровыми документами как между собой, так и с партнерами - управленческими и финансовыми структурами. Применение рекомендуемых стандартов в конкретных ситуациях может также быть связано с проблемами соблюдения и дополнительными расходами, а также, возможно, с необходимостью регулятивных или других правовых механизмов, что также необходимо учитывать при определении типа того общего положительного результата, который предполагается достичь.

И, конечно, остро стоит проблема *обеспечения информационной безопасности* в рамках международного информационного обмена.

Актуальность этой проблемы сегодня признает все мировое сообщество, что отражено в целом ряде документов, включая ежегодные резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности»[16]. В 2015 году Генеральная Ассамблея ООН в ходе 70-й сессии приняла резолюцию, подготовленную российской стороной. В ней отмечается, что распространение и использование информацион-

[13] Концепция конвенции ООН (или концепция безопасного функционирования и развития сети Интернет) // [Электронный ресурс]. URL: http://minsvyaz.ru/uploaded/files/ prilozheniekontseptsiikonventsiioon.docx (дата обращения: 05.12.2018).

[14] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // СЗ РФ. 2011. № 15. Ст. 2036.

[15] ECE/TRADE/C/CEFACT/2010/14/Rev.1 Рекомендация ЕЭК ООН № 37: Функциональная совместимость подписанных цифровых документов // [Электронный ресурс]. URL: http://www.unece.org/fileadmin/DAM/cefact/cf_plenary/plenary12/ECE_TRADE_C_ CEFACT_2010_14_Rev1R.pdf (дата обращения: 05.12.2018).

[16] Резолюции: A/RES/53/70 от 4 декабря 1998 года; A/RES/54/49 от 1 декабря 1999 года; A/RES/55/28 от 20 ноября 2000 года; A/RES/56/19 от 29 ноября 2001 года; A/RES/57/53 от 22 ноября 2002 года; A/RES/58/32 от 8 декабря 2003 года; A/RES/59/61 от 3 декабря 2004 года; A/RES/60/45 от 8 декабря 2005 года; A/RES/61/54 от 6 декабря 2006 года; A/RES/62/17 от 5 декабря 2007 года; A/RES/63/37 от 2 декабря 2008 года; A/RES/64/25 от 2 декабря 2009 года; A/RES/65/41 от 8 декабря 2010 года; A/RES/66/24 от 2 декабря 2011 года; A/RES/67/27 от 3 декабря 2012 года; A/RES/68/243 от 27 декабря 2013 года; A/RES/69/28 от 2 декабря 2014 года; A/RES/70/237 от 23 декабря 2015 г.; A/RES/71/28 от 5 декабря 2016 г.

ных технологий и средств затрагивают интересы всего международного сообщества и что широкое международное взаимодействие способствует обеспечению оптимальной эффективности. Соавторами данной резолюции выступили более 80 государств из всех регионов мира, в том числе США, Япония, Великобритания, Германия, Испания, Нидерланды и Франция.

В 2013 году Президент РФ утверждает Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года[17]. В этом документе определены цели, задачи и приоритетные направления государственной политики в области международной информационной безопасности. В качестве основной угрозы в данной сфере названо использование информационных и коммуникационных технологий в качестве «*информационного оружия*» [10] в военно-политических целях, для вмешательства во внутренние дела суверенных государств, а также для совершения преступлений. Противодействие этой угрозе и ее нейтрализация названы основными целями государственной политики России в области международной информационной безопасности. В качестве одной из задач названо содействие подготовке и принятию государствами - членами ООН акта, определяющего порядок обмена информацией о передовых практиках в области обеспечения безопасности функционирования элементов *информационной инфраструктуры* [10].

Для ее достижения необходимо сформировать *систему международной информационной безопасности* [2] на двустороннем, многостороннем, региональном и глобальном уровнях; установить международный правовой режим нераспространения информационного оружия. Поставлена задача создания механизма международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических и экстремистских целях.

В условиях становления глобального информационного общества одним из важных средств обеспечения информационной безопасности становиться установление технологических требований к безопасности систем информационного обмена и развитие системы международных (включая *RFC – Requests for Comments* – «требования к обсуждению») и национальных технико-правовых стандартов безопасности информации [11].

Такие требования на национальном уровне включают добровольные стандарты, принимаемые национальными структурами по стандартизации, которые содержат рекомендованные для использования правила добросовестной практики и государственные стандарты (серии Р в России)[18].

На международном уровне следует выделить британский стандарт *BS* 7799, направленный на формирование информационной защиты данных, и международный комплекс стандартов *ISO* 27002, разработанных Международной организацией по стандартизации (*ISO*), который представляет собой совокупность практик и рекомендаций по внедрению систем и оборудования информационной защиты.

Задачей международного *технического регулирования* являются содействие совместимости существующих и разрабатываемых национальных и международных стандартов[19] [12].

Многие специалисты в сфере технического регулирования считают, что человеку, как субъекту отношений, и его интересам в области технического нормирования отводится недостаточное внимание. Механизм технического регулирования должен обеспечить, с одной стороны, безопасность жизни и здоровья граждан, а с другой – свободное перемещение информации, использование информационных технологий и систем международного информационного обмена. Необходимо найти баланс между этими задачами [4].

Решение этих и многих других вопросов невозможно без разработки единой концепции правового регулирования международного информационного обмена и на ее основе создания правового обеспечения международного сотрудничества и участия России в деятельности международных организаций в информационной сфере.

Существующее правовое обеспечение участия России в международном информационном обмене сегодня разбросано по специальных нормативным актам в различных областях – гидрометеорологии, архивном

[17] Утв. Президентом РФ 24 июля 2013 г., № Пр-1753.

[18] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения; Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации; ГОСТ Р 51188-98. Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство; ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения; ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель; ГОСТ Р ИСО/МЭК 15408-2-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности; ГОСТ Р ИСО/МЭК 15408-3-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности; ГОСТ Р ИСО/МЭК 15408. Общие критерии оценки безопасности информационных технологий — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности, благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами; ГОСТ Р ИСО/МЭК 17799. Информационные технологии. Практические правила управления информационной безопасностью. Прямое применение международного стандарта с дополнением – *ISO/IEC* 17799:2005; ГОСТ Р ИСО/МЭК 27001. Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования. Прямое применение международного стандарта – *ISO/IEC* 27001:2005; ГОСТ Р 51898-2002. Аспекты безопасности. Правила включения в стандарты.

[19] Актуальные проблемы информационного права: Учебник / Под ред. И. Л. Бачило, М. А. Лапиной. М.: Юстиция, 2016. 534 с.

деле, налоговом законодательстве и др. По мнению ученых и практиков такая практика себя не оправдывает, а только вносит противоречивость в «информационную» терминологию и систему организационно-правовых механизмов [78].

Положения данной концепции должны найти отражение при разработке нового федерального закона об участии России в международном информационном обмене.

Рецензент: ***Полякова Татьяна Анатольевна****, доктор юридических наук, профессор, главный научный сотрудник, заведующая сектором информационного права ИГП РАН, г. Москва, Россия.*

E-mail: *polyakova_ta@mail.ru*

Литература

1. Виноградова С. М., Мельник Г. С. Проблемы преодоления неравенства в международном информационном обмене // Гуманитарный вектор. 2012. № 2 (30). С. 239–246.
2. Захаров Т. В. Международное сотрудничество государств в сфере информационной безопасности и правовые подходы к его регулированию // Государство и право в новой информационной реальности: Сб. науч. тр. / Отв. ред. Е. В. Алферова, Д. А. Ловцов. М. : ИНИОН РАН, 2018. С. 119–134.
3. Ефремов А. А. Электронное правительство и международное право // Труды XIV Всероссийской объединенной конференции «Интернет и современное общество» (IMS-2011). СПб., 2011. С. 192.
4. Красавин А. В. Проблемы правотворчества в сфере технического регулирования // Право и современные государства. 2013. № 6. С. 52–63.
5. Красиков Д. В. Международно-правовая ответственность государств в киберпространстве // Государство и право в новой информационной реальности: Сб. науч. тр. / Отв. ред. Е. В. Алферова, Д. А. Ловцов. М. : ИНИОН РАН, 2018. С. 235–247.
6. Красиков Д. В. Территориальный суверенитет и делимитация юрисдикций в киберпространстве // Государство и право в новой информационной реальности: Сб. науч. тр. / Отв. ред. Е. В. Алферова, Д. А. Ловцов. М. : ИНИОН РАН, 2018. С. 235–247.
7. Ловцов Д. А. Проблема эффективности международно-правового обеспечения глобального информационного обмена // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2011. № 11 (17). С. 24–31.
8. 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.
9. Ловцов Д. А. Система принципов эффективного правового регулирования информационных отношений в инфосфере // Информационное право. 2017. № 1. С. 13–18.
10. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере: Монография. М. : РГУП, 2016. 316 с.
11. Ловцов Д. А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3–7.
12. Ловцов Д. А., Лобан А. В., Цимбал В. А. Система информационного обеспечения технического регулирования Таможенного Союза // Известия Института инженерной физики. 2013. № 1. С. 56–64.
13. Нарышкин С. Е., Хабриева Т. Я., Абрамова А. И. и др. Научные концепции развития российского законодательства: Монография / Отв. ред. Т. Я. Хабриева, Ю. А. Тихомиров; 7-е изд. доп. и перераб. М. : «ИД Юриспруденция», 2015. 544 с.
14. Современное международное частное право в России и Евросоюзе. Кн. 1: Монография / Под ред. М. М. Богуславского, А. Г. Лисицына-Светланова, А. Трунка. М. : Норма, 2013. 656 с.
15. Lovtsov D. A. Effective methods of protection of the intellectual activity results in infosphere of global telematics networks // Открытое образование. 2016. № 5. С. 85–88.

THE DEVELOPMENT OF THE LEGAL REGULATION CONCEPT OF INTERNATIONAL INFORMATION EXCHANGE

Svetlana Chubukova, *Ph.D. in Law, assistant of Professor, Honored Teacher of the RF, assistant of Professor of chair of information law and digital technologies in Kutafin Moscow State Law University (MSAL).*
E-mail: *sgchubukova@msal.ru*

Keywords*: information society, information technology, information security, strategy of information society development, information and telecommunication networks, information legislation, society of knowledge, information sovereignty.*

Abstract.
Purpose of the paper: *the main directions of legal regulation of international information exchange concept*
Method used: *systematic analysis of legal regulation of international information exchange concept and the Russian information legislation.*
Results obtained: *Russia becomes a full participant of the global information society, but political independence, national identity and cultural traditions should be preserved. The solution of this problem requires the development of the legal regulation concept of international information exchange. The paper discusses the special principles of international information exchange, the problem of determining the informational state sovereignty, the problems of the subjects system of international information exchange and their legal status, the problem of recognition of electronic documents and electronic signatures for individuals and legal entities of foreign states.*
The provisions of this concept should be reflected in new Russia law on participation in international information exchange.

References

1. Vinogradova S. M., Mel'nik G. S. Problemy preodoleniia neravenstva v mezhdunarodnom informatsionnom obmene, Gumanitarnyi vektor, 2012, No. 2 (30), pp. 239-246.
2. Zakharov T. V. Mezhdunarodnoe sotrudnichestvo gosudarstv v sfere informatsionnoi bezopasnosti i pravovye podkhody k ego regulirovaniiu, Gosudarstvo i pravo v novoi informatsionnoi real'nosti: Sb. nauch. tr., otv. red. E. V. Alferova, D. A. Lovtsov, M. : INION RAN, 2018, pp. 119-134.
3. Efremov A. A. Elektronnoe pravitel'stvo i mezhdunarodnoe pravo, Trudy XIV Vserossiiskoi ob"edinennoi konferentsii "Internet i sovremennoe obshchestvo" (IMS-2011), SPb., 2011, p. 192.
4. Krasavin A. V. Problemy pravotvorchestva v sfere tekhnicheskogo regulirovaniia, Pravo i sovremennye gosudarstva, 2013, No. 6, pp. 52-63.
5. Krasikov D. V. Mezhdunarodno-pravovaia otvetstvennost' gosudarstv v kiberprostranstve, Gosudarstvo i pravo v novoi informatsionnoi real'nosti: Sb. nauch. tr., otv. red. E. V. Alferova, D. A. Lovtsov, M. : INION RAN, 2018, pp. 235-247.
6. Krasikov D. V. Territorial'nyi suverenitet i delimitatsiia iurisdiktsii v kiberprostranstve, Gosudarstvo i pravo v novoi informatsionnoi real'nosti: Sb. nauch. tr., otv. red. E. V. Alferova, D. A. Lovtsov, M. : INION RAN, 2018, pp. 235-247.
7. Lovtsov D. A. Problema effektivnosti mezhdunarodno-pravovogo obespecheniia global'nogo informatsionnogo obmena, Nauka i obrazovanie: khoziaistvo i ekonomika; predprinimatel'stvo; pravo i upravlenie, 2011, No. 11 (17), pp. 24-31.
8. Lovtsov D. A. Razvitie informatsionnoi sfery obshchestvenno-proizvodstvennoi deiatel'nosti: dostizheniia, ugrozy bezopasnosti i pravovoe regulirovanie, Gosudarstvo i pravo v novoi informatsionnoi real'nosti: Sb. nauch. tr., otv. red. E. V. Alferova, D. A. Lovtsov, M. : INION RAN, 2018, pp. 15-37.
9. Lovtsov D. A. Sistema printsipov effektivnogo pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere, Informatsionnoe pravo, 2017, No. 1, pp. 13-18.
10. Lovtsov D. A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia, M. : RGUP, 2016, 316 pp.
11. Lovtsov D. A. Obespechenie informatsionnoi bezopasnosti v rossiiskikh telematicheskikh setiakh, Informatsionnoe pravo, 2012, No. 4, pp. 3-7.
12. Lovtsov D. A., Loban A. V., Tsimbal V. A. Sistema informatsionnogo obespecheniia tekhnicheskogo regulirovaniia Tamozhennogo Soiuza, Izvestiia Instituta inzhenernoi fiziki, 2013, No. 1, pp. 56-64.
13. Naryshkin S. E., Khabrieva T. Ia., Abramova A. I. i dr. Nauchnye kontseptsii razvitiia rossiiskogo zakonodatel'stva : monografiia, otv. red. T. Ia. Khabrieva, Iu. A. Tikhomirov; 7-e izd. dop. i pererab., M. : ID Iurisprudentsiia, 2015, 544 pp.
14. Sovremennoe mezhdunarodnoe chastnoe pravo v Rossii i Evrosoiuze, kn. 1 : monografiia, pod red. M. M. Boguslavskogo, A. G. Lisitsyna-Svetlanova, A. Trunka, M. : Norma, 2013, 656 pp.
15. Lovtsov D. A. Effective methods of protection of the intellectual activity results in infosphere of global telematics networks, Otkrytoe obrazovanie, 2016, No. 5, pp. 85-88.

ПОНЯТИЕ КИБЕРПРОСТРАНСТВА И ОЧЕРЧИВАНИЕ ЕГО ТЕРРИТОРИАЛЬНЫХ КОНТУРОВ[1]

*Терентьева Л. В.**

Ключевые слова: *информационная сфера, информационное пространство, сеть Интернет, признаки, информационная инфраструктура, юрисдикция.*

Аннотация.

Цель: *выявление правовых и доктринальных подходов к определению понятий «сеть Интернет» и «киберпространство», а также решение юрисдикционного вопроса в отношении определенного сегмента киберпространства.*

Метод: *на основе сравнительного правового анализа правовых и доктринальных подходов к определению понятий «сеть Интернет» и «киберпространство» выявляются особенности содержания данных понятий и их соотношение; на основе формально-юридического метода исследования выявляются характерные признаки киберпространства, определяется его место в информационном пространстве, а также поднимается вопрос об установлении юрисдикции в отношении определенного сегмента киберпространства.*

Результаты: *обосновано распространение юрисдикции государства как на физический, материальный аспект киберпространства, представляющий собой определенную технологическую инфраструктуру (объекты информатизации, технические средства), так и на информацию в цифровой форме. Включение в информационную инфраструктуру РФ совокупности объектов информатизации, информационных систем, сетей связи, а также лишенных географических границ и пространственной протяженности сайтов в сети Интернет позволило заключить, что в Доктрине информационной безопасности РФ 2016 г. предпринята попытка «территориализации» определенного сегмента киберпространства в целях распространения на него юрисдикции государства. Показано, что понятие «киберпространство» по сравнению с понятием «сеть Интернет» включает в себя более широкий контур сетей связи, что обусловливает необходимость пополнения законодательного тезауруса данным термином, а также решения вопроса относительно очерчивания юрисдикции государства в отношении определенных сегментов киберпространства.*

DOI:10.21681/1994-1404-2018-4-66-71

Несмотря на разнообразные дискуссии, посвященные различным аспектам правового регулирования отношений в киберпространстве, сам термин «киберпространство», хотя и встречается в нормативных правовых актах, но содержательного определения не получил. На международном уровне данный термин фигурирует в Окинавской хартии[2] 2000 г., Конвенции о преступности в сфере компьютерной информации 2001 г. В национальном праве РФ широкое распространение получил термин «сеть Интернет», тогда как термин «киберпространство» не упоминается ни в одном внутреннем нормативном акте.

Термин «киберпространство» (от англ. *cyberspace*) представлено сочетанием двух частей «*cyber*» (в современном значении часто понимается как современная механическая технология[3]) и «*space*» (пространство). В характеристиках, которыми учеными наделяют киберпространство, как правило, отмечается его единый характер, неделимость, несводимость к границам *физического* пространства [6], их подвижность и изменчивость [10], отсутствие однозначной географической определенности [16], трансграничность, многомер-

[2] Хартия Глобального информационного общества // Дипломатический вестник. 2000. № 8. С. 51 — 56.

[3] Мацкевич И. М. Причины экономической преступности: Учеб. пособие. М.: «Проспект», 2017.

[1] Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта №18-29-16061 «Сетевое право в условиях сетевого общества: новые регуляторные модели».

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

E-mail: terentevamila@mail.ru

ность и отсутствие линейности, протяженности, физических параметров [2].

Что касается отсутствия однозначной географической определенности, то данный признак, как представляется, не вполне точно характеризует киберпространство, поскольку игнорируется определенная материальная база его функционирования, которой может являться та или иная технологическая инфраструктура в виде специального оборудования, сервера, компьютеров и др. В работе [10] содержание понятия киберпространства раскрывается в трех аспектах:

1) физический аспект киберпространства, который обусловлен тем, что его функционирование опирается на определенную технологическую инфраструктуру (хабы, серверы, компьютеры и др.);

2) информационный аспект киберпространства, представляющий собой совокупность бесчисленных информационных потоков в цифровой форме;

3) социальный аспект киберпространства, связанный с социальным взаимодействием в неосязаемой цифровой среде.

Отсутствие законодательного термина «киберпространство» переводит поиск его содержательных характеристик в научной доктрине. В литературе часто понятия сети Интернет и киберпространства синонимизируются [3, 4], хотя ряд авторов отмечает нелогичность отождествления киберпространства и Интернета в силу более широкого содержания первого понятия [9,10]. В то же время не во всех работах обозначается, в чем конкретно проявляется широкое содержание киберпространства. По мнению М.А. Федотова [16] только в подпункте 11 п. 2 ст. 1270 Гражданского кодекса РФ имеет место формула, в которой киберпространство определено имплицитно, через понятие «такого образа» доведения произведений до всеобщего сведения, при котором любой может получить доступ к произведениям «из любого места и в любое время по собственному выбору». Эта формула является фактически дословным воспроизведением нормы, содержащейся в ст. 8 Договора[4] Всемирной организации интеллектуальной собственности (ВОИС) по авторскому праву 1996 г. Как представляется, вышеуказанная формула не столько определяет само понятие киберпространства, сколько отображает специфику осуществления деятельности в нем.

В работе [9] представлено мнение Д. Менте [18], который под киберпространством[5] понимает конкретное место (точку) соединения между компьютерами, преобразовавшуюся в глобальное виртуальное сообщество, а сеть Интернет преимущественно определяет с функциональных позиций. При этом автор характеризует Интернет не только как объединение сетей и совокупность разнообразных сервисов, но и в качестве социальной структуры, объединяющей разных индивидуумов со всего мира — пользователей сети, распространителей информации, сервис-провайдеров и иных заинтересованных лиц.

В [7] киберпространство определяется через *техническую* базу, на основе которой оно функционирует. В состав данной базы автор включает совокупность программных средств, с помощью которых осуществляются обработка и передача информации. Помимо технической и технологической сущности киберпространства выделяется и *информационная база* [11], состоящая из потоков информации, которые люди передают друг другу посредством сетевых средств связи. Автор предлагает определять киберпространство как совокупность общественных отношений, возникающих в процессе использования функционирующей электронной компьютерной сети, складывающихся по поводу информации (информационных ресурсов), обрабатываемой с помощью ЭВМ и услуг информационного характера, предоставляемых с помощью ЭВМ и средств связи компьютерной сети, совокупность отношений, участвовать в которых можно только посредством ЭВМ и средств связи компьютерной сети. Автор специально не разграничивает киберпространство и сеть Интернет, но упоминает, что сеть Интернет представляет собой только один из видов компьютерных сетей (наряду, в частности, с глобальными телематическими сетями Релком, Ситек, *Sedab*, *Remart* и др. [13,14]). Отсюда можно заключить, что поскольку кибернетическое пространство создают также и обычные компьютерные сети внутри предприятия («интранет»), а также виртуальные сети, которые предназначены для соединения частных сетей различных компаний между собой («экстранет»), то, безусловно, можно сделать вывод о том, что понятие «киберпространство» шире понятия «сеть Интернет».

Наоборот, есть мнение[6], что поскольку киберпространство является свойством виртуального поля, которое может продуцироваться в инфраструктуре Интернета, определять термин «киберпространство» через понимание пространства не является конструктивным. Согласно этому мнению люди взаимодействуют с помощью элементов виртуального *интернет-поля*, а не киберпространства. Использовать понятие «киберпространство» предлагается в значении *интернет-пространства*, т.е. как юридический термин, обозначающий наличие национальной юрисдикции на некоторой территории. Как представляется, поскольку именно киберпространство включает в себя широкий контур сетей связи, следовательно, именно данный термин должен являться предметом обсуждения относительно очерчивания юрисдикции государства в отношении того или иного сегмента киберпространства.

[4] Для России Договор об авторском праве ВОИС вступил в силу с 5 февраля 2009 г.

[5] «Уникальный носитель, известный его пользователям как киберпространство, не находящийся на определённой территории, но доступный каждому в любой точке мира через Интернет» [18].

[6] Нестеров А. В. Интернет-поле VS киберпространства. URL: http://e-notabene.ru/nb/article_16743.html (дата обращения 21 ноября 2018 г.).

Вместе с тем, не смотря на отсутствие закрепления термина «киберпространство» в российском законодательстве, инициативы его определения имели место в проекте Концепции[7] стратегии кибербезопасности в РФ. В соответствии с данным Проектом предлагается рассматривать киберпространство как определенный, имеющий четкие границы элемент *информационного пространства* [11—14]. Тогда киберпространство можно определить как сферу деятельности в информационном пространстве, образованную совокупностью коммуникационных каналов сети Интернет и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства). В Проекте стратегии отмечена невозможность регулирования киберпространства исключительно на национальном уровне. В научной доктрине также были озвучены пожелания относительно заключения многосторонних международных договоров, содержащих унифицированные нормы и правила регулирования отношений в киберпространстве [8,17]. Но на сегодняшний день, исходя из современных политических реалий, пока не сложилось предпосылок для проведения такого рода работы на универсальном уровне, но есть возможности ее проведения на региональном уровне[8].

Если принимать во внимание указанный подход в проекте Концепции стратегии кибербезопасности в РФ как восприятие киберпространства в качестве части информационного пространства, то определенные содержательные признаки киберпространства можно выявить в Указах в Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы»[9] и «Об утверждении доктрины информационной безопасности Российской Федерации»[10]. Именно в данных Указах закреплены характерные признаки киберпространства, определено его место в информационной сфере, а также предложено решение вопроса об установлении юрисдикции в отношении определенного сегмента киберпространства.

Так Доктрина информационной безопасности включила киберпространство в *информационную сферу* [11—14], понимая под ней совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений. Как представляется, включение сети Интернет в информационную сферу может свидетельствовать и о включении киберпространства.

Что касается Указа Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы», то в нем не смотря на присутствие определений таких современных явлений как «интернет вещей», «облачные вычисления», «обработка больших данных» и др., сам термин «киберпространство» не обозначен. В данном Указе Президента *информационное пространство* определяется в качестве совокупности информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры. Доктринальные определения киберпространства как сферы деятельности в информационном пространстве [1], а также в качестве продукта функционирования любых информационно-коммуникационных технологий (в том числе и сети Интернет), к которым могут быть причислены и информационные ресурсы, и информационные системы, и необходимая *информационная инфраструктура* [10], позволяют отнести к информационному пространству и киберпространство.

Следует заметить, что в содержании определения «информационного пространства» в Указе Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы» включено немало терминов, которые либо закреплены в иных нормативных правовых актах, или же получили свои доктринальные толкования в отсутствие нормативно-правовых определений. Так, понятие *информационной системы* закреплено в Федеральном законе[11] «Об информации, информационных технологиях и защите информации» 2006 г., которая определена как совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Понятие *информационных ресурсов* имело место в утратившем силу Фе-

---

[7] Проект Концепции стратегии кибербезопасности РФ. URL: http://council.gov.ru/media/files/ 41d4b3dfbdb25cea8a73.pdf (дата обращения 21 ноября 2018 г.).

[8] Так, принимая во внимание, что работоспособность Интернета зависит, главным образом, от международной некоммерческой корпорации по распределению имен и адресов *ICANN*, которая находится в юрисдикции США, Совет безопасности России на заседании 26 октября 2018 г. поручил Минкомсвязи совместно с МИД России до 1 августа 2018 г. инициировать в рамках БРИКС (Бразилия, Россия, Индия, Китай и Южная Африка) обсуждение вопроса о создании для государств — участников объединения собственной «системы дублирующих корневых серверов доменных имен (*DNS*), независимой от контроля [международных организаций] *ICANN*, *IANA* и *VeriSign* и способной обслуживать запросы пользователей перечисленных стран на случай сбоев или целевых воздействий» — https://www.rbc.ru/technology_and_ media/28/11/ 2017/ 5a1c1db99a 794783ba546aca (дата обращения 1 декабря 2018 г.).

[9] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

[10] Указ Президента РФ от 5 декабря 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074..

[11] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; 2018; № 30. Ст. 4546.

деральном законе от 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации», под которыми понимались отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). В научном сообществе распространен более широкий подход к этим понятиям [5, 11—15].

Что касается *информационной инфраструктуры*, то данное определение представлено в Доктрине информационной безопасности 2016 г., которая обозначает информационную инфраструктуру РФ как совокупность объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории РФ, а также на территориях, находящихся под юрисдикцией РФ или используемых на основании международных договоров РФ.

Вышеуказанные определения, содержащиеся в Указах Президента РФ, представляют определенную сложность для восприятия. Так, информационные системы фактически дважды присутствуют и в понятии информационного пространства, представленного в Указе Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы», и в качестве содержательного элемента в определениях информационной инфраструктуры и информационной сферы, развернутые понятия которых представлены в Доктрине информационной безопасности 2016 г.

Кроме того, включение в содержание понятия информационной инфраструктуры сайтов в сети Интернет фактически дублирует содержание понятия информационных ресурсов, содержащееся в понятии информационного пространства, поскольку сайты в сети Интернет можно отнести к массивам документов в информационных системах.

Что касается «объектов информатизации», то в законодательстве не отражено, какой объем вкладывается в содержание данного понятия, что обусловливает обращение к Доктрине и глоссарию[12] терминов информационной безопасности, где данное понятие представляет собой совокупность информационных ресурсов, средств и систем информатизации, используемых в соответствии с заданной информационной технологией, и систем связи вместе с помещениями, в которых они установлены. Как представляется, объекты информатизации можно также представить в виде центра обработки данных, которые в Распоряжении Правительства РФ от 7 октября 2015 г. № 1995-р определены в качестве здания или части здания, предназначенные для размещения технических и технологических средств, обеспечивающих обработку данных), обеспеченная собственной информационно-телекоммуникационной инфраструктурой. Таким образом, фактически определение «объекты информатизации» включает в себя элементы, которые также содержатся в вышеуказанных нормативных понятиях «информационная инфраструктура», «информационные системы» и др.

Интерес вызывает определение *информационной инфраструктуры*, представленное в Доктрине информационной безопасности РФ. Именно данное определение нормативно обозначило сферу распространения юрисдикции и в отношении киберпространства. Доктрина информационной безопасности фактически придала территориальное значение совокупности объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, посредством определения их местонахождения на территории РФ, а также на территориях, находящихся под юрисдикцией Российской Федерации. Заметим, что *территориальный* аспект информационной инфраструктуры ранее выделялся и в научной доктрине. Так, в [11—14] информационная инфраструктура определяется как совокупность автоматизированных информационных систем, коммуникаций (информационно-компьютерные телекоммуникационные — телематические сети) и информационных ресурсов (библиотек, архивов, хранилищ и баз данных и знаний и др.), находящихся в ведении государства.

В соответствии с Доктриной об информационной безопасности под понятие информационной инфраструктуры РФ подпадают все объекты информатизации и информационные системы, под которыми в законе об информации понимается совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Таким образом, физическое оборудование, включая серверы, находящиеся на территории РФ, а также информация, которая поддерживается данным оборудованием, охватывается юрисдикцией РФ. Данный документ фактически провозгласил[13] суверенитет России в информационном пространстве в качестве одного из основных направлений информационной безопасности.

Таким образом, юрисдикция государства распространяется как на физический, материальный аспект киберпространства, представляющий собой определенную технологическую инфраструктуру (объекты информатизации, технические средства), так и на информацию в цифровой форме. Включение в информационную инфраструктуру РФ совокупности объектов информатизации, информационных систем, сетей связи, а также лишенных географических границ и пространственной протяженности сайтов в сети Интернет, позволяет заключить, что в Доктрине информационной безопасности РФ предпринята попытка «террито-

[12] Общие вопросы технической защиты информации — https://www.intuit.ru/studies/courses/2291 /591/lecture/12689 (дата обращения 1 декабря 2018 г.); Техническая защита информации. Основные термины и определения: рекомендации по стандартизации Р 50.1.056 — 2005. М.: Изд-во стандартов, 2005. С. 105.

[13] См., например: Добрикова Е. Кибербезопасность и цифровой суверенитет: стимул или препятствие для развития IT-рынка? // Гарант.ру. Информационно-правовой портал: Аналитические статьи. 2017. 2 мар. URL: http://www.garant.ru/article/1095177/

риализации» определенного сегмента киберпространства в целях распространения на него юрисдикции государства. При этом следует заметить, что понятие «киберпространство» по сравнению с понятием «сеть Интернет» включает в себя более широкий контур сетей связи, что обусловливает необходимость пополнения законодательного тезауруса данным термином, а также решения правового вопроса относительно очерчивания юрисдикции государства в отношении того или иного сегмента киберпространства.

Рецензент: ***Марков Алексей Сергеевич,*** *доктор технических наук, профессор кафедры ИУ-7 МГТУ им. Н.Э. Баумана, главный редактор журнала «Вопросы кибербезопасности», г. Москва, Россия.*
E-mail: *a.markov@npo-echelon.ru*

Литература

1. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5. С. 39—42.
2. Ансельмо Э. Л. Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве? // Экономические стратегии. 2006. Т. 8. № 2. С. 24—31.
3. Афанасьева В. В. Тотальность виртуального. Саратов, 2005.
4. Браже Р. А. Синергетика и творчество. Ульяновск, 2001.
5. Ващекин А. Н., Ващекина И. В. Информационное право: прикладные задачи и математические методы // Информационное право. 2017. № 3. С. 17—21.
6. Войниканис Е. А. Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М. : ИД «Юриспруденция», 2013.
7. Грибанов Д. В. К вопросу о правовой теории кибернетического пространства // Государство и право. 2010. № 4. С. 57—62.
8. Даниленков А. В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети «Интернет» // Lex Russica. 2017. № 7. С. 154—165.
9. Дашян М. С. Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет. М. : «Волтерс Клувер», 2007. 248 с.
10. Добринская Д. Е. Киберпространство: территория современной жизни // Вестник Московского Университета. Сер. 18. Социология и политология. 2018. Т. 24. № 1. С. 52—70.
11. Ловцов Д. А. Информационная теория эргасистем: Тезаурус. М. : РАН. Наука, 2005. 248 с.
12. Ловцов Д. А. Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере // Информационное право. 2015. № 2. С. 8—13.
13. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере: Монография. М. : РГУП, 2016. 316 с.
14. 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.
15. Ловцов Д. А., Ниесов В. А. Формирование единого информационного пространства судебной системы России // Российское правосудие. 2008. № 11. С. 78—88.
16. Федотов М. А. Конституционные ответы на вызовы киберпространства // Lex Russica. 2016. № 3. С. 164—182.
17. Федотов М. А. Конституция как уходящая натура доцифровой эпохи: Доклад на IX Междунар. конф. «Право и Интернет». URL: http://www.ifap.ru/pi/09 (дата обращения 21 ноября 2018 г.).
18. Menthe D. C. Jurisdiction in cyberspace: A theory of international spaces // Michigan Telecommunications and Technology Law Review. 1998. Vol. 4. Pp. 69—103. http://www.mttlr.org/volfour/menthe.pdf (дата обращения 21 ноября 2018 г.).

THE CONCEPT OF CYBERSPACE AND OUTLINING ITS TERRITORIAL CONTOURS

Liudmila Terent'eva, *Ph.D. (Law), Associate Professor at the Department of International Private Law of Kutafin Moscow State Law University, Moscow, Russian Federation.*
E-mail: *terentevamila@mail.ru*

Keywords: *information sphere, information space, Internet network, attributes, information infrastructure, jurisdiction.*

Abstract.

Purpose of the paper: *identifying legal and doctrinal approaches to defining the concepts of the Internet network u cyberspace as well as resolving the issue of jurisdiction as regards a certain segment of cyberspace.*

Method of study: *based on the comparative legal analysis of legal and doctrinal approaches to defining the concepts of Internet network u cyberspace, specific features of the content of these concepts and their correlation are identified; based on the formal juridical method of study, characteristic features of cyberspace are identified, the place cyberspace takes in the information space is determined, and the issue of establishing jurisdiction over a certain segment of cyberspace.*

Results obtained: *a justification is given for extending the jurisdiction of the state over the physical, material aspect of cyberspace being a certain technological infrastructure (informatisation objects, technical means) as well as over information in digital form. Including informatisation objects, information systems, telecommunication networks, and websites on the Internet network having no geographical boundaries and spatial extents in the information infrastructure of the Russian Federation allowed to conclude that an attempt at "territorialisation" of a certain segment of cyberspace has been made in the 2016 Doctrine of Information Security of the Russian Federation, with a view to extend the jurisdiction of the state over it. It is shown that the concept of cyberspace, as compared with that of the Internet network, includes a broader contour of telecommunication networks which leads to a need for including this term in the law-making thesaurus as well as for resolving the issue of outlining the jurisdiction of the state as regards certain segments of cyberspace.*

References

1. Alpeev A. S. Terminologiia bezopasnosti: kiberbezopasnost', informatsionnaia bezopasnost', Voprosy kiberbezopasnosti, 2014, No. 5, pp. 39-42.
2. Ansel'mo E. L. Kiberprostranstvo v mezhdunarodnom zakonodatel'stve: oprovergaet li razvitie Interneta printsip territorial'nosti v mezhdunarodnom prave?, Ekonomicheskie strategii, 2006, t. 8, No. 2, pp. 24-31.
3. Afanas'eva V. V. Total'nost' virtual'nogo. Saratov, 2005.
4. Brazhe R. A. Sinergetika i tvorchestvo. Ul'ianovsk, 2001.
5. Vashchekin A. N., Vashchekina I. V. Informatsionnoe pravo: prikladnye zadachi i matematicheskie metody, Informatsionnoe pravo, 2017, No. 3, pp. 17-21.
6. Voinikanis E. A. Pravo intellektual'noi sobstvennosti v tsifrovuiu epokhu: paradigma balansa i gibkosti, M. : ID "Iurisprudentsiia", 2013.
7. Gribanov D. V. K voprosu o pravovoi teorii kiberneticheskogo prostranstva, Gosudarstvo i pravo, 2010, No. 4, pp. 57-62.
8. Danilenkov A. V. Gosudarstvennyi suverenitet Rossiiskoi Federatsii v informatsionno-telekommunikatsionnoi seti "Internet", Lex Russica, 2017, No. 7, pp. 154-165.
9. Dashian M. S. Pravo informatsionnykh magistralei (Law of information highways): voprosy pravovogo regulirovaniia v sfere Internet, M. : "Wolters Kluwer", 2007, 248 pp.
10. Dobrinskaia D. E. Kiberprostranstvo: territoriia sovremennoi zhizni, Vestnik Moskovskogo Universiteta, ser. 18. Sotsiologiia i politologiia, 2018, t. 24, No. 1, pp. 52-70.
11. Lovtsov D. A. Informatsionnaia teoriia ergasistem : tezaurus, M. : RAN. Nauka, 2005, 248 pp.
12. Lovtsov D. A. Lingvisticheskoe obespechenie pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere, Informatsionnoe pravo, 2015, No. 2, pp. 8-13.
13. Lovtsov D. A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia, M. : RGUP, 2016. 316 pp.
14. Lovtsov D. A. Razvitie informatsionnoi sfery obshchestvenno-proizvodstvennoi deiatel'nosti: dostizheniia, ugrozy bezopasnosti i pravovoe regulirovanie, Gosudarstvo i pravo v novoi informatsionnoi real'nosti: sb. nauch. tr., otv. red. E. V. Alferova, D. A. Lovtsov, M. : INION RAN, 2018, pp. 15-37.
15. Lovtsov D. A., Niesov V. A. Formirovanie edinogo informatsionnogo prostranstva sudebnoi sistemy Rossii, Rossiiskoe pravosudie, 2008, No. 11, pp. 78-88.
16. Fedotov M. A. Konstitutsionnye otvety na vyzovy kiberprostranstva, Lex Russica, 2016, No. 3, pp. 164-182.
17. Fedotov M. A. Konstitutsiia kak ukhodiashchaia natura dotsifrovoi epokhi : doklad na IX Mezhdunar. konf. "Pravo i Internet", URL: http://www.ifap.ru/pi/09 (data obrashcheniia 21 noiabria 2018 g.).
18. Menthe D. C. Jurisdiction in cyberspace: A theory of international spaces, Michigan Telecommunications and Technology Law Review. 1998. Vol. 4. Pp. 69-103, URL: http://www.mttlr.org/volfour/menthe.pdf (data obrashcheniia 21 noiabria 2018 g.).

РЕЗУЛЬТАТЫ ФОРСАЙТ-СЕССИИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В XXI ВЕКЕ: ВЫЗОВЫ И ПРАВОВОЕ РЕГУЛИРОВАНИЕ» РОССИЙСКОЙ АКАДЕМИИ НАУК

*Полякова Т. А.**

Ключевые слова: *информационные угрозы и вызовы правовое обеспечение, международное сотрудничество, международная информационная безопасность, юридическая ответственность, приоритетные направления.*

Аннотация.

Цель: *гармонизация научно-прикладных подходов к созданию системы правового регулирования информационной безопасности.*

Метод: *системный анализ основных направлений и тенденций науки информационного права в развитии правового обеспечения информационной безопасности.*

Результаты: *в ходе обсуждения на предварительной (форсайт) сессии Института государства и права Российской академии наук «Информационная безопасность в XXI веке: вызовы и правовое регулирование», прошедшей 27 сентября 2018 г., были выявлены и проанализированы причины, обусловливающие необходимость особого внимания со стороны, как правовой науки, так и законодателя к проблемам правового обеспечения информационной безопасности. Были определены перспективные приоритетные направления разработки правового обеспечения информационной безопасности с учетом реализации Стратегии научно-технологического развития.*

Обоснована потребность в универсальных, междисциплинарных, сложноорганизованных механизмах правового регулирования и обеспечения информационной безопасности, учитывающих закономерности трансформации современного права в комплексной его связи с техническими, моральными и корпоративными нормами.

DOI: 10.21681/1994-1404-2018-4-72-76

В Институте государства и права Российской академии наук 27 сентября 2018 г. прошла первая форсайт-сессия «Информационная безопасность в XXI веке: вызовы и правовое регулирование», организованная сектором информационного права и международной информационной безопасности. В ней приняли участие представители юридической науки, органов исполнительной власти, финансовой сферы и банковского сообщества, научных и образовательных организаций из России и зарубежных стран. *Главная задача* мероприятия заключалась в интеллектуальной мобилизации усилий для выработки новых подходов к гармонизации и комплексному регулированию отношений, возникающих в связи с цифровым развитием, а также к формированию национальных стратегических программных документов и новой регуляторной среды, обеспечивающей благоприятный правовой режим развития современных информационных технологий.

В качестве *основных тем* для обсуждения участникам форсайт-сессии были предложены [1]: информация в системе объектов гражданских прав и публичных правоотношений; выработка государственной политики и обеспечение государственной защиты интересов российских граждан в информационной сфере в условиях развития цифровой экономики и глобализации, будущее и проблемы правового регулирования робототехники, обеспечение прав граждан на доступ к информации и факторы криминализации распространения цифровых данных, вопросы юридической ответственности, государственного суверенитета и юрисдикции в эпоху постиндустриальной экономики; проблемы и перспективы формирования системы международной информационной безопасности, зарубежные тенденции и подходы [2, 3] к правовому обеспечению информационной безопасности.

* ***Полякова Татьяна Анатольевна,*** *доктор юридических наук, доцент, заслуженный юрист Российской Федерации главный научный сотрудник, и.о. заведующего сектором информационного права и международной информационной безопасности Института государства и права Российской академии наук, г. Москва, Россия.*

E-mail: polyakova_ta@mail.ru

С основным докладом выступил врио директора Института государства и права РАН, член-корреспондент РАН, доктор юридических наук, профессор, заслуженный юрист Российской Федерации **А. Н. Савенков**. В докладе был затронут широкий спектр проблем – от правового регулирования современной ИКТ-среды и обеспечения ее информационной безопасности до регулирования импортозамещения и развития научно-технического потенциала Российской Федерации в области развития ИКТ. Он проанализировал развитие *правового обеспечения* информационной безопасности в условиях глобального информационного общества и цифровой экономики. Особое внимание докладчик уделил проблемам развития цифрового государства, включая «цифровизацию» в области государственного управления, судопроизводства и осуществления правосудия, нотариата, банковской и финансовой сфер. В частности, были рассмотрены проблемы развития технологии «блокчейн», мировые тенденции регулирования криптовалюты, в том числе проблемы и перспективы регулирования использования биткоинов в России и в мире. Было отмечено особое значение современных фундаментальных научных исследований, связанных с трансформацией права в условиях развития цифровой экономики, необходимостью разработки международных документов, направленных на выявление, изучение рисков, вызовов и угроз информационной безопасности, противодействие информационной преступности, особенно киберпреступности. То, что Интернет используется международными преступными синдикатами для совершения различных противоправных действий в информационной сфере, делает уязвимым практически любого человека, а это, в свою очередь, обусловливает сложный субъектный состав правонарушения и ставит на повестку дня вопросы юрисдикции и экстерриториальности. А.Н. Савенков отметил, что Россия ведет активную работу по подготовке проектов международных документов в сфере киберпреступлений. В 2011 г. Российской Федерацией предложен проект конвенции ООН «Об обеспечении международной информационной безопасности». К сожалению, вопрос о рассмотрении данного документа не был озвучен на уровне Генеральной Ассамблеи ООН. В связи с этим трудно прогнозировать позитивный результат и надеяться на успех в достижении международных договоренностей по информационной безопасности в киберпространстве.

Вопрос о базовых принципах правового обеспечения информационной безопасности в условиях формирования и развития киберпространства, его трансграничности имеет не только научное, но и практическое значение. Масштаб и технологический уровень деструктивного использования ИКТ неуклонно возрастает. При этом отсутствие необходимой международно-правовой базы, регулирующей деятельность государств в этой сфере, значительно осложняет ситуацию.

Первый заместитель директора Департамента информационной безопасности Банка России **А. М. Сычев** в своем выступлении отметил особую роль правового регулирования в условиях внедрения цифровых технологий в банковской сфере, а также с проблемой определения ответственности за принятие такого рода решений. В связи с этим *приоритетными* для научных исследований и регулирования в банковской сфере являются обоснование требований к информационной безопасности и разработка стандартов, упрощающих выявление компьютерных инцидентов. Особое внимание следует также уделять проблемам аутсорсинга в банковской сфере при оказании различных услуг, а также развития криптовалюты в условиях глобализации.

Старший научный сотрудник ИГП РАН кандидат юридических наук, доцент **В. Б. Наумов** остановился на проблемах научных исследований и тенденциях развития нормативного правового регулирования отношений в области робототехники в России и за рубежом. Имеет место проблема технологического расслоения и различий между странами, связанных с обработкой больших данных и принятием управленческих решений на их основе. В докладе было обращено внимание на необходимость развития фундаментальных правовых исследований и важность междисциплинарного подхода к решению проблем, связанных с массовым внедрением робототехники, в частности, проблем морали и нравственности, неизбежно возникающими при эксплуатации робототехники. Докладчик также указал на основные подходы к регулированию отношений в области киберфизических систем в иностранных юрисдикциях и констатировал, что механизмы такого регулирования только формируются. С одной стороны, это позволяет беспрепятственно разрабатывать и использовать киберфизические системы. С другой стороны, остаются открытыми вопросы безопасности, ответственности, охраны общественного порядка, защиты прав потребителей и др.

Начальник управления Государственного секретариата Совета Безопасности Республики Беларусь доктор юридических наук **О. С. Макаров** в своем докладе затронул актуальные вопросы развития цифровой экономики в Республике Беларусь, а также указал на тенденции развития «цифровой песочницы», криптовалюты, проблему обучения инженеров и программистов в международных *IT*-компаниях. Он отметил особое значение для науки такого предмета исследования, как правовое обеспечение информационной безопасности, и поддержал идею разработки международных документов о противодействии преступности и криминализации информационной сферы.

Исполнительный вице-президент по взаимодействию с органами государственной власти ПАО «ВымпелКом» **М. В. Якушев** в своем выступлении акцентировал внимание на вопросах *правового обеспечения* информационной безопасности и кодификации информационного законодательства в рамках программы «Цифровая экономика». Для обеспечения информационной безопасности существенное значение имеют вопросы доверия в информационной сфере, междуна-

родного сотрудничества, развития координационных механизмов наряду с запретительными. Были затронуты также проблемы развития корпоративных информационных норм и совершенствования образовательных программ в данной сфере, подчеркнута важность унификации терминологии, принятия технических нормативных правовых актов в сфере информационной безопасности.

Директор Российского фонда фундаментальных исследований **О. В. Белявский** охарактеризовал приоритетные направления фундаментальных исследований в условиях развития цифровой экономики, вопросы государственной политики, направленной на реализацию Стратегии научно-технологического развития Российской Федерации, новые полномочия Российской академии наук по координации фундаментальных исследований. Особое внимание О.В. Белявский обратил на фундаментальные исследования проблем регулирования цифровой экономики и искусственного интеллекта, отметив объективную необходимость укрепления международного сотрудничества при проведении фундаментальных исследований в данных областях. Современная наука обладает трансграничным характером развития, ни одно сколько-нибудь значимое и масштабное фундаментальное исследование, будь то проекты в естественных, технических или гуманитарных науках, не может быть проведено в административных границах одного государства. Информационные, финансовые, человеческие и прочие ресурсы в современном мире достаточно свободно перетекают из одного региона в другой, это же касается товаров, работ и услуг. Наука, не будучи изолирована от общемировых тенденций, также «глобализуется» и приобретает цифровую форму. Другая закономерность эволюции научной сферы состоит в возрастающей междисциплинарности. Как правило, любой крупный проект, как научный, так и научно-технологический, требует сотрудничества множества различных специалистов – от инженеров до психологов. К сожалению, имеют место и отрицательные тенденции, в основе которых лежат чисто субъективные факторы. Так, в сфере производства научных знаний и их последующей коммерциализации в настоящее время обозначилась общемировая гегемония стран Запада, прежде всего, США и Великобритании.

Негативное отношение некоторых представителей политической эли- ты данных стран к России влечет за собой отрицательные последствия и для научного сотрудничества: поиск объективной истины подменяется геополитическими интересами, а образ российского общества в целом и ученых в частности искажается (огромную роль здесь играют СМИ). Таким образом, имеет место как возрастание международной конкуренции (отнюдь не всегда добросовестной), так и угроз конфликтов, глобальной и региональной нестабильности. В такой ситуации необходимость поддержки отечественных исследователей становится еще более насущной.

Выступление заместителя директора Института проблем информационной безопасности МГУ им. М.В. Ломоносова доктора юридических наук, доктора технических наук, профессора **А. А. Стрельцова** было посвящено *правовым проблемам* международной информационной безопасности. Особое внимание докладчик обратил на обеспечение государственного суверенитета и международного сотрудничества в данной сфере в рамках ООН. Он отметил важную роль ИКТ-среды, как искусственной среды и юридической фикции, к которой применяется тот же подход, что и к традиционным суверенным «пространствам», таким как государство. Были также сформулированы проблемы объективизации компьютерных инцидентов и их расследования, требующие фундаментального научного обеспечения.

В результате состоявшейся в рамках форсайт-сессии научной дискуссии были определены, в частности, следующие ключевые *направления научных исследований* по вопросам правового обеспечения информационной безопасности:

- правовые методы обеспечения единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры Российской Федерации на всех уровнях информационного пространства;
- правовое обеспечение функционирования российского сегмента сети «Интернет»;
- правовые аспекты независимости и безопасности функционирования аппаратных средств и инфраструктуры обработки данных, устойчивости и безопасности функционирования информационных систем и технологий;
- правовой режим и технические инструменты функционирования сервисов и использования данных;
- правовой режим межмашинного взаимодействия для киберфизических систем;
- правовой режим функционирования машинных и когнитивных интерфейсов;
- организационно-правовые инструменты, обеспечивающие защиту государственных интересов, безопасное информационное взаимодействие граждан;
- эффективные механизмы государственного регулирования и поддержки в условиях интеграции в международную экономику;
- правовые основы для построения доверенной среды Евразийского экономического союза, обеспечивающей коллективную информационную безопасность;
- участие России в подготовке и реализации международных документов по вопросам информационной безопасности.

Подводя итоги работы первой форсайт-сессии и.о. заведующего сектором информационного права и международной информационной безопасности ИГП РАН доктор юридических наук **Т. А. Полякова** отметила продуктивность проведенного научного форума, по-

зволившего «взглянуть» в будущее научных исследований в информационной сфере, сфере развития информационного права, межотраслевого взаимодействия и международного сотрудничества. Апробированная новая форма «мозгового штурма и коллективной генерации идей» позволила определить общие подходы и приоритетные направления разработки правового обеспечения информационной безопасности с учетом реализации Стратегии научно-технологического развития. С целью координации межведомственных фундаментальных научных исследований в сфере цифровой экономики, искусственного интеллекта и международной информационной безопасности планируется создание Центра экспертно-правовых исследований информационных процессов и обеспечения информационной безопасности ИГП РАН.

Литература

1. Полякова Т. А., Минбалеев А. В., Наумов В. Б. Форсайт-сессия «Информационная безопасность в XXI веке: вызовы и правовое регулирование» // Труды Института государства и права РАН. 2018. Т. 13. № 5. С. 194–208.
2. Полякова Т. А., Стрельцов А. А., Ниесов В. А., Чубукова С. Г. Организационное и правовое обеспечение информационной безопасности // Под ред. Т. А. Поляковой, А. А. Стрельцова. М. : Юрайт, 2016. 325 с.
3. Стратегия национального развития и задачи юридической науки : монография / Бурмистрова Е.С., Ващекин А. Н., Ловцов Д. А., Ниесов В. А., Полякова Т. А, Чубукова С. Г. и др. Под общ. ред. Ю. Л. Васильченко, И. М. Рассолова, С. Г. Чубуковой. М. : РЭУ им. Г. В. Плеханова, 2016. 316 с.

RESULTS OF FORESIGHT SESSION: “INFORMATION SECURITY IN THE 21ST CENTURY: CHALLENGES AND LEGAL REGULATION”OF RUSSIAN SCIENCE ACADEMY

Tatyana Polyakova, *Doctor of Legal Sciences, Associate Professor, Honored jurist of the RF, Chief Research Fellow, Acting Head of the Information Law and International Information Security Department, Institute of State and Law, Russian Academy of Sciences Russian Federation, Moscow.*

E-mail: *polyakova_ta@mail.ru*

Keywords: *session, information threats and challenges, information security, legal regulation, legal support, international cooperation, international information security, legal liability, priority trends*

Abstract.

Purpose*: the harmonization of science and applied approaches to the creation of system of legal regulation of information security.*

Метод*: the system analysis of the basic directions and trends in the science of information law in the development of legal support of information security.*

Results*: in the course of discussion at the foresight session in the Institute of the State and Law of Russian Academy of Sciences “Information security in the 21st century: challenges and legal regulation” was held on September 27, 2018 causes stipulating the need for special attention from legal science and legislator to the issues of legal regulation of information security have been identified and analyzed. Furthermore, the prospective priority trends in development of legal regulation of information security with regard to implementation of the Strategy of scientific and technological development have been reviewed during the foresight session.*

The necessary for universal, interdisciplinary, complexly organized mechanisms of legal regulation and provision of information security with due regard to the patterns of transformation of contemporary law in its comprehensive interrelation with technical, moral and corporate standards is defined.

References

1. Poliakova T. A., Minbaleev A. V., Naumov V. B. Forsait-sessiia "Informatsionnaia bezopasnost' v XXI veke: vyzovy i pravovoe regulirovanie", Trudy Instituta gosudarstva i prava RAN, 2018, t. 13, No. 5, pp. 194-208.
2. Poliakova T. A., Strel'tsov A. A., Niesov V. A., Chubukova S. G. Organizatsionnoe i pravoe obespechenie informatsionnoi bezopasnosti, pod red. T. A. Poliakovoi, A. A. Strel'tsova, M. : Iurait, 2016, 325 pp.
3. Strategiia natsional'nogo razvitiia i zadachi iuridicheskoi nauki : monografiia, Burmistrova E.S., Vashchekin A. N., Lovtsov D. A., Niesov V. A., Poliakova T. A, Chubukova S. G. i dr., pod obshch. red. Iu. L. Vasil'chenko, I. M. Rassolova, S. G. Chubukovoi, M. : REU im. G. V. Plekhanova, 2016, 316 pp.