Том 13, 2016, № 6
Vol. 13, 2016, No. 6

ISSN: 1812-5220

Научно-практический журнал

Проблемы анализа риска

Scientific and Practical Journal

Issues of Risk Analysis

Главная тема номера:

Информационная безопасность и риски Брекзита

Volume Headline:

Information safety and Brexit risks

9 771812 522004

Официальное издание Экспертного совета МЧС России и Российского научного общества анализа риска
Official Edition of the Expert Council of EMERCOM of Russia and Russian Scientific Society for Risk Analysis

Том 13, 2016, № 6
Vol. 13, 2016, No.6

ISSN: 1812-5220

Научно-практический журнал

Проблемы анализа риска

Scientific and Practical Journal

Issues of Risk Analysis

Общероссийская общественная организация
«Российское научное общество анализа риска»

ФГБУ «Всероссийский научно-исследовательский
институт по проблемам гражданской обороны
и чрезвычайных ситуаций МЧС России» (ФЦ)

Финансовый издательский дом
«Деловой экспресс»

Содержание

О проектах новых документов Российского научного общества анализа риска

ISSN 1812-5220

А. А. Быков,
Главный редактор

Уважаемые коллеги!

29 ноября 2016 г. состоялось расширенное заседание Президиума Российского научного общества анализа риска, на котором помимо рабочих вопросов об итогах деятельности Общества были рассмотрены проекты двух новых документов Общества — Декларации Российского научного общества анализа риска «О дальнейшем развитии в Российской Федерации теории и практики оценки и управления рисками в области природной и техногенной безопасности» и Концепции Российского научного общества анализа риска «О направлениях деятельности по совершенствованию и развитию государственно-общественной системы управления защитой населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера».

Как указано в преамбуле к Декларации:

«Принимая во внимание, что:

• первая четверть XXI века характеризуется такими трендами, угрожающими безопасности населения, как:

– повышение риска аварий и катастроф;

– возрастание рисков трансграничных чрезвычайных ситуаций;

– возрастание хаоса и сложности решения первоочередных задач защиты населения;

• Россия ежегодно сталкивается с угрозами природного и техногенного характера, представляющими угрозу национальной безопасности Российской Федерации;

• на современном этапе наиболее значимыми факторами, способствующими возрастанию риска ЧС на территориях субъектов и муниципальных образований Российской Федерации, являются:

– повышение плотности населения, в результате чего происходит чрезмерная эксплуатация земель и коммуникаций, ведется застройка территорий, подверженных угрозам различного характера;

– концентрация на ограниченных площадях потенциально опасных производственных мощностей с большой стоимостью основных фондов;

– размещение потенциально опасных объектов в населенных пунктах с большой плотностью населения;

– старение основных производственных фондов промышленных предприятий, инфраструктуры и жилых зданий;

– недостаточная эффективность систем управления на местах, слабое участие заинтересованных сторон на местном уровне в процессах управления рисками ЧС;

– недостаточная координация между аварийно-спасательными службами, снижающая возможность быстрого реагирования и обеспечения готовности сил ликвидации ЧС;

– деградация экосистем в результате деятельности человека;

– неблагоприятные последствия изменения климата, влияющие на частоту возникновения стихийных бедствий;

• в зоне воздействия поражающих факторов чрезвычайных ситуаций природного и техногенного характера в России проживает более 100 миллионов человек;

• одним из главных приоритетов выживания и устойчивого социально-экономического развития Российской Федерации является умение оценивать наиболее существенные риски и способность через управление рисками парировать связанные с ними угрозы и опасности;

• эффективное снижение рисков чрезвычайных ситуаций возможно только при создании межведомственной и междисциплинарной системы оценки и управления рисками чрезвычайных ситуаций;

• одной из основных задач деятельности Общероссийской общественной организации "Российское научное общество анализа риска" является выработка предложений по установлению, достижению и поддержанию допустимых уровней риска, характеризующих вероятность нанесения ущерба жизни и здоровью населения, при воздействии поражающих факторов — источников природных, техногенных, биолого-социальных чрезвычайных ситуаций.

Общероссийская общественная организация "Российское научное общество анализа риска" провозглашает настоящую Декларацию "О дальнейшем развитии в Российской Федерации теории и практики оценки и управления рисками чрезвычайных ситуаций природного и техногенного характера", к выполнению которой предлагает присоединиться всем федеральным органам исполнительной власти, органам исполнительной власти субъектов Российской Федерации, органам местного самоуправления, организациям (учреждениям), а также специалистам, осуществляющим деятельность в области оценки и управления рисками чрезвычайных ситуаций природного и техногенного характера.

По Декларации Общества Решением Президиума поручено Научно-техническому совету и Исполнительному комитету Общества:

• в период с января по апрель 2017 года организовать проведение рассмотрения Декларации с участием общественных организаций, работающих в области анализа риска, для возможного придания ему междисциплинарного статуса;

• подготовить программу реализации Декларации для рассмотрения и принятия на предстоящей в 2017 году отчетно-выборной конференции Российского научного общества анализа риска в рамках целевой программы Российского научного общества анализа риска от 24 марта 2016 года "Развитие государственно-общественной системы оценки и анализа риска, совершенствование подготовки и обучения населения и специалистов в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера"».

Как указывается в Концепции: «Риски — неизбежное условие жизни, проблемы обществ и государств. Один из главных приоритетов выживания и успешного развития человечества — умение прогнозировать и оценивать наиболее существенные риски, в том числе риски чрезвычайных ситуаций, и способность парировать угрозы и опасности, связанные с этими рисками. Это важнейшая задача не только науки и техники, но и государства, и каждого человека, осуществляющего свою жизнедеятельность в условиях, подверженных рискам чрезвычайных ситуаций».

Концепция представляет собой систему взглядов Общества на становление и развитие государственно-общественной системы управления защитой населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера. Она призвана способствовать расширению общественного участия в защите населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера, росту влияния общества на обеспечение безопасной среды жизнедеятельности для населения, открытости системы управления рисками чрезвычайных ситуаций.

По Концепции Общества Решением Президиума поручено Научно-техническому совету и Исполнительному комитету:

• в первом квартале 2016 г. подготовить Концепцию и пояснительную записку к ней для внесения в Федеральное Собрание, Государственную Думу Российской Федерации, Правительство Российской Федерации, соответствующие федеральные органы исполнительной власти и общественные организации;

• подготовить план по дальнейшей реализации данного документа до 30 марта 2017 г. и вынести его на рассмотрение предстоящей в 2017 г. отчетно-выборной конференции Российского научного общества анализа риска.

Оба документа решено опубликовать на сайте Общества sra-russia.ru, и после доработки они будут опубликованы на страницах нашего журнала.

УДК 338.24

ISSN 1812-5220

Новый вид рисков — риски киберпространства

Ю. И. Соколов,
ФГУ ВНИИ ГОЧС (ФЦ) МЧС России, 6 Центр,
г. Москва

Аннотация

В статье рассматриваются вопросы риска использования киберпространства при автоматизации управления промышленными объектами, критически важными объектами и в работе органов управления, а также обеспечения кибербезопасности.

Ключевые слова: Интернет, киберпространство, автоматизированные системы управления технологическим процессом, информационно-коммуникационные технологии, ключевые системы информационной инфраструктуры, компьютерные вирусы, хакер, киберугрозы, кибератаки, кибервойна, кибербезопасность.

Содержание

1. Интернет — колыбель киберпространства

Киберпространство обязано своим появлением Интернету. Интернет явился концентрированным отражением общих тенденций информационной революции конца XX — начала XXI века, который интегрирует не только коммуникационные и технологические ресурсы, но и материальные, финансовые, интеллектуальные, гуманитарные, политические и прочие ресурсы, формирует и диверсифицирует процессы социальной регуляции.

Компьютеризацией пронизаны все сферы множественных коммуникаций и средств обеспечения как и внутри страны, так и между странами, государствами. Вся инфраструктура городов и стран сейчас зависима от компьютеров. Интернет, как паутина, охватил все страны и континенты. Это как некий мозг с нервной системой. Цифровые технологии стали кровеносной и нервной системой человеческих коммуникаций и взаимодействий [1].

Интернет соединяет все компьютеры, ноутбуки, серверы, планшеты и смартфоны в одну большую машину, которая стала самым надежным механизмом из всех, что человек придумал. За последнее десятилетие Интернет стал неотъемлемой частью каждой из сторон нашей жизни, и его значимость продолжает возрастать. В настоящий момент более 44% населения мира являются пользователями Интернета.

Современная архитектура Интернета позволяет на основе интернет-инфраструктуры создать виртуальное интернет-поле, границы которого не зависят от национальных границ.

Появление киберпространства способствовало формированию глобального информационного пространства, становлению «сетевого общества», основой функционирования которого становятся генерирование, обработка, передача и обновление информационного социального поля. Киберпространство включается в социальную среду и является одним из важнейших факторов, способствующих глобализации, становится инфраструктурным фундаментом новых областей жизнедеятельности человечества.

Интернет становится все более значимым фактором изменений социоэкономического характера, демонстрируя технико-технологическую, экономическую и экспоненциально возрастающую социальную значимость как собственно в Сети, так и в реальной жизни и в нашей стране.

Сказать, что в нашей стране возможности, предоставляемые Интернетом, используются чрезвычайно широко, значит не сказать ничего. Экономика страны и качество жизни граждан находятся в зависимости от работоспособности национального сегмента Всемирной сети.

По данным последнего исследования «*Развитие Интернета в регионах России. Весна 2016*», аудитория Интернета в России на осень 2015 г. составляет 78 млн человек — столько россиян пользуются Интернетом хотя бы раз в месяц. А 63 млн человек выходят в Сеть ежедневно [2].

Проникновение Интернета в России немного меньше, чем в среднем по Европе, и существенно выше, чем в среднем в мире.

Количество интернет-пользователей в России к 2016 г. достигнет 100 млн. По данным министра связи и массовых коммуникаций РФ Н. Никифорова, увеличение доступа населения к Интернету на 10% дает примерно 1,5% экономического роста страны.

По данным Росстата, Интернет используют в своей работе 87% организаций. Большая часть информационного обмена как внутри коммерческих компаний, так и между ними осуществляется в электронной форме.

По тем же данным, 93% органов власти и муниципалитетов используют Интернет «для осуществления управленческих функций и предоставления государственных услуг».

В России работают 24 тыс. только официально зарегистрированных Роскомнадзором электронных средств массовой информации (26% от общего числа СМИ), число незарегистрированных как СМИ информационных сайтов составляет сотни тысяч.

В 2013 г. через Интернет продано 23 млн (20% от общего числа) железнодорожных билетов, а доля продаж электронных авиабилетов составила 97%.

Даже эти цифры подтверждают, что при потере работоспособности российского сегмента Интернета страна вернется в глубокое технологическое прошлое.

Глобальная информатизация в настоящее время активно управляет существованием и жизнедеятельностью государств мирового сообщества, информационные технологии применяются при решении задач обеспечения национальной, военной, экономической безопасности и др. Вместе с тем одним из фундаментальных последствий глобальной информатизации государственных и военных структур стало возникновение принципиально новой среды противоборства конкурирующих государств — киберпространства, которое не является географическим в общепринятом смысле этого слова, но тем не менее в полной мере является международным.

Развитие Интернета, открывшего для человечества невиданные ранее возможности в сфере информации и коммуникации, создании киберпространства, сопровождается также целым рядом невиданных раннее рисков:

- проявление киберпреступности против личности, государства, общества;
- сращивание национальной и зарубежной преступности в транснациональные преступные синдикаты;
- информационный вандализм и хакерство;
- информационный терроризм на внутригосударственном и международном уровнях;
- информационные войны на внутригосударственном и международном уровнях, которые способны вызвать взрывы на химических заводах и токсичные облака над мегаполисами, пожары на нефтехранилищах и трубопроводах, транспорт-

ный коллапс на дорогах и в аэропортах, а нация оказывается буквально парализована без электричества, управления, защиты и информации о том, что происходит.

Все это позволяет злоумышленникам совершать с помощью Интернета негативные деяния как против элементов Интернета, так и против иных субъектов Интернета, а также наносить прямой ущерб любым юридическим субъектам, и даже их критически важной инфраструктуре, если она подключена к Интернету.

В своем докладе 2013 г. об экономических последствиях киберпреступности компания McAfee привела оценку, что вероятные ежегодные потери глобальной экономики от киберпреступности составляют более 455 млрд долл. [https://digital.report/zashhita-ict-infrastrukturyi/].

Ущерб экономике Российской Федерации от действий киберпреступных групп в 2015 г. составил 203,3 млрд руб., или 0,25% от валового внутреннего продукта страны. Такие выводы содержатся в исследовании «*Киберпреступность в России и ее влияние на экономику страны*», подготовленном экспертами Group-IB, Фонда развития интернет-инициатив (ФРИИ) и Microsoft [https://servernews.ru/931430].

2. Киберпространство

Термин «киберпространство» — популярный термин для обозначения воспринимаемого пользователем «виртуального» пространства, содержащегося в памяти компьютера и изображенного графически. В середине 1990-х гг. этот термин приобрел широкое распространение в связи с развитием Интернета и Всемирной компьютерной сети (www).

Киберпространство представляет собой уникальную среду, не расположенную в географическом пространстве, но доступную каждому в любой точке мира посредством доступа в Интернет [1].

Общегосударственное определение киберпространства впервые прозвучало в докладе исследовательской службы конгресса США в 2001 г., где киберпространство определено как «всеохватывающее множество связей между людьми, созданное на основе компьютеров и телекоммуникаций вне зависимости от физической географии».

Термин «киберпространство» помогает осознать Интернет как новую форму пространства, не отвечающую материальным характеристикам, но позволяющую осуществлять в ней либо с ее помощью различные действия, которые могут иметь реальные последствия. Киберпространство является неотъемлемой частью современного мироустройства.

Киберпространство как противоположность естественному физическому пространству содержит информационный эквивалент вещей. Одна из главных составляющих киберпространства — это передвижение информации, которое осуществляется посредством программирования и цифровой коммуникации. Таким образом, определение термина «киберпространство» должно соотноситься с совокупностью множества процессов, которые осуществляются с использованием цифровых сетей: электронной перепиской, финансовыми операциями, разработкой и использованием компьютерных программ и созданием виртуальной реальности.

В начале 2014 г. Советом Федерации для публичного обсуждения был предложен проект концепции стратегии кибербезопасности Российской Федерации, которая должна была определить направления усилий государства в отношении новых угроз, возникающих в современном информационном мире.

Киберпространство в проекте концепции определяется следующим образом: «*Киберпространство — сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)*».

Данное определение во многом перекликается с позицией Международного стандарта ИСО/МЭК 27032:2012 «*Руководящие указания по кибербезопасности*». Киберпространство — это сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, программного обеспечения, интернет-сервисов посредством технологических устройств и сетевых связей.

Важной особенностью киберпространства является его глобальность, обеспечивающая возможность информационного взаимодействия людей и объектов, располагающихся на территории различ-

ных государств. Глобальность киберпространства достигается посредством соединения национальных электронных сред в единую электронную среду сбора, передачи, хранения и обработки информации на основе единой системы цифровой адресации субъектов и объектов киберпространства.

3. Киберугрозы промышленным объектам

Киберпространство не замыкается в самом себе и повсеместно стыкуется с реальными объектами на программном уровне. Так, управление технологическими процессами, процессами производства материальных благ, системами безопасности все шире передается компьютерам и компьютерным программам, и защита автоматизированных систем управления технологическими процессами (АСУ ТП) все больше и больше выходит на передний край. Ведь АСУ ТП — это область, где виртуальный мир соприкасается с миром физическим.

На промышленных объектах АСУ ТП являются ключевыми системами информационной инфраструктуры. От корректной и стабильной работы этих систем зависит безопасность всего объекта. Большинство АСУ ТП, которые в настоящее время работают в промышленности, созданы без учета возможности кибератак.

Системы АСУ ТП в настоящее время применяются практически в каждой отрасли: начиная с транспортной (скоростные поезда «Сапсан», метрополитен), заканчивая атомными и гидроэлектростанциями, сетями распределения электроэнергии и водоснабжения.

Более 40% подключенных к Интернету АСУ ТП, применяющихся на предприятиях в энергогенерирующей, нефтеперерабатывающей и других отраслях, уязвимы для хакерских атак, в результате чего целые заводы могут быть выведены из строя, говорится в исследовании российской компании Positive Technologies [http://digit.ru/technology/20121107/396404269.html].

Последствия успешной хакерской атаки на любую из таких систем могут оказаться катастрофическими. Компания Positive Technologies является одним из мировых лидеров в области комплексной защиты крупных информационных систем от современных киберугроз.

Специалисты отмечают рост числа именно подключенных к Сети систем (еще несколько лет назад такие примеры были редкостью и АСУ ТП в основном работали автономно).

США и Европа лидируют по числу доступных из Интернета систем АСУ ТП, при этом 54% доступных извне систем в Старом Свете и 39% в США уязвимы и могут быть взломаны. На третьей позиции — Азия (32%). В России процент подключенных к Интернету АСУ ТП заметно ниже, однако страна входит в первую двадцатку государств с наибольшим количеством подобных сетевых ресурсов.

В настоящий момент 35% всех представленных уязвимостей АСУ ТП имеют эксплойты (готовые средства для использования уязвимости), которые свободно распространяются в виде отдельных утилит, входят в состав программных пакетов для проведения тестов на проникновение либо описаны в уведомлениях об уязвимости, отмечают исследователи.

Исследование охватило период с 2005 г. до 1 октября 2012 г. В период с 2005 по 2010 г. было обнаружено всего 9 уязвимостей в системах АСУ ТП. Однако после появления червя Stuxnet в 2010 г., который атаковал ряд ядерных объектов Ирана, за 2011 г. было найдено уже 64 уязвимости.

За первые восемь месяцев 2012 г. появились сообщения о 98 новых уязвимостях: это больше, чем за все предыдущие годы. При этом около 65% уязвимостей относятся к высокой и критической степени риска.

Исследования «Лаборатории Касперского», опубликованные в 2016 г., показали, что 92% подключенных к Интернету АСУ ТП уязвимы для киберугроз [https://www.pcweek.ru/security/news-company/detail.php?ID=186782].

Как выяснила «Лаборатория Касперского», большое количество автоматизированных систем управления (АСУ), использующихся на критически важных инфраструктурных и промышленных объектах, не только доступны из Интернета, но также имеют уязвимости в программном обеспечении, что подвергает их риску стать целью кибератаки. Кибератаки против критически важной гражданской инфраструктуры могут оставить тысячи человек без воды, еды и электричества, а диверсии против атомных электростанций и дамб — технически

они тоже возможны — могут привести к огромным жертвам.

В общей сложности эксперты компании обнаружили в 170 странах мира более 188 тыс. узлов, на которых размещено 220 тыс. разных промышленных систем, содержащих компоненты АСУ. Свыше 13 тыс. обнаруженных узлов принадлежат крупным компаниям, работающим в энергетике, нефтегазовой и химической отраслях, промышленном секторе, в сфере транспорта и автомобилестроения, в производстве продуктов питания, а также в области финансов и здравоохранения.

При развитии информационно-коммуникационных технологий в Российской Федерации широко применяются зарубежные аппаратно-программные средства. Очевидна возможность наличия в таких средствах программных или программно-аппаратных закладок, а также не декларированных возможностей. В большинстве зарубежных «защищенных микросхем» для коммерческого применения, в том числе предназначенных для защиты информации и продаваемых за пределы стран-изготовителей, предусмотрен «полицейский» режим, позволяющий получить доступ к ключевой информации и защищаемым данным, записанным в микросхемах.

В настоящий момент сложилась критическая ситуация, при которой на каждом из участков инфокоммуникационной инфраструктуры (чипы, схемотехника, электронные компоненты, транспорт и передача данных, системы управления, программное обеспечение от библиотек до отдельных продуктов и т.п.) с высокой долей вероятности используются зарубежные решения с неизвестной начинкой. Даже после проведения специальных мероприятий по проверке и анализу потенциально опасных свойств используемых решений нет оснований полагать, что данные свойства гарантированно не смогут проявиться при определенном наборе условий в дальнейшем [http://www.connect.ru/article.asp?id=10936].

Сегодня сложилась ситуация, когда на этапе ОКР по созданию продукта, гарантирующего соблюдение требований обеспечения кибербезопасности, невозможно получить результат, взаимодействуя только с российскими предприятиями.

Еще один пример похожей проблемы — зависимость от современных информационно-коммуникационных технологий (ИКТ). С одной стороны, государства продолжают массово закупать необходимые для развития их экономик современные технологии у относительно узкого круга поставщиков, что делает их уязвимыми перед решениями этих поставщиков (например, перед введением односторонних ограничений на поставки оборудования). Другой стороной этой же проблемы часто является невозможность проверить безопасность этого оборудования на всех уровнях — как программном, так и техническом. В итоге большинство стран мира оказываются заложниками узкого круга компаний и тех специальных структур, с которыми эти компании сотрудничают.

Именно поэтому и Совет безопасности, и руководство страны уделяют значительное внимание вопросам безопасности АСУ ТП критически важных объектов. В развитие принятых Советом безопасности решений 15 января 2013 г. Президентом Российской Федерации был подписан указ о создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Данным указом определен федеральный орган, на который возложены полномочия по созданию такой системы, — Федеральная служба безопасности.

4. Киберугрозы для критически важных объектов и ключевых систем информационной инфраструктуры

Критически важным признается объект (КВО), оказывающий существенное влияние на национальную безопасность Российской Федерации, прекращение или нарушение функционирования которого приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны либо для жизнедеятельности населения, проживающего на соответствующей территории. На территории Российской Федерации функционирует около 4,5 тыс. КВО [4, 5].

Основным признаком принадлежности объекта к критически важным является наличие на нем экологически опасного или социально значимого производства либо технологического процесса, нарушение штатного режима которого приводит к чрезвычайной ситуации определенного уровня и масштаба, или наличие на объекте информационно-телеком-

муникационной системы (ее элемента), которая осуществляет функции управления чувствительными (важными) для Российской Федерации процессами и нарушение функционирования которой приводит к негативным для страны последствиям.

Критически важными являются объекты, прекращение или нарушение функционирования которых может привести к тяжелым последствиям для региона или государства в целом, в том числе и к человеческим жертвам.

Перечни видов критически важных объектов и критически важных систем составляются специально создаваемой группой экспертов, состав которой утверждается соответствующим руководителем федерального органа исполнительной власти (организации).

Критичность объекта и соответственно его инфраструктуры во всем мире определяется на государственном уровне, критические для существования и функционирования государств предприятия и отрасли фиксируются в специальных перечнях. Естественно, государствообразующими являются самые различные секторы и отрасли — от финансовой и банковской системы до систем управления водо- и энергоснабжением.

Если говорить об отраслях, наиболее часто относимых к критической инфраструктуре и связанных не только с физической, но и с кибербезопасностью, то на основании усредненного мирового опыта можно составить следующий перечень, в определенной степени совпадающий у большинства государств [http://www.pircenter.org/media/content/files/13/14683392340.pdf]:

- электроэнергетика (атомная энергетика часто выделяется отдельно);
- управление природными ресурсами (в частности, нефтегазовый сектор);
- управление водными ресурсами (включая водоочистку и управление сточными водами);
- транспорт;
- пищевая промышленность;
- здравоохранение;
- телекоммуникации;
- финансовая и банковская системы;
- органы государственной власти.

Сюда же следует отнести и объекты жизнеобеспечения. *Объекты жизнеобеспечения* — объекты, обеспечивающие жизнедеятельность населения. К таковым относятся объекты водоснабжения (насосно-фильтровальные станции, станции очистки сточных вод, плотины, гидроузлы, водозаборы, водохранилища, дамбы, водосбросные, водоспускные и водовыпускные сооружения и т. п.), теплоснабжения (ТЭЦ, крупные городские котельные, работающие под давлением более 0,07 МПа или при температуре нагрева воды более 115 °С), энергоснабжения (ГРЭС, трансформаторные подстанции мощностью свыше 110 кВт).

Следствиями нарушения функционирования критически важного объекта могут быть:

- гибель или физическое травмирование людей;
- нарушение систем обеспечения жизнедеятельности городов и населенных пунктов;
- нарушение социальной стабильности в стране, регионе, субъекте Федерации, области, районе;
- авария или катастрофа, разрушение или заражение среды обитания в национальном масштабе;
- нанесение крупного экономического (финансового) ущерба государству, государственным и частным предприятиям и организациям, физическим лицам, нарушение стабильности финансовой и банковской системы страны, остановки непрерывных производств;
- крупномасштабное уничтожение национальных ресурсов (природных, сельскохозяйственных, продовольственных, производственных, информационных);
- нарушение системы государственного управления на федеральном, региональном и территориальном уровне;
- нанесение крупного внешнеполитического ущерба стране;
- причинение значительного ущерба в сфере обороны и безопасности страны.

Эффект от поражения программными средствами объектов критической инфраструктуры уже не исчерпывается похищением данных, а переходит в плоскость нанесения физического ущерба работе промышленных и логистических объектов вплоть до их полного разрушения.

Символом беспрецедентной опасности кибернетических атак стал компьютерный червь Stuxnet, который в 2009—2010 гг. поразил информационные системы иранского комбината по обогащению урана.

Дальнейшее развитие подобных средств программного воздействия уже позволяет применять их для осуществления диверсий на электростанциях, в том числе для разрушения энергогенерирующих турбин атомных электростанций и тому подобных составляющих критической атомной инфраструктуры. Подобные последствия выходят за рамки национальных границ государств, чья инфраструктура подвергается атакам, и представляют непосредственную угрозу международной безопасности наравне с международным терроризмом, трансграничной преступностью, а в перспективе и использованием оружия массового уничтожения.

Разработка и применение подобных программных инструментов осуществляется анонимно, в силу того, что существующие технические возможности не позволяют достоверно и однозначно идентифицировать конечный источник атаки и непосредственного ее автора. Кроме того, даже при наличии технической возможности определить, откуда осуществляется атака, не существует каких бы то ни было юридических и международно-правовых механизмов, позволяющих отнести ответственность за осуществление такой деятельности на конкретное лицо и тем более субъект международного права.

В таблице перечислены отрасли экономики России, наиболее уязвимые с точки зрения компьютерной безопасности.

Ключевая система информационной инфраструктуры (КСИИ) — это информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), либо информационное обеспечение управления таким объектом (процессом), либо официальное информирование граждан [5]. В результате деструктивных информационных воздействий на КСИИ может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

Системы, относящиеся к КСИИ

Информационные (информационно-телекоммуникационные) системы относятся к ключевым в зависимости от их назначения в соответствии с перечнем критически важных сегментов информационной инфраструктуры. В свою очередь, критически важными сегментами информационной и телекоммуникационной инфраструктуры России признаются сегменты, образуемые системами, нарушение штатного режима функционирования которых может нарушить функции управления чувствительными для Российской Федерации процессами, в том числе:

- системами органов государственной власти и органов местного самоуправления;
- системами органов управления правоохранительных структур;
- системами финансово-кредитной и банковской деятельности;

Отрасли экономики России, наиболее уязвимые с точки зрения компьютерной безопасности, % *Таблица*
[http://cs.groteck.ru/IB_6_2014/files/ib_6_2014.pdf]

Отрасль	Очень уязвимы	В какой-то степени уязвимы	Неуязвимы	Абсолютно неуязвимы	Всего
Аэрокосмическая и оборонная	22	30	33	15	51
Химическая	15	37	40	8	52
Финансы	32	36	24	8	68
Правительство и госорганы	21	39	29	10	61
Медицина/здравоохранение/фармацевтика	17	45	32	6	62
Нефтегазовая	16	39	36	9	55
Энергетика	15	39	37	8	54
Телекоммуникации/IT	27	42	26	6	68
Туризм	25	30	29	6	65

• системами предупреждения и ликвидации кризисных и чрезвычайных ситуаций;

• географическими и навигационными системами;

• программно-техническими комплексами центров управления взаимоувязанной сети связи России;

• сетями связи общего пользования на участках, не имеющих резервных или альтернативных видов связи;

• системами специального назначения;

• спутниковыми системами, используемыми для обеспечения органов управления и в специальных целях;

• системами управления добычей и транспортировкой нефти, нефтепродуктов и газа;

• системами управления потенциально опасными объектами;

• системами управления транспортом (наземным, воздушным, морским);

• системами управления водоснабжением;

• системами управления энергоснабжением.

Таким образом, в категорию КСИИ попадают не только многочисленные АСУ ТП, но и системы государственного управления, телевидения, банковской отрасли.

5. Крупные атаки хакеров в 2000—2015 годах

В апреле 2000 г. хакеры получили контроль над газовыми потоками «Газпрома» [https://lenta.ru/internet/2000/04/27/gasprom].

25 января 2003 г. в Республике Корея в результате действий хакеров произошел общенациональный сбой в Интернете, в течение нескольких часов вся страна была лишена доступа в мировую сеть. Впервые действия кибертеррористов отразились на деятельности компаний в общенациональном масштабе. Помимо Южной Кореи пострадали интернет-пользователи множества других стран, включая Россию, по всему миру были поражены по меньшей мере 22 тыс. серверов [http://tass.ru/info/1408961].

В апреле 2009 г. киберпреступники проникли в компьютерную систему Пентагона и похитили информацию о новом многоцелевом истребителе пятого поколения Joint Strike Fighter.

7 июля 2009 г. хакеры вывели из строя практически все важнейшие интернет-порталы в Южной Корее, включая сайты президента, парламента и министерства обороны.

В сентябре 2010 г. вирус Stuxnet поразил компьютеры сотрудников АЭС в Бушере (Иран) и создал проблемы в функционировании центрифуг комплекса по обогащению урана в Натанзе. По мнению экспертов, Stuxnet стал первым вирусом, который был использован как кибероружие.

23 апреля 2013 г. группа хакеров взломала аккаунт информагентства AP в сервисе микроблогов Twitter и разместила ложное сообщение о взрывах в американском Белом доме и ранении президента Барака Обамы.

В мае 2013 г. газета The Washington Post, ссылаясь на конфиденциальный доклад, направленный руководству Пентагона, сообщила, что в распоряжение китайских хакеров попали секретные военные документы США, включая чертежи и описания военных самолетов и кораблей, а также систем противоракетной обороны.

27 ноября 2013 г. и 15 декабря 2014 г. хакеры похитили персональные данные (номера телефонов, электронные и почтовые адреса, номера и PIN-коды кредитных и дебетовых карт) 110 млн клиентов компании Target, владеющей третьей по величине торговой сетью США. В результате американские финансовые институты понесли убытки в размере более 200 млн долл.

16 февраля 2015 г. в результате хакерской операции Carbanak киберпреступники украли около миллиарда долларов из 100 финансовых организаций по всему миру. Об этом говорится в сообщении компании «Лаборатория Касперского», которая провела совместное расследование с Европолом и Интерполом. Хакерская атака длилась в течение двух лет.

Кибератаки на атомные станции

Множество гражданских ядерных объектов по всему миру подвержены риску хакерских атак, уверены специалисты британского аналитического центра Chatham House. Многие АЭС не готовы к защите от подобного рода угроз, а устройство сетей отдельных ядерных объектов даже можно найти в Интернете [6].

Инцидент с АЭС «Дэвис-Бесс» в Огайо произошел в 2003 г., когда программное обеспечение об-

служивающей АЭС компании было заражено вирусом Slammer, который привел к отказу серверов корпоративной сети. Оператор совершил ошибку и в ходе расследования инцидента подключил корпоративную сеть к внутренней компьютерной сети станции, и вирус распространился дальше, что сделало невозможным использование компьютеров сотрудниками самой АЭС, которые потеряли связь друг с другом. Также на шесть часов была выведена из строя система отображения параметров безопасности, которая показывает операторам, как работает оборудование и насколько оно исправно.

Серьезный случай произошел в 2006 г. на АЭС «Браунс Ферри» в Алабаме, когда главная система безопасности АЭС оказалась перегруженной сетевым трафиком, что едва не привело к опасной аварии.

В декабре 2014 г. серьезный общественный резонанс вызвал взлом южнокорейского оператора АЭС Hydro and Nuclear Power Co Ltd. Хакер разослал 5986 содержащих вредоносный код электронных писем более чем 3 тыс. сотрудников компании и в итоге получил доступ в ее внутреннюю сеть. Затем злоумышленник через Twitter потребовал заглушить три реактора АЭС, угрожая их разрушением. В итоге он потребовал выкуп под угрозой раскрытия украденной из сети оператора АЭС конфиденциальной информации, однако представители компании заявили, что критически важная информация похищена не была.

6. Кибервойна

В процессе формирования глобального киберпространства происходит конвергенция военных и гражданских компьютерных технологий. В ведущих зарубежных государствах интенсивно разрабатываются новые средства и методы активного воздействия на информационную инфраструктуру потенциальных противников, создаются различные специализированные кибернетические центры и подразделения управления и командования, основной задачей которых является защита государственных и военных информационных инфраструктур, подготовка и проведение активных деструктивных действий в информационных системах противника. Так, собственные официальные кибервойска уже существуют у США, Китая, Англии, Франции, Германии, Израиля и ряда других государств. Противоборство в киберпространстве становится принципиально новой сферой противоборства между государствами [8].

Ведущие мировые державы открыто обсуждают и необходимость защиты от враждебных действий противника в киберпространстве, и планы по наращиванию своих кибермощностей. Это порождает цепную реакцию и вынуждает остальные страны также собирать команды высокопрофессиональных программистов и хакеров (*хакер в переводе с английского означает рубщик (to hack — рубить)*) для разработки специализированных киберсредств — как для защиты, так и для нападения. Гонка кибервооружений набирает обороты.

Принципиальное отличие кибервойны от традиционных военных действий состоит в том, что кибератаки на государственные информационные ресурсы могут вестись негосударственными субъектами. Кибервойна — это не только продолжение политики иными средствами, но и продолжение войны иными средствами. Стратегические цели кибервойны те же — вывод из строя важнейших инфраструктурных, финансовых и правительственных объектов противника.

Всемирный экономический форум (ВЭФ) опубликовал доклад «*Глобальные риски 2015*» (Global Risk Report 2015), на многих страницах которого можно встретить упоминание кибератак и угроз кибербезопасности. Кибератаки вошли в число десяти ведущих глобальных рисков с точки зрения вероятности, а их последствия — в число десяти ведущих глобальных рисков с точки зрения воздействия.

Уже в 2016 г. доклад ВЭФ вводит риски киберпространства в число четырех основных долгосрочных геополитических рисков. Причем риски киберпространства в ближайшее время способны затмить все остальные, потому что границы и армии не могут их ограничить. Особую угрозу представляют вредоносные программы для критической инфраструктуры — электросетей, авиадиспетчерских систем, нефтепроводов, водоснабжения, финансовых платформ и так далее, и не обязательно, что государства должны быть вовлечены во все это: физические и негосударственные субъекты могут использовать вредоносные программы, просто наняв на работу необходимых специалистов на международном подпольном рынке.

Специальная технология, позволяющая обойти или обмануть системы кибербезопасности, в том

числе те, которые должны защищать такие сверхсекретные промышленные объекты, как АЭС, называется атака «нулевого дня». Она представляет собой определенный вредоносный код, выполняемый перед основной вредоносной программой, и предназначена для использования уязвимости, которая является новой и неизвестной в целевой системе.

Атака «нулевого дня» способна полностью или временно вывести из строя систему управления кибербезопасностью и таким образом открыть целевую компьютерную систему для внедрения и начала работы основной вредоносной программы. Многие высококвалифицированные хакеры усердно работают над обнаружением новых уязвимостей в системах, которые позволяют создавать новые атаки «нулевого дня». Мотивацией для этих хакеров является то, что атаки «нулевого дня» можно дорого продать государствам или экстремистам. Атаки «нулевого дня», обнаруженные и разработанные высококвалифицированными хакерами, являются важной составляющей существующего поколения кибероружия.

В международном договоре между Правительством Российской Федерации и Правительством Китайской Народной Республики закреплено понятие «*компьютерная атака*», которое трактуется как «целенаправленное воздействие программными (программно-техническими) средствами на информационные системы, информационно-телекоммуникационные сети, сети электросвязи и автоматизированные системы управления технологическими процессами, осуществляемое в целях нарушения (прекращения) их функционирования и (или) нарушения безопасности обрабатываемой информации» [10].

Кибератака представляет собой преднамеренные действия по изменению, разрушению, искажению, запрещению, нарушению или уничтожению информации и программ, находящихся в компьютерных системах и сетях, или самих компьютеров и сетей.

Спецификой кибервойны являются относительно низкие затраты по сравнению с обычными военными действиями. К примеру, стоимость производства современного атомного авианосца — порядка 5 млрд долл., стоимость его годовой эксплуатации — 160 млн долл. Стоимость кибератаки, способной вывести из строя программное обеспечение (ПО) крупного военного объекта, — менее 5 млн долл. Иногда существенно меньше.

«Вывод из строя любого компьютера, отвечающего за работу ядерных и химических предприятий, будет равносилен поражению части территории нашей страны ядерной бомбой», — заявил не так давно экс-министр обороны США Леон Панетта [8].

Кибератаки могут проводить и террористические группировки — кибертерроризм. Кибертерроризм может быть определен как использование компьютеров в качестве оружия или целей политически мотивированными международными или национальными группами или тайными агентами, причиняющими или угрожающими причинить ущерб и посеять панику, с целью воздействия на население или правительство для изменения политики.

Объектом нападения необязательно должен быть крупный военный или гражданский объект. Им может быть информационная система. Достаточно вывести из строя три-четыре крупнейших банка какой-нибудь европейской страны, и финансовая система этого государства окажется в коллапсе.

Сегодня становится ясно, что для сохранения суверенитета государство должно не только отстаивать социально-экономические и политические интересы, но и тщательно охранять свое информационное пространство. И теперь едва ли не на первый план выступает задача контролировать критически важные для государства информационные системы.

Устав ООН предусматривает руководящие принципы для обоснования ответных действий на кибератаки, являющиеся применением силы. Они приведены в статье 2 (4) — разрушительные действия, подходящие под определение «применение силы», и в статье 51 — разрушительные действия, подходящие под определение «вооруженного нападения», несущие угрозу государственному суверенитету.

Наиболее опасными мишенями кибератак являются в первую очередь ключевые системы информационной инфраструктуры (КСИИ), управляющие критически важными объектами. Для управления объектами в КСИИ используется то или иное программное обеспечение, не лишенное ошибок и уязвимостей.

Вывод из строя таких объектов может привести к хаосу и катастрофам. Наша жизнедеятельность так или иначе зависит от этих систем. Они обогревают наши дома, подают в них воду и электричество, обеспечивают радио- и телевещание,

управляют транспортными потоками, контролируют добычу ресурсов и производственные процессы на фабриках и заводах.

Помимо промышленных объектов существует множество организаций, для которых несанкционированный доступ к информации может стать серьезной проблемой: банки, медицинские и военные учреждения, исследовательские институты и бизнес.

Кибероружие становится опаснее ядерного. Под кибероружием следует понимать технические и программные средства поражения (устройства, программные коды), которые конструктивно предназначены для воздействия на программируемые системы, эксплуатацию уязвимостей в системах передачи и обработки информации или программно-технических системах, с целью уничтожения людей, нейтрализации технических средств либо разрушения объектов инфраструктуры противника. Данное понятие может быть соотнесено с более общим понятием «информационное оружие».

В июне 2013 г. президенты РФ и США Владимир Путин и Барак Обама поручили установить линию прямой связи по вопросам урегулирования ситуаций, создающих угрозу кибербезопасности, используя в этих целях линию прямой связи между центрами по уменьшению ядерной опасности США и России [http://tass.ru/mezhdunarodnaya-panorama/617111].

Характерными чертами кибероружия являются: 1) отсутствие физического вмешательства при воздействии на систему; 2) эксплуатация уязвимостей внутри конкретной системы (или определенного типа систем); 3) точно предустановленный результат комплексов, воздействующих по установленным алгоритмам.

Киберсредства поражения представляют собой *вирусы*. Для вирусных атак уязвимы все компьютерные операционные системы. Пути попадания вирусов в компьютеры различны, но общее в них одно — вирусы входят в компьютерные системы только из внешних источников. Известны несколько различных форм вирусов, которые могут вторгнуться в компьютерную систему. В настоящее время существует 3 основные категории вредоносных ПО: вирусы, черви и трояны («троянский конь»).

В принципе, любое киберсредство является специальной программой, разработанной в единичном экземпляре и предназначенной для однократного использования при осуществлении конкретной операции. Первым общеизвестным вредоносным боевым кодом, использовавшимся как кибероружие, стал червь Стакснет (Stuxnet). Червь был запрограммирован на распространение через USB, что позволяло вторгаться в защищенные от воздействия из мировой сети объекты. Также он имел подробный алгоритм создания и загрузки своих модулей в атакуемую систему в зависимости от работы на компьютере определенных защитных решений. Таким образом Stuxnet старался свести к минимуму воздействие на заведомо защищенную достаточным образом систему во избежание обнаружения.

«Лаборатория Касперского» за последние несколько лет нашла уже 4 боевых вируса. Изучение этих вирусов показало, что они созданы отнюдь не группой частных лиц, чтобы воровать персональные данные, деньги с кредитных карт. Это вирусы, созданные на государственном уровне. Стоимость разработки одного или двух таких вирусов в «Лаборатории Касперского» оценили в 100 млн долл. Этого не может себе позволить ни одна группа хакеров. Кроме того, вирусы настолько сложные, что совершенно очевидно, что их много лет разрабатывало много людей очень высокой квалификации.

В 2013 г. «Лабораторией Касперского» была опубликована информация о совершенно новом явлении в области компьютерных атак. Была раскрыта шпионская сеть «Красный Октябрь» (Red October), на протяжении пяти лет занимающаяся хищением государственных секретов. Это сложнейший комплекс вредоносных программ, около 1000 вредоносных файлов, относящихся к 30 различным группам модулей.

Информатизация общества постоянно создает новые потенциальные цели для кибероружия. Любое медицинское учреждение с тяжелым оборудованием вроде томографов способно стать жертвой специально разработанного вредоносного кода, отдельные электростанции и даже системы ПВО могут быть выведены из строя по невнимательности или злому умыслу. Разумеется, подобные объекты становятся целью кибератаки в случае полномасштабной войны или террористического акта, но кибервойна может быть и экономической.

Кибервойна из фазы проверки противника на уязвимость может решительно перейти к стадии нанесения полномасштабных кибердаров по экономическим и военным объектам, всем объектам критической инфраструктуры, от которых зависит сама жизнеспособность, безопасность государств, общественная стабильность. Кибервойны могут оказаться не менее разрушительными и жестокими по сравнению с так называемыми обычными. При этом еще надо делать поправку на трансграничный и всепроникающий характер информационных технологий и соответствующего оружия.

Военное руководство США рассматривает борьбу в киберпространстве как составную часть информационного противоборства, которое должно вестись не только в четырех традиционных пространствах — наземном, морском, воздушном и околоземном космическом, но и в киберпространстве. Еще в 2008 г. министерство обороны США определило противоборство в киберпространстве как оперативно-стратегическую категорию, характеризующую процесс соперничества конфликтующих сторон, в котором каждая проводит в отношении другой операции, мероприятия или акции, связанные с программно-математическим и другими видами воздействия на объекты системы боевого управления и связи противника, его оружие и военную технику в интересах решения поставленных задач.

В целом кибероружие предназначено для решения следующих задач:

- временное отключение от компьютерной сети критически важных узлов коммуникационной инфраструктуры;
- блокирование компьютерных операций и функций;
- нарушение работы и вывод из строя автоматизированных систем управления и связи;
- искажение и фальсификация информации, распространение дезинформации.

США на официальном уровне заявляют, что готовы на кибернападение ответить всеми имеющимися в их распоряжении средствами. По американским данным, более 120 стран в современном мире экспериментируют в области кибервойны. К этому нужно добавить преступников и террористов в области использования ИКТ, так называемый субъективный фактор в лице отдельных хакеров.

7. Кибербезопасность

В XXI веке кибербезопасность начинает выступать как основной фактор национальной и международной безопасности [7, 14].

Кибербезопасность (философское определение) — это свойство или состояние системы сохранять надежность и функциональную устойчивость в условиях современного информационного противоборства.

Кибербезопасность (определение по технической сущности) — информационная безопасность компьютерных информационно-управляющих систем, обеспечивающая их высокую надежность и функциональную устойчивость в условиях современного информационного противоборства.

Россия как одно из ведущих государств мира является первоочередным объектом для негативных кибервоздействий в стремлении других стран к мировому лидерству. В настоящее время существует потенциальная угроза нарушения функционирования критически важных информационных систем основных объектов жизнеобеспечения государства, ВС РФ, МВД, ФСБ, ФСО, МЧС России при массированном воздействии компьютерных атак на их уязвимости. При этом прежние базовые информационные защищенные компьютерные технологии и традиционные средства защиты информации недостаточны и уже не обеспечивают необходимого уровня защищенности и функциональной устойчивости.

Нормативное обеспечение кибербезопасности

Актуальность проблемы кибербезопасности признается на высшем уровне руководства государства и определена в следующих регламентирующих документах в области защиты КВО и КСИИ.

1. «*Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации*» (документ Совета безопасности, утвержденный Президентом Российской Федерации 3 февраля 2012 г. № 803).

Целью государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфра-

структуры Российской Федерации является снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем, а также минимизация негативных последствий подобного вмешательства.

К 2020 г. должен быть обеспечен:

• ввод в эксплуатацию Ситуационного центра единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру Российской Федерации и оценки уровня реальной защищенности ее элементов и ситуационных центров регионального и ведомственного уровней;

• ввод в эксплуатацию в целом единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов.

В период после 2020 г. должен осуществляться комплекс мероприятий по поддержанию организационной, экономической, научно-технической и технологической готовности Российской Федерации к предотвращению угроз безопасности ее критической информационной инфраструктуры.

2. Указ Президента РФ от 15 января 2013 г. № 31с *«О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»*. Для ознакомления была опубликована открытая выписка из Указа Президента, согласно которой:

• на ФСБ России возложены полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом;

• определены основные задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

• полномочия ФСБ России в части:

– разработки методики обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети государственных органов и по согласованию с их владельцами — на иные информационные системы и информационно-телекоммуникационные сети;

– определения порядка обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах, связанных с функционированием информационных ресурсов Российской Федерации;

– организации и проведения мероприятий по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

– разработки методических рекомендаций по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак.

3. Указ Президента РФ от 22 мая 2015 г. № 260 *«О некоторых вопросах информационной безопасности Российской Федерации»* [http://base.garant.ru/71035416/#block_1000#ixzz4K2WDys6u].

«В целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети Интернет на территории Российской Федерации постановляю:

1. Преобразовать сегмент международной компьютерной сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Федеральной службы охраны Российской Федерации, в российский государственный сегмент информационно-телекоммуникационной сети "Интернет", являющийся элементом российской части сети "Интернет" и обеспечивающий:

а) подключение к сети "Интернет" предназначенных для взаимодействия с ней государственных информационных систем и информационно-телекоммуникационных сетей государственных органов, а также информационных систем и информационно-телекоммуникационных сетей организаций, созданных для выполнения задач, поставленных перед федеральными государственными органами;

б) размещение (публикацию) в сети "Интернет" информации государственных органов и названных в подпункте "а" настоящего пункта организаций.

4. Администрации Президента Российской Федерации, Аппарату Правительства Российской Федерации, Следственному комитету Российской Федерации, федеральным органам исполнительной власти и органам исполнительной власти субъектов Российской Федерации осуществить до 31 декабря 2017 г. подключение находящихся в их ведении государственных информационных систем и информационно-телекоммуникационных сетей к российскому государственному сегменту сети "Интернет" и обеспечить размещение (публикацию) информации в сети "Интернет" в соответствии с порядком, утвержденным настоящим Указом.

5. Рекомендовать Совету Федерации Федерального Собрания Российской Федерации, Государственной Думе Федерального Собрания Российской Федерации, судебным органам Российской Федерации, органам прокуратуры Российской Федерации, Счетной палате Российской Федерации, а также организациям, созданным для выполнения задач, поставленных перед федеральными государственными органами, осуществить подключение находящихся в ведении названных органов и организаций информационных систем и информационно-телекоммуникационных сетей к российскому государственному сегменту сети "Интернет" и обеспечить размещение (публикацию) информации в сети "Интернет" в соответствии с порядком, утвержденным настоящим Указом.

Подключение информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" через российский государственный сегмент сети "Интернет" осуществляется по каналам передачи данных, защищенным с использованием шифровальных (криптографических) средств.

Защита информации в информационных системах и информационно-телекоммуникационных сетях, подключаемых к сети "Интернет" через российский сегмент, в том числе с использованием средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, обеспечивается в соответствии с законодательством Российской Федерации».

4. В настоящее время ведется и находится на стадии завершения работа по согласованию следующих проектов документов:

- проект Федерального закона «*О безопасности критической информационной инфраструктуры Российской Федерации*».

Проектом определяются цели и принципы обеспечения безопасности критической информационной инфраструктуры Российской Федерации, полномочия органов государственной власти в этой сфере, порядок категорирования объектов критической информационной инфраструктуры и оценки их защищенности, источники финансирования мероприятий по обеспечению безопасности.

В законопроекте определяются такие понятия, как информационные ресурсы РФ, компьютерная атака, компьютерный инцидент, критически важный объект, критическая информационная инфраструктура РФ, субъекты критической информационной инфраструктуры РФ и ряд других.

Документ также предусматривает разработку критериев отнесения объектов критической информационной инфраструктуры к различным категориям опасности и установление требований к системам безопасности данных объектов;

- проект закона, вносящий поправки в Федеральный закон «*О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"*».

5. ГОСТ РО 0043-001-2010 «Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Термины и определения».

6. Федеральной службой по техническому и экспортному контролю (ФСТЭК) России разработан пакет руководящих документов (РД) по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, включающий:

- «Базовую модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Методику определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);

• «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007);

• Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

В 2013 г. организованы работы по созданию Национального центра управления обороной государства (НЦУОГ), предназначенного для решения задач контроля и управления всеми силами и средствами, действующими в интересах обороны страны как в военное, так и в мирное время, в том числе и системой кибербезопасности России. В том же году принято решение и организованы работы по созданию в Минобороны России киберкомандования для защиты общенациональных интересов в киберпространстве.

В Стратегии развития отрасли информационных технологий в Российской Федерации на 2014—2020 гг. и на перспективу до 2025 г. включен раздел по обеспечению информационной безопасности:

«*Учитывая масштабы проникновения информационных технологий в повседневную жизнь граждан, организаций и органов власти всех уровней, а также высокий уровень зависимости создаваемых в стране информационных систем от импортной продукции, особенно актуальным становится вопрос обеспечения должного уровня информационной безопасности страны в современном глобальном информационном мире. В этих условиях необходимо предпринять меры, направленные на обеспечение информационной безопасности не только государственных органов власти, но и других организаций и граждан, проживающих на территории России*».

25 марта 2015 г. на сайте ФСБ России была опубликована выписка из *Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации*, в которой описывается государственная Система обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА). Концепция была принята Указом Президента от 12 декабря 2014 г. № К 1274, а в выписке есть ссылка на Указ Президента от 15 января 2013 г. № 31с «*О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации*», который и определяет основные цели и задачи СОПКА.

В выписке говорится: «*Система представляет собой единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, и федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования Системы*».

В сентябре 2016 г. стало известно, что в ближайшее время в России заработает центр реагирования на инциденты в сфере информационной безопасности (CERT), созданный «Лабораторией Касперского» для сбора информации об уязвимостях и отражении атак на такие объекты, как атомные электростанции, предприятия ядерно-топливного, нефтегазового и энергетического комплексов. CERT-GIB (Computer Emergency Response Team — Group-IB) — центр круглосуточного реагирования на инциденты информационной безопасности.

CERT будет собирать информацию о найденных уязвимостях, угрозах, инцидентах, а также привлекаться к проведению обследований, тестов на проникновение и расследований инцидентов на промышленных объектах.

Заключение

В настоящее время риски киберпространства приобретают все больший вес и обеспечение кибербезопасности становится серьезной задачей для любого развитого государства. Атаки на промышленные системы стали важнейшей угрозой, которая носит глобальный характер и представляет опасность не только для экономики, но и для безопасности обеспечения жизнедеятельности населения.

Актуальность темы цифрового суверенитета РФ продолжит расти, особенно в связи с обострением в отношениях с Западом и введением санкций в отно-

шении России. Отсюда — приоритетность информационной безопасности критически важных объектов.

Проблема кибербезопасности в нашей стране стоит особенно остро во многом из-за слабой нормативно-правовой базы. Фактически сформулированный и закрепленный целостный подход к национальной проблематике кибербезопасности на сегодняшний день отсутствует.

Сегодня все больше предприятий понимают серьезность киберугроз, более того, киберугрозы, например, критической энергетической инфраструктуре признаются реальными на уровне регулирующих органов. Например, в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 31 декабря 2015 г., обращается внимание на угрозы критической информационной инфраструктуре Российской Федерации.

МЧС России в Прогнозе чрезвычайной обстановки на территории Российской Федерации на 2016 г. от 24.12.2015 г. выделяет кибертерроризм относительно энергетических объектов России. В прогнозе отмечается, что в настоящее время уровень информационной безопасности не соответствует уровню угроз в данной сфере и в 2016 г. возможно повышение числа хакерских атак с целью создания условий для возникновения техногенных ЧС. Отмечается, что из промышленных объектов наиболее уязвимы при хакерских атаках энергетические и коммуникационные сети России.

Литература

1. Шапинская Е. Н. Человек XXI века на просторах киберпространства: безграничные возможности и новые опасности. http://gigabaza.ru/doc/4749.html
2. Развитие интернета в регионах России. Весна 2016. https://yandex.ru/company/researches/2016/ya_internet_regions_2016
3. Защита ключевых систем информационной инфраструктуры. http://ace-net.ru/security/sec-facility.html
4. Царев Е. Нормативная база защиты критически важных объектов (КВО). http://www.securitylab.ru/blog/personal/tsarev/23617.php
5. Безопасность ключевых систем информационной инфраструктуры: точка доверия. https://securelist.ru/analysis/obzor/131/bezopasnost-klyuchevy-h-sistem-inform/
6. Пискунова Н. Кибербезопасность и атомная энергетика: все еще предстоит // Индекс безопасности. 2014. № 1 (108). Т. 20.
7. Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века. Ч. 1 // Вопросы кибербезопасности. 2013. № 1.
8. Неманья Никитович. Стратегия и тактика кибервойн: в ожидании серьезных межгосударственных конфликтов // Information Security/Информационная безопасность. 2013. № 5.
9. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. 2013 г. www.scrf.gov.ru/documents/6/114.html
10. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, 8 мая 2015 года, Москва.
11. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.
12. Цирлов В. Л. Правовые основы кибербезопасности Российской Федерации // Правовая информатика. 2014. Вып. № 3.
13. Кибербезопасность и управление Интернетом: Документы и материалы для российских регуляторов и экспертов / Отв. ред. М. Б. Касенова. М.: Статут, 2013.
14. Клименский М. М. Кибербезопасность: существующие угрозы и проблемы ее обеспечения на современном этапе. https://pglu.ru/upload/iblock/70f/kiberbezopasnost-sushchestvuyushchie-ugrozy-i-problemy-ee-obespecheniya-na-sovremennom-etape.pdf

Сведения об авторе

Соколов Юрий Иосифович: старший научный сотрудник 6 Центра ФГУ ВНИИ ГОЧС (ФЦ) МЧС России

Число публикаций: более 200

Область научных интересов: риски ЧС и высоких технологий

Контактная информация:

Адрес: 121352, г. Москва, ул. Давыдковская, д. 7

Тел.: +7(495) 413-84-50

E-mail: soko-718@rambler.ru

УДК 330.131.7

ISSN 1812-5220

Риски Брекзита

О. В. Хмыз,
Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации

Аннотация

В статье анализируются уже наступившие и вероятные последствия исторического решения Великобритании о выходе из Европейского Союза, приводящие к появлению и обострению национальных, региональных и глобальных рисков.

Ключевые слова: риск, Брекзит, Великобритания, Европейский Союз, Германия, Лондон, Франкфурт, финансовый риск, валютный риск, процентный риск, рынки капитала, валютный курс, финансовые рынки, бюджет, фунт, доллар, евро.

Содержание

Введение

16 сентября 2016 г. впервые встреча в верхах ЕС в Братиславе прошла без участия Великобритании. На этой встрече очерчивалось будущее ЕС после Брекзита. Брекзитом (от англ. Britain Exit, или выход Великобритании из Европейского Союза) называется процедура, инициированная этой страной после принятия соответствующего решения на всенародном референдуме, который состоялся 23 июня 2016 г. и на котором более 50% принявших участие граждан изъявили свою волю отделиться от Европейского Союза. Многие экономисты и политики, представители разных государств неоднократно критиковали политику Брюсселя, но только британцы воплотили словесные выпады в жизнь. И уже в сентябре 2016 г. на встрече А. Меркель, Ф. Олланда и М. Ренци, представителей крупнейших государств ЕС, были обновлены обещания о сотрудничестве. Причем их встреча состоялась в символичном для Европейского Союза месте — на острове Вентотене, фактическом месте возникновения будущего союза — именно на этом острове в 1941 г. политзаключенные режима Муссолини написали манифест об объединенной Европе. И в 2016 г. на борту «Гарибальди», флагманского корабля миссии ЕС, все трое политиков говорили, что Европа становится более сильной и сплоченной, что выход Великобритании из Европейского Союза не окажет серьезного негативного влияния ни на европейскую экономику, ни на политику [1].

Однако многие эксперты (и экономисты, и политики) с этими заключениями не согласны. И евроскептики, и еврооптимисты видят значительное число разнообразных рисков, с которыми неминуемо (в случае реализации Брекзита, запланированного на март 2017 г., или в случае отказа от продолжения действий по выходу Великобритании из Европейского Союза) столкнутся и сам Европей-

ский Союз, и Великобритания. Окажут они свое влияние и на всю мировую экономику, ведь после такого прецедента меняется само восприятие интеграционных группировок со стороны международного сообщества.

1. Риски экономической политики Европейского Союза и европейской интеграции

Сам факт, что граждан самой консервативной европейской страны вынудили сделать самый радикальный политический шаг за последние 20 лет, свидетельствует об исключительности ситуации, приведшей к нему. ЕС за годы своего существования трансформировался из организации, выгодной для всех членов, в институт по охране интересов малого числа государств-членов в ущерб остальным. Достаточно посмотреть на существовавшие ранее формы сотрудничества в Европе, начиная с Европейского экономического сообщества или Центрально-Европейской зоны свободной торговли, — эти объединения возникли для обеспечения экономической интеграции на базе единого рынка, что было выгодно для многих европейских стран. Но как только экономические институты становились политическими и начинали разрабатывать совместную внешнюю политику, раздувать чиновничий аппарат, наделяя его решающими компетенциями (тогда как Европейский парламент до сих пор не получил законодательной инициативы), становилось ясно, что нарастают риски глобального характера, ведь фактически речь идет о создании европейского супергосударства. Неважно, ставилась ли при этом экономическая цель противопоставить евро доллару, это имело бы смысл с финансовой точки зрения. Но как только Европейский Союз стал институтом, строящим собственную государственность, не отражающим при этом интересы всех стран-членов, и особенно после принятия Лиссабонского соглашения [2], которое в решающих процедурах не учитывало интересы некоторых стран Союза, стало ясно, что дни Союза сочтены в обозримом будущем. Стоило подлить немного миграционного масла, и огонь разгорелся.

Интересно, что, по оценкам, выход Великобритании из Европейского Союза может оказать более серьезное негативное влияние на европейскую экономику, чем наоборот. Прежде всего поскольку Великобритания является одним из главных торговых партнеров других стран Европейского Союза (в т. ч. ведущих), ЕСовские финансовые потоки также в значительной степени (40%) приходят из Великобритании. Доля лондонского Сити в европейском финансовом рынке велика и составляет 25% банковских активов, 43% валютной торговли, 51% страхования морских перевозок, 70% внебиржевой торговли деривативами, 85% активов хеджевых фондов и др. [3]. Следовательно, Брекзит, или приостановление или сжатие этих потоков, приведет к ухудшению состояния платежного баланса Европейского Союза, усугубив и без того немалое число внутриесовских проблем — экономических, финансовых и политических. Свой негативный вклад в развитие европейской экономики внес и глобальный финансово-экономический кризис 2007—2008 гг., но тем же Штатам удалось выйти из него быстрее [4, с. 6], чем Европейскому Союзу, в котором кризис перерос в долговой, причем не только в странах PIIGS, но и в наиболее развитых — у Германии долговая нагрузка превысила 150% ВВП, а у Франции вплотную подошла к 250% [5, с. 107—108]. И при этом Европейский Союз продолжает процессы финансовой энтропии, следуя интенсивной модели роста. Впрочем, в связи с Брекзитом ужесточились и требования ЕС к своим новым членам, в т. ч., например, к вышеградской четверке, страны которой в соответствии с проектом о реформировании Европейского Союза от 27 июня 2016 г. [6] фактически должны отказаться от национального суверенитета в военно-политической и экономико-финансовой областях. То есть Европейский Союз все ближе подходит к единому европейскому супергосударству (уже отмечается централизация монетарной политики), что противоречит его первоначальным целям и обостряет центробежные силы в ЕС, ведь для усиления Европейского Союза и евро необходима локальная европейская глобализация вокруг Брюсселя, а не Германии. А это сложно даже с учетом только греческого кризиса и соответственно Грекзита. Греческое руководство неоднократно заявляло о своих намерениях вывести страну из Европейского Союза, поскольку не только национальный финансовый сектор, но и вся

национальная экономика стоит на пороге краха. Однако в отличие от более развитой (в особенности в финансовой сфере) Великобритании Греции это сделать сложнее, ее экономика в значительной степени интегрирована в европейскую, и от национальной валюты греки отказались, получая взамен финансовую поддержку других стран Союза. К ноябрю 2016 г. Греция финализировала первый этап спасательной программы лета 2015 г., но на очереди второй, более сложный, затрагивающий социальное обеспечение и пенсионную систему. Руководство страны надеется на прощение части долгов, заявляя о возможности бездефицитного сведения бюджета. Но по оценкам экспертов бюджетный дефицит составит 0,15—0,2% ВВП страны, что приведет к необходимости сокращения расходов в размере минимум 360 млн евро, чего можно добиться либо сжатием социальных расходов, либо увеличением налогов, т. е. непопулярными мерами. Некоторые экономисты в этой связи предлагают Греции временно вернуться к драхме, но в сочетании со списанием ее государственного долга, как в свое время поступила Аргентина [7, с. 173], и это станет новым решением в сочетании с программой устойчивого развития. Без списания долга Греция останется в паутине, и выполнение третьего этапа программы будет под вопросом. Для восстановления суверенитета Греции либо нужно коренным образом реформировать сам союз, либо стране придется выйти из него. Сейчас Греция борется за возвращение на рынки капитала и за участие в программе количественных смягчений Европейского центрального банка. А поскольку Греция — часть Европейского Союза, все эти неурядицы затрагивают и сам Союз.

В отличие от Греции Великобритания практически все время проводила собственную политику. Так, в 1949 г. был создан Совет Европы, а единая европейская конституция принята не была, в 1950 г. Европейскому объединению угля и стали англичане противопоставили план Макмиллана — Эклза, в 1951 г. страна отказалась подписать договор о Европейском оборонительном сообществе, в 1956 г. Общему рынку противопоставила план западноевропейской интеграции, в 1985 г. отказалась войти в Шенгенскую зону, в 2003 г. отказалась вступить в зону евро, в 2011 г. отказалась участвовать в создании фискального союза ЕС, в 2013 г. — в банковском союзе и др.

И сегодня мы видим, как на фоне британских действий набирает силу евроскептицизм в Германии, Франции, Нидерландах и других странах — прежде всего в государствах-донорах, предоставляющих значительные финансовые ресурсы в европейский бюджет. Именно Великобритания, Германия и Франция перечисляли самое большое количество средств [8]. А после своего выхода Великобритания перестанет делать взносы (в размере 18 млрд евро, как в 2015 г.), что окажется чувствительным для бюджета Европейского Союза. Поэтому Брекзит не следует рассматривать как случайность, нивелирующую блага европейской интеграции. Щепетильный Лондон фактически так и не избавился от традиционного недоверия к континентальной Европе и имперских замашек. Сегодняшняя ориентация постколониальных государств на заморскую сверхдержаву базируется на многолетнем сотрудничестве, в том числе военном, в разных частях света. Это может привести к изменению финансового миропорядка, ведь подписание договора о трансатлантическом торговом и инвестиционном партнерстве, которое за закрытыми дверями готовится Брюсселем уже почти два года, подрывает основополагающие принципы группировки. И хотя его подробности неизвестны, в общих чертах ясно, что будущее европейского рынка будет тесно связано с американскими корпорациями, поскольку лидеры европейских государств во время длительных переговоров вели себя сдержанно, тогда как должны были отстаивать региональные интересы.

Все эти факторы и дали возможность провести Брекзит. Но многие экономисты и политики негативно восприняли и само действо, и его идею, предсказывая Великобритании годы хаоса и экономических неурядиц. Так, по подсчетам Фонда Бертельсманна к 2030 г. финансовые потери Великобритании из-за Брекзита будут больше 300 млрд евро [9]. Причины — зависимость Великобритании от Европейского Союза: доля Европейского Союза в ВВП Великобритании составляет около 10%, в занятости — 10%, в банковских активах — 25%, в совокупном объеме зарубежных финансовых обязательств — 42%, в накопленном объеме иностранных инвестиций — 43% [10], что немало.

2. Валютно-курсовые риски

Активизировались и международные валютные спекулянты. 4 октября 2016 г. валютный курс фунта стерлингов из-за опасений возможных последствий Брекзита вышел по отношению к американскому доллару на новый рубеж, обновив минимум за последний 31 год. Его значение опустилось ниже уровня после июльского референдума о выходе Британии из Европейского Союза. За несколько часов падение превысило 0,5% и курс достиг 1,2757 доллара (это минимальное значение с июня 1985 г.). Падение началось 3 октября 2016 г. и составило 1,3% с минимума, показанного в начале июля. Таким образом, с момента голосования о Брекзите фунт потерял к доллару около 15% (по данным Рейтер) [11], реагируя на заявление британского премьер-министра Т. Мэй о начале официального процесса выхода из ЕС — самое позднее в конце марта 2017 г. [12]. Многие инвесторы опасаются сценария «жесткого Брекзита» [13] (табл. 1), согласно которому Британия может выйти из единого рынка, чтобы сохранить контроль над иммиграцией. Это могло бы вызвать уход ряда банков из Лондона и подорвать торговые отношения с ЕС. В обоих сценариях предусмотрена 15%-я девальвация фунта, но «мягкий» предполагает умеренное и краткосрочное влияние, тогда как «жесткий» — более значительное и соответственно более продолжительный период неопределенности.

До марта 2017 г. Т. Мэй хочет активировать ст. 50 Лиссабонского договора и тем самым начать минимум двухлетние переговоры о выходе Британии из ЕС, выторговав для своей страны лучшие условия. Островная экономика будет бороться с потрясениями, вероятно, ее ожидают несколько лет нестабильности. Но после Брекзита Британия опять станет независимой и суверенной страной, хотя ей и придется строить новые отношения с Европейским Союзом. С одной стороны, страна не будет ориентироваться на швейцарскую или норвежскую модель. С другой — британские законы не будут интерпретировать судьи из Люксембурга. Получается партнерство с Европейским Союзом, но собственные решения.

Все это может оказать серьезное влияние и на мировую экономику, как дестабилизирующее, так и наоборот. Фунт стерлингов испокон веков был одной из наиболее значимых валют для мировой экономики и международных финансов, и лишь в середине XX века он уступил свои ведущие позиции американскому доллару. Но и сегодня фунт занимает четвертое место в обороте мирового валютного рынка [15, p. 10], третье — в официальных международных резервах [16]. Лондон занимает первое место среди ведущих международных финансовых центров мира [17, p. 4], несмотря на усиление международной конкуренции в свете глобализации мировой экономики. И неблагоприятные тенденции из этой страны, даже по мнению Международного валютного фонда, могут отразиться на многих странах мира (табл. 2).

Более того, Брекзит может привести к росту геофинансовой значимости Британии, и в новых условиях она может начать возвращаться к роли веду-

Влияние девальвации фунта стерлингов на ВВП, % *Таблица 1*

Страна/Регион	«Мягкий» сценарий		«Жесткий» сценарий	
	2016	2017	2016	2017
Великобритания	–0,3	–0,9	–0,6	–2,6
Зона евро	–0,1	–0,2	–0,2	–0,5
ЕС-27	0	–0,2	–0,2	–0,5

Источник: [14].

Прогнозируемый Международным валютным фондом рост ВВП, % *Таблица 2*

Страна/Регион	Прогноз апреля 2016 г.		Прогноз июля 2016 г.	
	2016	2017	2016	2017
США	2,4	2,5	2,2	2,5
Великобритания	1,9	1,2	1,7	1,3
Зона евро	1,5	1,6	1,6	1,4
Германия	1,5	1,6	1,6	1,2
Франция	1,1	1,1	1,5	1,2

Источник: [18].

щего государства, ведь эту роль она утратила в т.ч. из-за членства в этом аморфном союзе. А фунт мог бы усилить свои позиции на мировом валютном рынке, вспомнив, что в позапрошлом и начале XX века он был доминирующей ключевой валютой. Все это содействовало бы укреплению позиций лондонского международного финансового центра и национального финансового рынка.

В связи с этим интересно, не станет ли Британия создавать новое европейское сообщество, основанное на экономическом и валютно-финансовом сотрудничестве, во главе которого и встанет? А оно может быть выгодным для многих, если будет опираться не на политическую волю, а на реальные экономико-финансовые условия.

Брекзит также дает Британии еще одну формальную возможность — создавать новый валютный союз, основанный на принципах равноправного сотрудничества, как предлагал в свое время Дж. М. Кейнс и как это было в начале европейской интеграции, пока в ней не стало формироваться ядро (из шести стран-основателей — Германии, Франции, Италии, Нидерландов, Бельгии и Люксембурга, которые уже проводят совещания в узком кругу).

В любом случае решение государства, традиционно имевшего важное значение для мировой экономики и международных финансов, является ощутимым ударом по самой идее европейской интеграции [19] и становится прецедентом, первым, но, вероятно, не единственным — все больше сторонников получает теория секулярной стагнации [20] и антиглобализма [21]. Брекзит уже повысил волатильность на мировом финансовом рынке. Прежде всего это относится к колебаниям (преимущественно в сторону падения) курсов акций ведущих банков мира (HSBC, BNP Paribas, Deutsche Bank, Sosiete Generale, UniCredit Bank, Kommerz-Bank, Santander, Iteza). Конечно, ситуация связана не только с Брекзитом, но и со спекулятивными операциями самих банков, но и Брекзит внес свой вклад. Повышенная волатильность может быть связана с опасениями перехода финансовой активности из Лондона во Франкфурт и из Франкфурта в Лондон.

Скептики указывают на непредсказуемость последствий Брекзита, которые в худшем случае могут привести к расколу Европы и даже к хаосу в Старом Свете, что негативно отразится на всей мировой экономике и международных финансах. В качестве аргумента приводятся уже ставшие явными задержки и проблемы при разработке соглашения о Транстихоокеанском торговом и инвестиционном партнерстве. Со своей стороны, Северная Ирландия, Гибралтар (стратегически важный транспортный пункт) и Шотландия остались недовольны результатами референдума 24 июня и выразили свое желание присоединиться к Ирландии, Испании соответственно, а Шотландия — приобрести автономность. В связи с этим даже фунт стали называть оппозицией британскому правительству Т. Мэй, предсказывая, что до конца следующего года его курс может ослабеть до 1,10 долл. В любом случае и фунт, и лондонский международный финансовый центр традиционно имели важное значение для мировой экономики. Даже МВФ считает, что воздействие Брекзита на мировую экономику будет проявляться постепенно, содействуя прежде всего финансовой и экономической неопределенности, а реакция финансовых рынков на этот шок будет возрастать [22].

Заключение

Экономико-финансовые последствия и риски Брекзита можно сгруппировать в виде последствий и рисков для Великобритании, для Европейского Союза, для третьих стран и всей мировой экономики и системы международных финансов в целом.

Для Великобритании главное негативное последствие — повышение волатильности валютного курса фунта стерлингов, что в интересах прежде всего международных спекулянтов.

Для Европейского Союза Брекзит может стать поводом для обострения валютно-финансовых проблем в затянувшейся рецессии и в итоге вылиться в дезинтеграцию. Поэтому представители промышленности и финансисты хотят оставить Британию в Европейском Союзе, опасаясь крупных убытков во взаимной торговле. Более того, если Британия выйдет, другие государства могут захотеть для себя особых правил (так, даже Техас изъявил желание выйти из США). Также появляется опасность формирования в Европейском Союзе центрального ядра (Германия и Франция) и периферического (во главе с Польшей). В любом случае остаются вопросы отношений с Великобританией,

решившей начать переговоры о выходе, слабости экономического сотрудничества, служащего цементирующей базой для евро, а также проблемы внутренней безопасности и фрагментарности. Тремя приоритетами нового начала объединенной и сильной Европы после Брекзита названы безопасность, инвестиции и возможности молодежи.

В мировой экономике Брекзит приведет к снижению темпов роста, ужесточению условий и требований к работе на финансовых рынках, перемещению финансовой активности. Это усилит финансовую напряженность, особенно в Европе, и может привести к серьезным негативным последствиям для всей системы международных финансов.

В целом выхода одного государства (даже столь значимого, как Великобритания) для распада Европейского Союза недостаточно, но политика Союза продолжает подвергать испытаниям его экономику. Главное, чтобы эти действия не разрушили «Храм мира» У. Черчилля.

Литература

1. Sommella Di R. Vertice Ventotene: Renzi, Merkel, Hollande insieme per sconfiggere la paura di Euxit // L'huffington post. 21.08.2016. [Electronic resource] Mode of access URL: http://www.huffingtonpost.it/2016/08/21/ventotene-vertice_n_11641032.html (accessed 23.09.2016)
2. The Lisbon Treaty [Electronic resource] Mode of access URL: http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-the-functioning-of-the-european-union-and-comments.html (accessed 13.09.2016)
3. Key Facts about UK Financial and Related Professional Services 2016. The City of UK. [Electronic resource] Mode of access URL: https://www.thecityuk.com/assets/2016/Reports-PDF/Key-facts-about-UK-financial-and-related-professional-services-2016.pdf (accessed 17.11.2016)
4. Портной М. А. Финансовый кризис в США: причины, масштабы, последствия // США и Канада: экономика, политика, культура. 2008. № 12. С. 4—18.
5. Звонова Е. А. Современные проблемы государственных долгов и суверенных дефолтов в странах Евросоюза // Вестник Финансового университета. 2016. Т. 20. № 4. С. 105—117.
6. Assessing the implementation of the EU Framework for National Roma Integration Strategies and the Council Recommendation on effective Roma integration measures in the Member States — 2016. Brussels, 27.6.2016. [Electronic resource] Mode of access URL: https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-424-EN-F1-1.PDF (accessed 17.11.2016)
7. Мировая экономика и международные экономические отношения / Под ред. А. С. Булатова, Н. Н. Ливенцева. М.: Магистр, 2008. 654 с.
8. Kirkup J. EU Facts: how much does Britain pay to the EU budget? // The Telegraph. 2016. November, 19. [Electronic resource] Mode of access URL: http://www.telegraph.co.uk/news/newstopics/eureferendum/12176663/EU-Facts-how-much-does-Britain-pay-to-the-EU-budget.html (accessed 21.11.2016)
9. BREXIT could be expensive — especially for the United Kingdom… [Electronic resource] Mode of access URL: https://www.bertelsmann-stiftung.de/en/topics/aktuelle-meldungen/2015/april/brexit-could-be-expensive-especially-for-the-united-kingdom/ (accessed 25.11.2016)
10. UK balance of payments statistics. Office for National Statistics. [Electronic resource] Mode of access URL: https://www.ons.gov.uk/economy/nationalaccounts/balanceofpayments/datasets/balanceofpaymentsstatisticalbulletintables (accessed 14.11.2016)
11. Leong R. Sterling hits 31-year low; report on ECB helps euro // Reuters Business News. 2016. October, 4. [Electronic resource] Mode of access URL: http://www.reuters.com/article/us-global-forex-idUSKCN12401D?il=0 (accessed 11.10.2016)
12. Price R. BREXIT: Theresa May will trigger Article 50 before the end of March 2017 // Business Insider UK. 2016. October, 2. [Electronic resource] Mode of access URL: http://uk.businessinsider.com/r-uk-pm-says-will-begin-brexit-process-before-german-election-sunday-times-2016-10 (accessed 12.10.2016)
13. Hollande demands tough Brexit negotiations. // Financial Times. 2016. October, 6.
14. Cave S., Allen M. Possible models for the UK-EU relationship post 'Brexit' [Electronic resource] Mode of access URL: http://www.niassembly.gov.uk/globalassets/documents/raise/publications/2016-2021/2016/aera/4716.pdf (accessed 12.10.2016)
15. Triennial Central Bank Survey. Bank for International Settlements, 2016. September.
16. Share of national currencies in total identified official holdings of foreign exchange, end of year 2016. Washington DC: International Monetary Fund. 2016. [Electronic resource] Mode of access URL: http://data.imf.org/?sk=E6A5F467-C14B-4AA8-9F6D-5A09EC4E62A4 (accessed 22.11.2016)
17. The Global Financial Centres Index 20. Long Finance, 2016. September.

18. Uncertainty in the Aftermath of the U.K. Referendum. Washington DC: International Monetary Fund. 2016. July [Electronic resource] Mode of access URL: https://www.imf.org/external/pubs/ft/weo/2016/update/02/ (accessed 22.11.2016)
19. Сумароков В.Н. Европейская интеграция: испытание кризисом // Экономические науки. 2012. № 97. С. 185—191.
20. Summers L. Why stagnation might prove to be the new normal // Financial Times, 2013. December, 15.
21. FT Banking Summit 2016. Security, Agility and Resilience in Volatile Times. London, 2016. November, 16.
22. Brexit throws 'spanner in the works' of global growth // BBC News. 2016. July, 19. [Electronic resource] Mode of access URL: http://www.bbc.com/news/business-36834977 (accessed 25.06.2016)

Сведения об авторе

Хмыз Ольга Васильевна: кандидат экономических наук, доцент, доцент кафедры международных финансов Московского государственного института международных отношений (университета) Министерства иностранных дел Российской Федерации

Количество публикаций: 277 научных, 98 учебных и учебно-методических

Область научных интересов: международное движение капиталов, международные финансы

Контактная информация:

Адрес: 119454, г. Москва, пр-т Вернадского, д. 76

Тел.: +7 (495) 434-60-10

E-mail: khmyz@mail.ru

УДК 336

ISSN 1812-5220

Индексный подход к оценке страновых рисков реальных инвестиций

И. В. Демкин,
Д. А. Власов,
А. О. Габриелов,
В. Д. Бархатов,
ООО «НИИгазэкономика», г. Москва
Н. В. Лукьянович,
Финансовый университет при Правительстве РФ, г. Москва

Аннотация
Глобализация мировой экономики заставляет промышленные компании выходить на международные рынки, реализуя инвестиционные проекты и конкурируя за ограниченные ресурсы и рынки сбыта в зарубежных странах. Перед компаниями встает задача оценки страновых рисков с целью выбора перспективных стран с приемлемым уровнем риска. Данная работа посвящена разработке подхода к качественной оценке странового риска при определении перспективных стран для инвестирования.

Ключевые слова: оценка рисков, страновой риск, индексы развития стран, кредитные рейтинги.

Содержание

Введение

Оценка рисков является неотъемлемой частью инвестиционного анализа, а ее результаты должны играть ключевую роль при принятии инвестиционных решений. Серьезной проблемой при учете рисков инвестиционных проектов является количественная оценка страновых рисков, особенно актуальная при формировании программы инвестиций промышленной компании в зарубежные активы. Страновые риски связаны с возможными потерями доходов промышленных компаний вследствие как возможного дефолта, так и снижения уровня государственного управления в стране, выбранной для инвестирования. Как показывает мировая практика, некорректная оценка таких рисков в ряде случаев приводит к существенным потерям части доходов или сверхплановым затратам для компании (например, косвенные потери компании в случае невозможности перевода полученных доходов из страны, выбранной для инвестирования) или даже потере всего бизнеса (например, в случае проведения национализации собственности в стране, выбранной для инвестирования). Вместе с тем к настоящему времени наблюдается определенный дефицит подходов к оценке страновых рисков. Большая часть из них оценивает лишь одну из составляющих странового риска — риск дефолта

страны, что приводит к недооцениванию странового риска. На наш взгляд, в основу комплексного многофакторного подхода к качественной оценке страновых рисков целесообразно положить индексный метод. Однако трудности его использования связаны, во-первых, с обоснованием выбора совокупности используемых индексов и, во-вторых, с их корректным применением в ходе качественной оценки странового риска. В ходе проведенных исследований были решены обе поставленные задачи. Полученные результаты были апробированы в ходе оценки страновых рисков 33 возможных для инвестирования стран одной из российских промышленных компаний.

1. Анализ основных подходов к оценке страновых рисков

История последних финансовых кризисов, происшедших в странах Азии, России, Бразилии и приведших к значительным потерям иностранных инвесторов, показала преимущества и недостатки существующих подходов к оценке страновых рисков. Существующие в настоящее время подходы к их количественной оценке можно разделить на:

- подходы, основанные на использовании кредитных рейтингов и индексов [1—3];
- подходы, основанные на вычислении спредов доходностей суверенных облигаций и иных финансовых инструментов оценки риска [4—6].

Вышеперечисленные подходы имеют определенные недостатки, снижающие их эффективность. Так, значения кредитных рейтингов подвержены влиянию таких факторов, как ангажированность значений рейтингов отдельных стран, неполный учет национальной специфики и субъективность ряда получаемых оценок. Методики, основанные на вычислении спредов доходностей облигаций и других финансовых инструментов, в свою очередь, обладают такими недостатками, как отсутствие суверенных облигаций (финансовых инструментов) ряда стран, сложности подбора облигаций (финансовых инструментов) некоторых стран (например, номинирование облигаций только в локальной валюте; разница в параметрах сравниваемых облигаций).

К числу наиболее известных подходов, основанных на вычислении спредов доходностей суверенных облигаций и иных финансовых инструментов оценки риска, можно отнести подход, разработанный А. Дамодараном [4]. Автор предлагает рассчитывать премию за страновой риск на основе зависимости суверенного рейтинга S&P Global или Moody's (в случае отсутствия значения рейтинга S&P Global) и спредов кредитных дефолтных свопов[1] (далее — CDS). Основным и наиболее значимым ограничением предлагаемого подхода является отсутствие долгосрочных CDS, а также их малая ликвидность. А. Дамодаран использует десятилетние CDS, что в значительной степени искажает результаты расчета премии за риск дефолта многих проектов, например нефтегазовой отрасли, ввиду более длительного их жизненного цикла (как правило, жизненный цикл нефтегазовых проектов составляет 30 и более лет). Более того, автор предлагает использовать кредитные рейтинги стран в местной валюте, тем самым увеличивая ошибку результатов, связанную с игнорированием инфляционных процессов местных валют.

К общему недостатку вышеперечисленных подходов к оценке странового риска относится предпосылка о распространении результатов оценки риска дефолта страны на совокупный страновой риск для компаний, размещающих реальные инвестиции за рубежом.

Таким образом, актуальным на сегодняшний день является разработка методического подхода оценки странового риска, позволяющего в определенной степени устранить недостатки существующих подходов.

2. Основные факторы, влияющие на уровень странового риска

Под страновым риском будем понимать риск потерь промышленной компании в результате ее прямого инвестирования в международные проекты, периметры которых связаны с определенной зарубежной страной.

В первую очередь целесообразно определить основные факторы, влияющие на страновой риск. Проведенный анализ показал, что основные из них условно можно разделить на две группы:

1) факторы, влияющие на риск последствий дефолта страны на компанию, размещающую в ней инвестиции (далее для простоты — риск дефолта);

[1] Кредитный дефолтный своп является производным финансовым инструментом (деривативом), страхующим эмитента от дефолта по долгам.

2) факторы, вызванные возможными односторонними негативными действиями со стороны правительства страны размещения инвестиций или иных сил.

Перечень основных факторов влияния каждой из групп приведен в табл. 1 и 2 соответственно. Стоит отметить, что в табл. 2 факторы, вызванные односторонними негативными действиями со стороны правительства страны размещения инвестиций или иных сил, представлены в виде факторов первого и второго уровней. Целесообразность подобного представления вызвана невозможностью прямого (непосредственного) оценивания факторов первого уровня второй группы ввиду недостаточности статистических данных для такого оценивания и отсутствия необходимого числа экспертов, обладающих соответствующими компетенциями.

Факторы страновых рисков, представленные в табл. 1 и 2, в случае их реализации могут привести к потере доходов, росту затрат или даже к полной потере всей собственности компании и отказу от реализации иностранных проектов.

Основные факторы, влияющие на риск дефолта в стране размещения инвестиций *Таблица 1*

№ п/п	Основные факторы
1	Увеличение отношения общего долга к ВВП страны
2	Усиление инфляционных и девальвационных процессов в стране
3	Наличие дефолтной истории страны
4	Соотношение обязательств в национальной и иностранной валютах (структура долга) страны
5	Большее значение суммы долга по отношению к сумме годового экспорта страны
6	Ухудшение структуры задолженности (невозможность реструктуризации долга, требования эмитентов облигаций о преждевременных выплатах по облигациям)
7	Снижение ВВП страны размещения инвестиций
8	Уменьшение отношения золотовалютных резервов к сумме импорта страны
9	Технологические и финансово-экономические санкции по отношению к странам
10	Хронический дефицит бюджета страны

Основные факторы, вызванные односторонними негативными действиями со стороны правительства страны размещения инвестиций или иных сил *Таблица 2*

№ п/п	Негативные действия со стороны правительств стран размещения инвестиций (факторы первого уровня)	Политические факторы, оказывающие влияние на факторы первого уровня (факторы второго уровня)
1	Одностороннее изменение параметров соглашений правительством или национальной компанией *(например, установление требований по обязательной продаже продукции на внутреннем рынке по нерыночным ценам, наложение штрафов, схем налогообложения, изменение требований комплексной безопасности и проч.)*	Изменение уровня демографического давления Изменение уровня миграции беженцев Появление/изменение недовольных и мстительно настроенных групп Изменение уровня эмиграции из страны Неравномерность экономического развития Изменение уровня экономической нестабильности Изменение уровня делегитимизации и криминализации государственных структур Наличие и качество общественных услуг Изменение уровня нарушения прав человека Изменение уровня влияния аппарата государственной безопасности в качестве «государства в государстве» Изменение уровня влияния групповых и (или) клановых элит Изменение степени вмешательства других государств или внешних политических субъектов, а также МЭ и ФО Изменение инвестиционного законодательства Активизация/спад активности террористических атак
2	Полная или частичная национализация собственности компании	
3	Наложение ограничений на движение капитала *(введение ограничений на вывоз капитала, изменение ставок, установление фиксированных валютных курсов)*	
4	Эмбарго на ввоз и вывоз товаров из страны	
5	Невозможность заимствования на ряде рынков капитала на определенные сроки, ограничение в использовании эффективных технологий	

3. Предложения по качественной оценке страновых рисков с использованием индексного подхода

В настоящее время разработано большое количество индексов, используемых для качественной оценки политических, экономических, финансовых, социальных и прочих факторов страновых рисков [1]. Основные из них представлены на рис. 1 справа.

Для отбора релевантных индексов для целей качественной оценки странового риска предлагается использовать критерии, представленные в табл. 3.

На основе требований, указанных в табл. 3, был осуществлен анализ основных индексов, в результате которого часть из них была исключена из дальнейшего рассмотрения. Перечень индексов, исключенных из дальнейшего рассмотрения, а также причины их отсеивания представлены в табл. 4.

Как видно из табл. 4, большая часть причин отсеивания индексов заключается в значительной доле экспертных оценок, неполноте учета составляющих странового риска и малом числе стран, в отношении которых оцениваются индексы. Основные характеристики индексов, в наибольшей степени соответствующих сформулированным выше требованиям, представлены в табл. 5 [1].

Рис. 1. Взаимосвязь основных факторов и индексов измерения странового риска

Основные критерии отбора индексов *Таблица 3*

Критерии отбора индексов	Целесообразность применения критериев отбора
Множественность учитываемых индексом индикаторов/показателей	Учет социальных, политических, экономических и финансовых аспектов странового риска
Диверсификация стран — разработчиков индексов	Снижение ангажированности оценки странового риска
Объективность оцениваемых показателей, включенных в индекс	Снижение доли экспертных оценок для минимизации влияния мнений экспертов на значения индексов (например, предпочтительным является использование таких объективных показателей, как наличие нормативных документов, процедур, подтверждающих подверженность страны отдельным аспектам странового риска)
Периодичность обновления индекса не реже чем ежегодно	Принятие релевантных управленческих решений разработчиками индексов
Международный охват индексом не менее 100 стран	Позволяет добиться увеличения числа потенциальных стран размещения реальных инвестиций

Перечень индексов, исключенных из дальнейшего рассмотрения *Таблица 4*

Наименование индекса	Причина отсеивания индекса
Political Risk Services	Индексом учитывается лишь исключительно политическая составляющая странового риска. Прогностический характер индекса
Control Risks Group	Индексом учитывается лишь исключительно политическая составляющая странового риска. Риск измеряется исключительно на основе экспертных заключений
Bank of America World Information Services	Предлагаются исторические и прогнозные значения индекса лишь для 80 государств
Business Environment Risk Intelligence	Оценка странового риска предлагается лишь для 50 стран. Базируется исключительно на экспертных оценках
Economist Intelligence Unit	Недостаточная обоснованность весовых коэффициентов, составляющих индекс. Не учитывает социальную/демографическую составляющую странового риска
Euromoney	Недостаточная обоснованность весовых коэффициентов, составляющих индекс. Не учитывает социальную/демографическую составляющую странового риска. Базируется исключительно на экспертных оценках
Institutional Investor	Оценивает риск дефолта страны. Анализирует значительно меньшее количество стран, чем агентство S&P Global. Базируется исключительно на экспертных оценках
Индекс вовлеченности стран в международную торговлю	Не учитывает социальную/демографическую составляющую странового риска. Значительная доля экспертных оценок
Индекс регуляторных ограничений для прямых иностранных инвестиций (OECD's FDI regulatory restrictiveness index)	Оценка индекса предлагается лишь в отношении 56 стран. Значительная доля экспертных оценок

Описание основных характеристик, выбранных для качественной оценки странового риска индексов *Таблица 5*

Наименование индекса	Характеристики	Описание характеристик
Индекс недееспособности государства (Failed States Index)	Направленность индекса	Индекс отражает способность властей контролировать целостность территории, а также демографическую, политическую и экономическую ситуацию в стране
	Анализируемые индикаторы (показатели)	Социальные показатели: – уровень демографического давления; – уровень миграции беженцев и (или) перемещенных лиц; – наличие недовольных и мстительно настроенных групп; – устойчивая эмиграция из страны. Экономические показатели: – неравномерность экономического развития; – уровень экономической нестабильности. Политические показатели: – уровень делегитимизации и криминализации государственных структур; – наличие и качество общественных структур; – уровень нарушений прав человека; – уровень влияния аппарата государственной безопасности в качестве «государства в государстве»; – уровень влияния групповых и (или) клановых элит; – степень вмешательства других государств или внешних политических субъектов

Таблица 5 (продолжение)

Наименование индекса	Характеристики	Описание характеристик
	Методология	Состояние недееспособности государства варьируется по шкале от 0 (низкая степень) до 10 (высокая степень). Для оценки уровня недееспособности государств выводится средний показатель на основе оценки 12 индикаторов по социальным, экономическим и политическим показателям. Итоговые значения индексов представлены в таблице, в которой страны поделены на несколько групп в соответствии с уровнем стабильности: 1) государства с высоким уровнем нестабильности (критический уровень рисков); 2) государства с уровнем стабильности ниже среднего (опасный уровень рисков); 3) государства с уровнем стабильности выше среднего (низкий уровень рисков); 4) государства с высоким уровнем стабильности (отсутствие рисков). Таким образом, чем выше значение индекса, тем более высокий риск недееспособности государства
	Период выпуска рейтинга и частота	С 2005 г. ежегодно
	Количество стран	178
	Организация, разрабатывающая индекс	Общественная организация Американский Фонд Мира; журнал Foreign Policy — США
	Адрес хранения базы данных	http://www.fundforpeace.org/global/?q=fsi2012
	Недостатки индекса	Отсутствует методика расчета итогового значения индекса, его значение подвержено субъективной оценке экспертов
Индекс легкости ведения бизнеса (Ease of doing business rank)	Направленность индекса	Представляет собой анализ количественных показателей нормативного регулирования предпринимательской деятельности, способствующего или затрудняющего ее развитие, а также степень защиты прав собственности
	Анализируемые индикаторы (показатели)	Рейтинг составляется на основе 10 индикаторов регулирования предпринимательской деятельности, а именно: – создание предприятий (количество процедур, стоимость процедур, затрачиваемое время, размер уставного капитала); – получение разрешений на строительство (количество процедур, срок, стоимость); – подключение к системе электроснабжения (количество процедур, срок, стоимость); – регистрация собственности (количество процедур, срок, стоимость); – получение кредитов (индекс юридических прав, индекс кредитной информации, количество человек на учете в государственном реестре, а также на учете в частном бюро); – защита инвесторов (индекс открытости, индекс ответственности директора, индекс возможности подачи иска акционерами, индекс защиты интересов инвесторов); – налогообложение (количество налоговых выплат, время, налог на прибыль, налог и выплаты на зарплату, другие налоги, общая налоговая ставка); – международная торговля (количество документов для экспорта, время на экспорт, стоимость экспорта, количество документов для импорта, время на импорт, стоимость импорта); – обеспечение выполнения контрактов (срок, размер судебных издержек, количество процедур); – разрешение неплатежеспособности (время, стоимость, коэффициент взыскания)
	Методология	Для определения рангов по показателям времени и движения, как правило, МБРР и МФК используют данные из официальных информационных источников (прейскуранты, законодательные и нормативные правовые акты). В случае отсутствия данных привлекаются эксперты (экономисты, юристы, чиновники и др.). В рамках каждого из индикаторов осуществляется усреднение рангов показателей, составляющих индикатор. Впоследствии для каждой из анализируемых стран значения индикаторов также подвергаются усреднению и ранжируются. Стоит заметить, что все индикаторы, а также показатели, составляющие индикаторы, имеют одинаковые весовые коэффициенты. Так, чем выше итоговый ранг, тем более привлекательной является страна

Таблица 5 (продолжение)

Наименование индекса	Характеристики	Описание характеристик
	Период выпуска рейтинга и частота	С 2005 г. ежегодно
	Количество стран	189
	Организация, разрабатывающая индекс	Международный банк реконструкции и развития Всемирного банка (МБРР) и Международная финансовая корпорация (МФК) — США
	Адрес хранения базы данных	http://www.doingbusiness.org/rankings
	Недостатки индекса	Анализ данных по самым крупным городам страны, анализ предприятий лишь с формой собственности «ООО», незначительная подверженность субъективности оценки
Международный справочник страновых рисков (International Country Risk Guide)	Направленность индекса	Рейтинги стран используются для прогнозирования рисков (политических, экономических и финансовых) международных корпораций. Причем предлагается не просто оценка значимости индекса в перспективе (через 1 год, 5 лет), но и уровень влияния индекса на процесс реализации инвестиционного проекта сейчас и в будущем
	Анализируемые индикаторы (показатели)	Рейтинги составляются на основе 3 индексов рисков: политический, экономический, финансовый. Каждый из индексов, в свою очередь, состоит из некоторого количества определяющих показателей. Перечень и балльная шкала показателей, составляющих индекс оценки политических рисков: – стабильность государственного управления (0—12); – социально-экономические условия существования государства (0—12); – инвестиционный профиль (0—12); – наличие внутренних конфликтов (0—12); – наличие внешних конфликтов (0—12); – уровень коррупции (0—6); – военная сила в политике (0—6); – религиозная напряженность (0—6); – закон и порядок (0—6); – этническая напряженность (0—6); – демократическая ответственность (0—6); – качество бюрократии (0—4). Перечень и балльная шкала показателей, составляющих индекс оценки экономических рисков: – ВВП на душу населения для текущего года (0—5); – реальный рост ВВП (0—10); – ежегодный уровень инфляции (0—10); – бюджетный баланс (0—10); – торговый баланс страны (0—15). Перечень и балльная шкала показателей, составляющих индекс оценки финансовых рисков: – внешний долг в текущем году (0—10); – внешний долг на услуги относительно экспорта и импорта товаров и услуг (0—15); – текущий платежный баланс как процент от экспорта продуктов и услуг (0—15); – ликвидность (0—5); – стабильность обменного курса валют (0—5)

Таблица 5 (*продолжение*)

Наименование индекса	Характеристики	Описание характеристик
	Методология	Итоговый индекс оценки странового риска рассчитывается с использованием следующих весовых коэффициентов каждого из 3 индексов: 50% экономический риск, по 25% политический и финансовый риски. Причем политический риск измеряется по 100-балльной шкале, а остальные риски по 50-балльной. Шкала оценивания каждого из параметров представлена в характеристике «Анализируемые индикаторы (показатели)». Прежде всего оценке поддаются показатели рисков, после чего полученные оценки сводятся в единый индекс риска. Стоит заметить, что политический риск рассчитывается преимущественно на основе субъективных оценок экспертов, а экономический и финансовый риски рассчитываются на основе совокупности объективных статистических данных. Создатели индекса предлагают также возможность самостоятельной корректировки балльной шкалы оценки параметров индексов. Страны с низким уровнем риска имеют итоговые балльные оценки от 80 до 100, а страны с очень высоким уровнем риска от 0 до 49,9
	Период выпуска рейтинга и частота	С 1984 г. ежемесячно
	Количество стран	146
	Организация, разрабатывающая индекс	The PRS Group — США
	Адрес хранения базы данных	http://www.prsgroup.com/ircg.aspx
	Недостатки индекса	Необоснованные весовые коэффициенты индексов, составляющих итоговое значение индекса ICRG, незначительная подверженность субъективности оценки
Кредитные рейтинги (S&P)	Направленность индекса	Рейтинг используется как индикатор кредитоспособности эмитента для размещения инвестиций. Рейтинги могут использоваться для оценки риска контрагента (риска неисполнения контрагентом финансовых обязательств)
	Анализируемые индикаторы (показатели)	Методика включает в себя оценку политического риска (3 фактора) как желания страны платить вовремя по долгам и экономического (5 факторов) как способности платить по долгам. Как правило, аналитиками изучаются финансовые и нефинансовые характеристики эмитента, в том числе показатели эффективности, экономические, политические и регулятивные факторы, особенности практики менеджмента и корпоративного управления, а также конкурентоспособность компании. При определении рейтинга государства основное внимание уделяется вопросам налогово-бюджетной политики, экономическим показателям, стабильности денежно-кредитной политики и эффективности государственных институтов. К ключевым экономическим и политическим рискам, которые эксперты S&P принимают в расчет при определении рейтингов суверенного долга, относятся риски, связанные со следующими факторами: – институты и тенденции политического развития страны и их влияние на эффективность и прозрачность условий проведения экономической политики, а также общественная безопасность и геополитические проблемы; – структурная организация экономики и перспективы роста; – гибкость доходов расширенного правительства и факторы, оказывающие давление на расходы, дефицит расширенного правительства и размер долговой нагрузки, объем условных обязательств финансовой системы и государственного сектора; – гибкость денежно-кредитной сферы; – внешняя ликвидность и тенденции динамики обязательств государственного и частного сектора перед нерезидентами

Таблица 5 (*окончание*)

Наименование индекса	Характеристики	Описание характеристик
	Методология	Кредитные рейтинги основываются на анализе, проведенном опытными профессионалами, которые оценивают и интерпретируют информацию, полученную от эмитентов и других доступных источников. Стоит заметить, что в рамках кредитного анализа S&P изучает доступную текущую информацию и данные прошлых лет, а также оценивает потенциальное влияние будущих событий, которые можно предвидеть. На основании анализа странам присваиваются рейтинги от AAA до D. Выделяют 2 категории рейтингов: инвестиционная категория (от BBB– до AAA) и спекулятивная категория (от D до BB+). В случае если в ближайшие 6—24 месяца прогноз может измениться, S&P указывает направление изменения рейтинга (позитивное, негативное, стабильное и развивающееся)
	Период выпуска рейтинга и частота	С 1860 г. по мере поступления информации и необходимости обновления
	Количество стран	Более 120
	Организация, разрабатывающая индекс	Standard and Poor's Global Ratings
	Адрес хранения базы данных	https://www.standardandpoors.com/en_US/web/guest/ratings
	Недостатки индекса	Частичный субъективизм оценок (как следствие, разные кредитные агентства могут присваивать разные кредитные рейтинги одним и тем же странам), учет ведется только на конкретную дату, а не временной период
Индекс глобализации (ИГ)	Направленность индекса	Индекс измеряет глобализацию по экономическим, политическим и социальным показателям жизни общества. В отличие от остальных индексов ИГ предлагает отдельно индексы по каждому из видов глобализации, что предоставляет возможность использовать отдельные компоненты совокупного индекса
	Анализируемые индикаторы (показатели)	Экономическая глобализация: 1) текущие экономические потоки (торговля, иностранные прямые инвестиции, потоки, акции, портфельные инвестиции); 2) экономические ограничения (скрытые барьеры на импорт, средняя тарифная ставка, налоги на международную торговлю, ограничения на счета предприятий). Социальная глобализация: 1) данные о персональных контактах (телефонный трафик, переводы средств, международный туризм, иностранное население, международные письма); 2) данные об информационных потоках (пользователи Интернета, телевидение, торговля новостными газетами); 3) данные о культурной интеграции (количество «Макдональдсов», количество магазинов «ИКЕА», торговля книгами). Политическая глобализация: 1) посольства в стране; 2) членство в международных организациях; 3) участие в миссиях Совета Безопасности ООН; 4) международные договоры
	Методология	Каждому из субиндексов и переменных присвоены весовые коэффициенты на основе анализа главных компонент таким образом, чтобы вариация итоговой компоненты была максимальной. Каждый из субиндексов и переменных трансформируется в индекс по шкале от 0 до 100. Чем выше значение, тем выше уровень глобализации
	Период выпуска рейтинга и частота	С 2002 г. ежегодно
	Количество стран	208
	Организация, разрабатывающая индекс	Швейцарский экономический институт (KOF Swiss Economic Institute)
	Адрес хранения базы данных	http://globalization.kof.ethz.ch
	Недостатки индекса	Неоднозначное влияние субиндексов и переменных, используемых для оценки глобализации

Результаты корреляционного анализа индексов *Таблица 6*

	Кредитный рейтинг	Индекс недееспособности государств	Индекс глобализации	Индекс легкости ведения бизнеса
Кредитный рейтинг	1	0,45	0,62	0,61
Индекс недееспособности государств	0,45	1	0,47	0,49
Индекс глобализации	0,62	0,47	1	0,75
Индекс легкости ведения бизнеса	0,61	0,49	0,75	1

С целью окончательного отбора характеризующих страновой риск индексов был проведен корреляционный анализ представленных в табл. 5 индексов по состоянию на конец I квартала 2016 г. по 33 странам[2]). Стоит отметить, что индекс ICRG был исключен из анализа ввиду его лишь прогностического характера (до 5 лет). Результаты корреляционного анализа по оставшимся четырем индексам представлены в табл. 6.

Результаты проведенного корреляционного анализа показали, что почти все анализируемые индексы имеют значения корреляции не выше среднего уровня согласно шкале Чеддока (табл. 7).

Шкала корреляции Чеддока *Таблица 7*

Значение	Интерпретация
0—0,3	Очень слабая
0,3—0,5	Слабая
0,5—0,7	Средняя
0,7—0,9	Высокая
0,9—1	Очень высокая

Однако индекс глобализации и индекс легкости ведения бизнеса сильно коррелируют друг с другом. В этой связи нами рекомендуется оставить индекс легкости ведения бизнеса и исключить из дальнейшего анализа индекс глобализации.

Качественную оценку странового риска перспективных стран размещения реальных инвестиций целесообразно осуществлять в три этапа, как представлено на рис. 2.

В рамках выполнения этапа 1 методического подхода предполагается осуществить ранжирование стран по риску дефолта. Ранжирование стран по риску дефолта целесообразно осуществлять путем усреднения значений кредитных рейтингов китайского рейтингового агентства (далее — РА) Dagong [5] и американского РА S&P Global [6]. Представленные РА используют схожую методологию присвоения суверенных рейтингов, а также одинаковые шкалы экспертных оценок от «AAA» — высокие возможности эмитента отвечать по долговым обязательствам до «D» — дефолт эмитента. Более того, каждое из РА имеет значительное количество стран присвоения рейтингов (> 100 стран). Использование усредненных значений РА позволит значительно снизить один из основных недостатков применения экспертных подходов, а именно ангажированность оценок экспертов. Так, в рамках этапа 1 посредством использования усредненных значений суверенных рейтингов предлагается сформировать структурированные по риску дефолта перечни стран. Результат этапа целесообразно представить в виде двух списков: страны с приемлемым уровнем риска (страны, имеющие инвестиционный суверенный рейтинг) и страны с высоким уровнем риска (страны, имеющие суверенный рейтинг «B–»

[2] Для оценки страновых рисков были выбраны следующие 33 перспективные для размещения реальных инвестиций страны: Ангола, Бангладеш, Боливия, Бразилия, Китай, Конго, Египет, Габон, Гана, Индия, Индонезия, Казахстан, Малайзия, Мозамбик, Нигерия, Пакистан, Перу, ЮАР, Таиланд, Тринидад и Тобаго, Уругвай, Венесуэла, Израиль, Аргентина, Филиппины, Вьетнам, Иран, Ливия, Алжир, Танзания, Бруней, Экваториальная Гвинея, Мьянма.

* Рейтинг страны считается ниже инвестиционного, если значение кредитного рейтинга «B–» с негативным прогнозом или ниже.

Рис. 2. Методический подход к качественной оценке странового риска

с негативным прогнозом и ниже) согласно рекомендации PA S&P Global.

Однако помимо риска дефолта страны размещения инвестиций существует вторая составляющая странового риска, а именно негативные для бизнеса действия со стороны правительства страны размещения инвестиций или иных сил, не связанные напрямую с риском дефолта. Для учета данной составляющей рекомендуется использовать индекс недееспособности государства (далее — ИНГ), отражающий способность властей контролировать целостность территории, а также демографическую, политическую и экономическую ситуацию в стране. В случае высоких значений ИНГ страновой риск для инвестора сильно возрастает. В разделе 5 представлены примеры взаимосвязи ИНГ и негативных последствий для иностранных промышленных компаний. Стоит заметить, что данный индекс имеет слабую тесноту связи с суверенным рейтингом страны (0,45), что говорит о достаточно слабой корреляционной взаимосвязи с кредитным рейтингом. Так, существуют страны, имеющие инвестиционный суверенный рейтинг, но попадающие в зону высокого странового риска в связи с неприемлемым значением второй его составляющей.

В качестве примера можно привести Филиппины, по состоянию на конец I квартала 2016 г. имеющие суверенный рейтинг BBB, но ИНГ — 86,3 (уровень стабильности государства — ниже среднего). Стоит заметить, что границу приемлемости значений индекса каждая компания определяет самостоятельно исходя из установленного уровня толерантности к риску[3]). В качестве границы приемлемости значений рассматриваемого индекса для российских промышленных компаний предлагается использовать значение ИНГ Российской Федерации (РФ). Другими словами, предполагается, что реальные инвестиции имеют приемлемый уровень риска по рассматриваемому критерию, если значение ИНГ страны размещения реальных инвестиций ниже значения ИНГ РФ и наоборот. Результатом этапа 2 являются структурированные по двум критериям, а именно по риску дефолта и индексу недееспособности, перспективные страны размещения реальных инвестиций.

Таким образом, если потенциальная страна размещения реальных инвестиций имеет значение су-

[3] Согласно международным стандартам в области риск-менеджмента, например COSO Enterprise Risk Management Integrated Framework.

веренного рейтинга ниже приемлемого и/или значение ИНГ ниже значения ИНГ РФ, тогда ее следует расположить в списке стран с высоким уровнем риска. В случае если значения первого и второго критериев приемлемые, тогда страну следует отнести к списку стран с приемлемым уровнем странового риска.

В рамках заключительного этапа 3 рекомендуется осуществить ранжирование стран в рамках каждого из сформированных в результате выполнения этапов 1, 2 списков по критерию «Индекс легкости ведения бизнеса» (далее — ЛВБ). Использование данного индекса позволит компании учесть особенности нормативного регулирования предпринимательской деятельности, способствующего или затрудняющего ее развитие, а также степень защиты прав собственности в той или иной стране размещения инвестиций.

4. Основные результаты качественной оценки странового риска

Результаты первых двух этапов предложенного методического подхода оценки странового риска представлены на рис. 3. Потенциальные страны размещения реальных инвестиций закрашены на карте темным и светлым цветами в зависимости от уровня странового риска (незакрашенные страны не рассматривались). Темным цветом выделены страны с высоким уровнем риска, светлым — страны с низким уровнем риска (уровень риска для Мьянмы не был определен).

Страны, имеющие низкий кредитный рейтинг, на рис. 3 отмечены в скобках цифрой 1, а страны, имеющие высокий индекс недееспособности государства, — цифрой 2. На рис. 4 показаны результаты этапа 3 предлагаемого методического подхода оценки странового риска.

Рис. 3. Результаты этапа 1 и 2 методического подхода качественной оценки странового риска

Критерий ранжирования стран: индекс легкости ведения бизнеса (по убыванию)

Ранжированный перечень стран по уровню странового риска

Страны с приемлемым уровнем риска		Страны с высоким уровнем риска		Страны с неопределенным уровнем риска	
№ п/п	страна	№ п/п	страна	№ п/п	страна
1	Малайзия	20	Филиппины	33	Мьянма
2	Таиланд	21	Египет		
3	Перу	22	Мозамбик		
4	Израиль	23	Пакистан		
5	ЮАР	24	Иран		
6	Гана	25	Танзания		
7	Казахстан	26	Экв. Гвинея		
8	Вьетнам	27	Нигерия		
9	Тринидад и Тобаго	28	Бангладеш		
10	Уругвай	29	Конго		
11	Китай	30	Ангола		
12	Бруней	31	Венесуэла		
13	Индонезия	32	Ливия		
14	Бразилия				
15	Аргентина				
16	Индия				
17	Габон				
18	Алжир				
19	Боливия				

Рис. 4. Ранжированные перечни стран по уровню странового риска

На рис. 4 рассматриваемые страны сгруппированы по таким критериям, как значение кредитного рейтинга и индекс недееспособности государств, а также проранжированы по индексу легкости ведения бизнеса.

5. Примеры взаимосвязи индексов недееспособности государств и негативных последствий для иностранных промышленных компаний

Для объективного анализа странового риска рейтинги стран имеет смысл оценить в динамике, если количество стран, охваченных исследованиями, является постоянным и методология их оценки не меняется. Этому требованию в полной мере соответствует индекс недееспособности государств. Динамика данного индекса приведена в табл. 8 [9].

Из представленных в табл. 8 стран Нигерия в 2016 г. входила в группу государств с критическим уровнем рисков, все остальные — в группу государств с уровнем стабильности ниже среднего — опасный уровень рисков. Это самая многочисленная группа в исследованиях американского Фонда Мира и журнала «Foreign Policy» (в 2016 г. 90 государств).

Слабая корреляция между кредитными рейтингами (S&P и др.) и индексом недееспособности государств связана в первую очередь с различной методологией оценки факторов и показателей, определяющих конечное значение того или иного индекса и, как уже указывалось выше, с определенной субъективностью оценок, лежащих в основе расчета данных показателей, минимизировать которую достаточно сложно.

Кроме этого, необходимо учитывать, что показатели, определяющие индекс недееспособности государств, учитывают большее количество политических факторов, чем экономических и финансовых, а в кредитных рейтингах — наоборот. В теоретическом плане корреляцию между политическими и экономическими показателями не всегда можно установить однозначно, а тем более количественно. Например, Филиппины имеют кредитный рейтинг S&P на два пункта выше, чем у России (инвестиционная категория BBB– с негативным прогнозом), но рейтинг недееспособности попадает в темную

Динамика индекса недееспособности государств в 2010—2016 гг. *Таблица 8*

	Филиппины		Нигерия		Венесуэла		Россия	
	место	баллы	место	баллы	место	баллы	место	баллы
2016	54	84,7	13	103,5	63	81,6	65	81,0
2015	48	86,3	14	102,4	75	78,6	65	80,0
2014	52	85,3	17	99,7	83	76,7	85	76,5
2013	59	82,8	16	100,7	89	75,3	80	77,1
2012	56	83,2	14	101,1	82	79,8	83	79,8
2010	51	87,1	14	100,2	82	78,7	80	79,0

зону (не рекомендуется инвестировать в страну). Россия в соответствии с данным индексом также находится в темной зоне, но занимает 65-место, тогда как Филиппины только 54-е, то есть уровень дееспособности государственных институтов в России существенно выше, чем у Филиппин.

Данное противоречие можно объяснить тем обстоятельством, что зависимость Филиппин от иностранных инвесторов, особенно из США, существенно выше, чем у России и, соответственно, риск национализации и других негативных по отношению к ним действий намного ниже. Нормативно-правовая база Филиппин соответствует требованиям со стороны иностранных инвесторов, они имеют ряд льгот, которые не предоставляют другие страны. Так, например, американская корпорация «Дженерал моторс» при решении вопроса о выборе страны для строительства завода по выпуску автомашин и запчастей — на Филиппинах или в Таиланде, выбрала Филиппины. По мнению экспертов, Таиланд имел ряд преимуществ, так как автомобильный рынок в этой стране более развит, чем на Филиппинах. Но в конечном счете выиграли Филиппины, предложив «Дженерал моторс» ряд налоговых, таможенных и других льгот, которые стимулировали строительство завода именно в этой стране.

В этой связи необходимо отметить, что традиционно американские корпорации имели преимущества на Филиппинах по сравнению с корпорациями из других стран, поскольку они исторически являлись подконтрольной США страной, связанной с ними с 1951 г. Договором о взаимной обороне. США имеют на территории этой страны военные базы, спецслужбы обеих стран работают в тесном контакте, политическая элита получает образование в США и т. д. Вместе с тем национальное правительство не в состоянии полностью контролировать территорию страны, поскольку там имеются мощные сепаратистские движения, к тому же связанные с международным терроризмом, и уровень террористических угроз оценивается как достаточно высокий. На Филиппинах действует сильная коммунистическая партия, ориентированная на Китай, которая имеет боевые отряды и способна серьезно влиять на политическую ситуацию в стране. При этом антикитайский курс, традиционно проводимый правительством Филиппин, в условиях усиления конфронтации между США и Китаем поддерживается далеко не всеми группами населения и политической элиты страны. В известной степени отражением этих противоречивых тенденций являются и заявления нового (с 2016 г.) президента Филиппин Родриго Дутерте. При сохранении в целом внешнеполитического антикитайского курса после осуждения в ООН в августе 2016 г. внесудебных расправ над наркоторговцами он заявил, что рассматривает вопрос о выходе Филиппин из ООН.

Именно вследствие этих противоречивых тенденций индекс недееспособности Филиппин имеет небольшие колебания и, по всей видимости, если и будет ухудшаться, то незначительно.

Нигерия фактически находится в состоянии вялотекущих гражданских конфликтов, а деятельность многочисленных террористических группировок различной ориентации делает внутриполитическую ситуацию в стране нестабильной и слабопрогнозируемой. Именно поэтому по индексу недееспособности государств Нигерия устойчиво относится к группе государств с критическим уровнем рисков.

Вместе с тем она является одной из крупнейших нефтедобывающих стран мира и занимает первое место в Африке по добыче нефти. Экспорт нефти составляет большую часть ВВП страны и обеспечивает около 80% доходов государственного бюджета. Основные экспортные потоки нефти из страны ориентированы на США и ЕС (более 90% экспорта нефти). Нефтедобычу в стране контролирует Национальная нефтяная компания Нигерии — НННК (Nigerian National Petroleum Company, NNPC) и крупные транснациональные корпорации: Shell (до 52% добычи в стране), Exxon Mobil, Chevron Texaco, Conoco Phillips, Eni, Total и Addax (Китай), многие из которых имеют совместные предприятия с НННК.

В настоящее время иностранные корпорации в Нигерии могут работать только на условиях соглашений о разделе продукции или в качестве технических партнеров нигерийских компаний.

Нигерия является членом ОПЕК. В целях снижения зависимости от западных технологий и рынков сбыта именно по ее инициативе в 1987 г. была создана Африканская ассоциация производителей нефти, но, как показывает практика, решить эту проблему не удалось и в обозримом будущем вряд ли удастся.

Кроме нефти ведется промышленная добыча природного газа (по его запасам Нигерия занимает 10-е место в мире), имеется производство СПГ. На сегодняшний день основная часть добычи природного газа в Африке южнее Сахары приходится на Нигерию, и наравне с Алжиром, Египтом и Ливией она входит в «большую четверку газовых гигантов» на Африканском континенте. Вместе с тем решить проблему увеличения добычи природного газа без привлечения крупных зарубежных ТНК Нигерия просто не сможет, а возможности для наращивания такой добычи имеются — по доказанным запасам газа Нигерия уступает только России, Ирану и Катару. Поэтому принятая правительством страны стратегия газификации и модернизации энергетического сектора в целом предполагает широкое участие иностранных ТНК на максимально льготных условиях. Препятствуют этому запредельные политические риски и соответственно низкие рейтинги страны, в частности S&P дало Нигерии рейтинг BBB+ со стабильным прогнозом. Эта оценка связана с высоким уровнем коррупции и бюрократизированности в государственных органах власти, неразвитостью инфраструктуры, низкими ценами на газ на внутреннем рынке и другими факторами.

Естественно, что западные ТНК в этой стране стремятся компенсировать высокие риски увеличением нормы прибыли. Именно поэтому разработанный еще в 2011 г. законодательный акт о реформировании нефтегазового сектора Нигерии так и не вступил в действие вследствие лоббирования отдельными группами нигерийской политической элиты интересов западных корпораций [10]. Активно используют противоречия между западными ТНК и правительством Нигерии китайские энергетические компании, которые достаточно активно осваивают нигерийский рынок.

В наибольшей степени в Нигерии представлена французская ТНК Total, как и в целом в странах Африки. С 2008 по 2012 г. ею инвестировано в энергетический сектор африканских стран примерно столько же, сколько инвестировано всеми другими ТНК (около 18 млрд долл.).

Необходимо отметить, что стратегией Нигерии, как и в целом в развивающихся странах в отношении иностранных ТНК, является стремление, с одной стороны, в максимальной степени привлечь данные корпорации к разработке нефтяных и газовых месторождений, а с другой — использовать их возможности для решения внутренних экономических и политических проблем. Решить одновременно эти две задачи крайне сложно, и чаще всего правительства этих стран попадают в зависимость от иностранных ТНК, учитывая высокий уровень коррупции в странах, значительную социально-экономическую дифференциацию, несовершенство нормативно-правовой системы, которая часто формируется с учетом интересов иностранных ТНК, и т.д. Крупные корпорации используют эти факто-

ры для укрепления своего положения в этих странах на выгодных для них условиях. Этим, в частности, и объясняется тот факт, что в Нигерии, невзирая на высокий индекс недееспособности вследствие перманентной политической нестабильности и наличия террористических угроз, продолжают оставаться и активно действовать иностранные, в основном западные, ТНК.

Как показывает мировой опыт, ТНК развитых стран, в первую очередь США, не уходят с освоенных рынков, а если такое и происходит, то они используют все механизмы давления, в том числе и государственные, на развивающиеся страны, чтобы возвратиться на ранее завоеванные рынки. В этом смысле показателен пример стран Латинской Америки, в частности Венесуэлы. Ее индекс недееспособности начал постепенно ухудшаться после смерти президента Уго Чавеса в 2013 г., проводившего четко выраженную антиамериканскую политику. Именно он в 2007 г. национализировал нефтяную отрасль страны, заставив ТНК подписать Меморандум о взаимопонимании и передаче под контроль государственной нефтегазовой компании Petroleos de Venezuela всех нефтеразработок в бассейне реки Ориноко, где по заключенным в 1990-е гг. операционным соглашениям добычу нефти вели американские компании Exxon Mobil, Chevron, Conoco, британская BP, французская Total и норвежская Statoil [11].

Но национализация активов иностранных ТНК не уменьшила зависимость Венесуэлы от добычи и экспорта нефти (около 96% доходов от всего экспорта), поэтому падение в 2014 г. мировых цен на нефть крайне негативно отразилось на экономике страны и ее внутриполитической ситуации. Если учесть также и значительную зависимость страны от импорта — около 70% товаров ввозится из-за границы, то тотальный дефицит и связанный с ним черный рынок, рост преступности стали обыденным явлением в стране. Снижение ВВП страны в 2014 г. составило 4%, в 2015 г. — уже около 7%, инфляция, по экспертным оценкам, достигла за год более 100%. Кредитный рейтинг S&P (BBB– в 2015 г.) свидетельствует о высоком уровне инвестиционных рисков. Как следствие этих экономических проблем в стране возникла реальная угроза государственного переворота. В начале сентября 2016 г. преемник Уго Чавеса президент Венесуэлы Николас Мадуро заявил о его неудачной попытке, обвинив оппозицию в ее организации.

Основной вывод, который можно сделать исходя из приведенного качественного анализа, состоит в следующем.

Уровень инвестиционных рисков является заметно более высоким для инвесторов из развивающихся стран при условии инвестиций не в составе консорциума с ТНК, поскольку они не имеют такой поддержки своей страны базирования, которую имеют западные ТНК и, следовательно, в большей степени зависят от центральных и местных властей принимающего государства. Это является прямым следствием того обстоятельства, что ТНК развивающихся стран, как правило, не обладают необходимыми ресурсами для нивелирования негативных для их деятельности политических и экономических факторов в стране — реципиенте капитала. А западные ТНК, являясь фактически «государствами в государстве», имеют свои вооруженные формирования, разведку, дипломатию, лоббистские группы в принимающих странах, что позволяет им активно вмешиваться во внутреннюю и внешнюю политику этих стран для продвижения своих корпоративных интересов [12—14]. Арсенал средств воздействия достаточно широкий — от создания условий для принятия нужных для ТНК законов до организации государственных переворотов и прямой военной агрессии. Так, в Бразилии временно отстраненная президент страны Дилма Русеф, проводившая политику дистанцирования от США, окончательно отправлена в отставку в сентябре 2016 г. За ее импичмент проголосовал 61 член верхней палаты национального парламента из 81. В случае прямой агрессии, как это было в Ираке и Ливии, происходит переформатирование экономического пространства этих стран в интересах ТНК государств — инициаторов и участников агрессии.

Способствует консолидации усилий иностранных ТНК в принимающих странах и то обстоятельство, что они, как правило, в проблемных государствах, как, например, в Нигерии, действуют в составе стратегических альянсов, то есть не стремятся самостоятельно осваивать новые перспективные месторождения, а привлекают и другие ТНК на заранее оговоренных условиях (участие на долевых

началах). Понятно, что в случае изменения политической ситуации в принимающей стране, количественно выражающемся в увеличении индекса недееспособности государства, стратегическому альянсу гораздо проще, чем одной отдельно взятой компании, отстаивать общие корпоративные интересы.

Впечатляющим примером активного воздействия таких альянсов на глобальную политику является лоббирование США по инициативе своих крупных ТНК двух масштабных соглашений о свободной торговле, которые получили названия Трансатлантического торгового и инвестиционного партнерства (ТТИП) и Транстихоокеанского партнерства (ТТП), дополняющих друг друга. Переговоры по заключению ТТП начались в 2013 г. и завершились в 2015 г., переговоры по ТТИП планируется завершить к 2017 г. В этих соглашениях в первую очередь речь идет о нивелировании государственного права и прямом диктате западных ТНК в отношении суверенных государств, поскольку в случае реализации данных соглашений экономическая политика стран-участниц будет определяться крупными ТНК и их юридическими структурами. В соглашении о ТТП уже определено, что инвесторы имеют право подавать в независимый арбитражный суд иски к государствам, а в планируемом к подписанию ТТИП также предусмотрено создание неправительственного арбитражного суда (Investor-State Dispute Settlement — ISDS). При этом в данных соглашениях зафиксированы меры, ограничивающие деятельность крупных корпораций с государственным участием[4]), а в нефтегазовой отрасли это корпорации из развивающихся государств, что в будущем может заметно снизить их роль на мировых рынках энергоносителей.

[4] В группу Seven Sisters мировой нефтегазовой отрасли в середине XX века входили Exxon Corporation (н. в. — Exxon Mobil), Royal Dutch/Shell, Texaco Incorporated (впоследствии поглощена компанией Chevron), Chevron, Mobil Corporation (поглощена Exxon), Gulf Oil Corporation (поглощена Chevron) и British Petroleum. Таким образом, семерка превратилась в четверку: американские Exxon Mobil и Chevron и европейские BP и Royal Dutch Shell. По определению Financial Times, в мировой энергетике в конце XX века появились новые «семь сестер»: это Saudi Aramco, «Газпром», китайская CNPC, иранская NIOC, венесуэльская PDVSA, бразильская Petrobras и малайзийская Petronas. Все новые «семь сестер» являются государственными корпорациями.

Заключение

Использование предложенного методического подхода к оценке странового риска позволило:

- учесть влияние всех значимых факторов странового риска;
- выделить группы стран с высоким и приемлемым уровнями странового риска для промышленных компаний;
- ранжировать страны по уровню странового риска.

Данный методический подход целесообразно применять:

- при формировании стратегии приобретения иностранных активов или обмена активами, выхода на зарубежные рынки, как элемент методики формирования и балансировки портфеля зарубежных проектов;
- в ходе анализа и управления страновыми рисками в системе риск-менеджмента промышленных компаний на этапах анализа рисков управления зарубежными проектами.

На наш взгляд, одной лишь качественной оценки страновых рисков в ходе решения вышеперечисленных задач недостаточно. В ходе экономической оценки зарубежных проектов промышленные компании используют модели денежных потоков и выполняют расчет показателей экономической эффективности проектов, таких как чистый денежный доход, внутренняя норма доходности и др. При этом возникает задача учета в таких моделях страновых рисков. На наш взгляд, одним из эффективных способов такого учета является количественная оценка премии за страновой риск. Такую премию целесообразно прибавить к минимальной требуемой внутренней норме доходности проекта. Увеличение требуемой внутренней нормы доходности для зарубежных проектов с повышенным страновым риском, в свою очередь, позволит отфильтровать высокорискованные проекты. Однако проблема заключается в построении адекватных моделей оценки премий за страновой риск, учитывающих как премии за риск дефолта, так и премии за риск односторонних негативных действий со стороны зарубежных правительств или иных политических сил.

Литература

1. Индексы развития государств мира [Текст]: справочник / О.Т. Гаспарян, Р.У. Камалова, Е.А. Кочешкова и др.; под ред. Ю.А. Нисневича; Нац. исслед. ун-т «Высшая школа экономики». М.: Изд. дом Высшей школы экономики, 2014. 247 с.
2. Сайт рейтингового агентства Dagong. Электронный ресурс: https://www.en.dagongcredit.com
3. Сайт рейтингового агентства S&P. Электронный ресурс: https://www.spglobal.com
4. Сайт А. Дамодарана Электронный ресурс: http://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/ctryprem.html
5. Шарп У., Александер Г. Дж., Бэйли Дж. Инвестиции: Пер. с англ. М.: ИНФРА-М, 2004. XII. 1028 с.
6. Fisher L. Determinants of risk premiums on corporate bonds // Journal of Political Economy. Vol. 67. No. 3 (Jun., 1959). P. 217—237.
7. Электронный ресурс: [http://www.fundforpeace.org/global/?q=fsi2012]
8. Рассохин Н.А. Стратегии нефтегазовых ТНК в странах Африки южнее Сахары: Дис. ... канд. экон. наук. М., 2015. С. 36.
9. Лукьянович Н.В. Направленность и последствия политической деятельности транснациональных корпораций // Экономист. 2016. № 5.
10. Ивашенцов Г.А. Мьянма: смена власти. URL: http://riss.ru/analitycs/28859/ (дата обращения 11.09.2016).
11. Попов С., Поповкин И. Стратегические альянсы — дорога в будущее. Реформирование нефтегазового комплекса требует поиска новых управленческих подходов / Информационно-аналитический портал «Нефть России». URL: http://www.oilru.com/nr/72/576/ (дата обращения 10.09.2016).
12. Электронный ресурс: [http://knoema.ru/atlas]
13. Электронный ресурс: [http:// imf.org]
14. Электронный ресурс: [https://www.cia.gov/ru]

Сведения об авторах

Демкин Игорь Вячеславович: доктор экономических наук, заместитель директора центра анализа рисков ООО «НИИгазэкономика»
Количество публикаций: более 70
Область научных интересов: анализ и управление рисками, управление проектами
Контактная информация:
Адрес: 105066, г. Москва, ул. Старая Басманная, д. 20, стр. 8
Тел.: +7 (964) 505-08-26
E-mail: i.demkin@econom.gazprom.ru

Власов Дмитрий Александрович: специалист отдела анализа рисков нефтегазовых проектов ООО «НИИгазэкономика»
Количество публикаций: 1
Область научных интересов: анализ и управление рисками, управление проектами
Контактная информация:
Адрес: 105066, г. Москва, ул. Старая Басманная, д. 20, стр. 8
Тел.: +7 (495) 631-54-95
E-mail: d.vlasov@econom.gazprom.ru

Габриелов Александр Олегович: старший научный сотрудник отдела анализа рисков нефтегазовых проектов ООО «НИИгазэкономика»
Количество публикаций: около 20
Область научных интересов: анализ и управление рисками, управление проектами
Контактная информация:
Адрес: 105066, г. Москва, ул. Старая Басманная, д. 20, стр. 8
Тел.: +7 (495) 631-56-34
E-mail: a.gabrielov@econom.gazprom.ru

Бархатов Владимир Дмитриевич: старший научный сотрудник отдела анализа рисков нефтегазовых проектов ООО «НИИгазэкономика»
Количество публикаций: около 20
Область научных интересов: анализ и управление рисками, управление проектами
Контактная информация:
Адрес: 105066, г. Москва, ул. Старая Басманная, д. 20, стр. 8
Тел.: +7 (495) 631-56-34
E-mail: v.barkhatov@econom.gazprom.ru

Лукьянович Николай Васильевич: доктор политических наук, профессор, профессор Департамента мировой экономики и мировых финансов Финансового университета при Правительстве Российской Федерации
Количество публикаций: более 20
Область научных интересов: анализ и управление геополитическими и геоэкономическими рисками
Контактная информация:
Адрес: 125993, г. Москва, Ленинградский пр-т, д. 49, корп. 241
Тел.: +7 (905) 549-89-71
E-mail: lukjanovich@rambler.ru

УДК 338.1

Раскрытие информации об управлении рисками в годовых нефинансовых отчетах российских нефтегазовых компаний, действующих в Арктике[1]

ISSN 1812-5220

С. Н. Бобылев,
С. М. Никоноров,
А. В. Корнилова,
МГУ им. М. В. Ломоносова,
г. Москва

Аннотация

Предметом данного исследования является система управления рисками российских нефтегазовых компаний, которые реализуют проекты по разведке и разработке ресурсов в Арктической зоне Российской Федерации. В рамках исследования изучаются такие компании, как Газпром нефть, ЛУКОЙЛ, Роснефть, Зарубежнефть, Сургутнефтегаз и НОВАТЭК. Цель исследования — проанализировать систему управления рисками, включая систему управления экологическими и социальными рисками, на основе информации, раскрываемой в публичной годовой нефинансовой отчетности исследуемых компаний. Сравнительный анализ раскрытой информации проводится на основе разработанной авторами методологии оценки качества раскрытия информации по выделенным авторами ключевым показателям в области управления рисками. В данном исследовании изучается информация, представленная компаниями в годовых отчетах за 2014 г. Основные результаты исследования заключаются в определении лидеров в области управления рисками, включая социальные и экологические, среди исследуемых компаний. Практическое значение исследования определяется возможностью применения разработанной методологии оценки раскрытия показателей в области управления рисками для компаний других секторов экономики и из других стран. Изучение раскрытия информации об управлении рисками в годовых отчетах компаний является частью более масштабного исследования, направленного на анализ системы экологической и социальной ответственности российских нефтегазовых компаний, реализующих проекты в Арктике.

Ключевые слова: управление рисками, социальные риски, экологические риски, Арктика, нефинансовая отчетность.

Содержание

[1] Статья подготовлена при поддержке гранта РГНФ 16-02-00299.

Введение

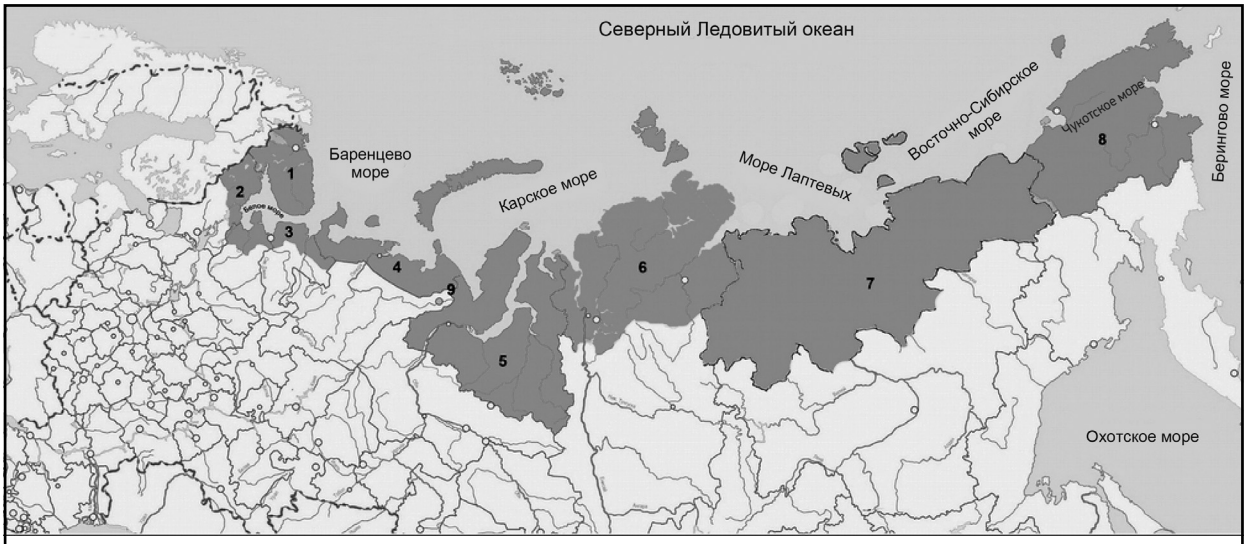
Арктика в настоящий момент является регионом новых возможностей и рисков, которыми необходимо грамотно управлять любым компаниям, осуществляющим деятельность в данном регионе.

В данном исследовании рассматриваются российские нефтегазовые компании, реализующие проекты по разведке и разработке ресурсов в Арктической зоне Российской Федерации (АЗРФ). АЗРФ представляет собой «часть Арктики, в которую входят полностью или частично территории Республики Саха (Якутия), Мурманской и Архангельской областей, Красноярского края, Ненецкого, Ямало-Ненецкого и Чукотского автономных округов, определенные решением Государственной комиссии при Совете Министров СССР по делам Арктики от 22 апреля 1989 г., а также земли и острова, указанные в Постановлении Президиума Центрального Исполнительного Комитета СССР от 15 апреля 1926 г. "Об объявлении территорией СССР земель и островов, расположенных в Северном Ледовитом океане", и прилегающие к этим территориям, землям и островам внутренние морские воды, территориальное море, исключительная экономическая зона и континентальный шельф Российской Федерации, в пределах которых Россия обладает суверенными правами и юрисдикцией в соответствии с международным правом» (http://www.scrf.gov.ru/documents/98.html). Регионы, входящие в АЗРФ, отмечены на рис. 1 темно-серым цветом.

К основным тенденциям, которые оказывают прямое влияние на будущее Арктического региона как ресурсной базы, относятся следующие.

• *Высокий ресурсный потенциал Арктического региона и рост спроса на ресурсы.*

Арктика представляет собой регион с высоким ресурсным потенциалом — в особенности это касается запасов нефти и газа. Это регион, который может обеспечить мир нефтью и газом как минимум на ближайшие 50 лет. По разным оценкам в Арк-



1 — Мурманская область
2 — Республика Карелия (в составе Лоухского, Кемского и Беломорского муниципальных районов)
3 — Архангельская область (в составе Онежского, Приморского и Мезенского муниципальных районов, городских округов Архангельск, Северодвинск и Новодвинск, а также административно принадлежащих ей арктических островов)
4 — Ненецкий автономный округ
5 — Ямало-Ненецкий автономный округ
6 — Красноярский край (в составе Таймырского (Долгано-Ненецкого) муниципального района, городского округа Норильск, муниципального образования г. Игарка Туруханского муниципального района)
7 — Республика Саха (Якутия) (в составе Абыйского, Аллаиховского, Анабарского, Усть-Янского и Эвено-Бытанайского улусов)
8 — Чукотский автономный округ
9 — Республика Коми (в составе городского округа Воркута)

Рис. 1. Арктическая зона Российской Федерации

тике насчитывается около 20% неразведанных запасов нефти и газа (Ernst & Young, 2013). Согласно исследованию Геологической службы США, в Арктике сосредоточено около 13% всех неразведанных мировых запасов нефти и 30% неразведанных мировых запасов природного газа (Arctic Oil and Gas Potential, 2009). При этом рост спроса на традиционные источники энергии не снижается, напротив, согласно исследованию Международного энергетического агентства (International Energy Agency, IEA), мировой спрос на нефть и газ может возрасти на 35% к 2035 г. по сравнению со спросом 2010 г. (Opportunities and Challenges…, 2014).

• *Изменение климата и глобальное потепление.*

Арктический регион в настоящий момент подвергается существенным изменениям намного быстрее, чем другие регионы планеты. Так, последствия изменения климата в Арктике более ощутимы, чем в других регионах, — глобальное потепление приводит к сокращению ледового покрова, изменениям длительности сезонов и режимов погоды. Согласно пятому докладу Межправительственной группы экспертов по изменению климата (МГЭИК), оценивающему последние климатологические результаты, уровень ледового покрова Арктики сократился с 3,5 до 4,1% в период с 1979 по 2012 г. (IPCC, 2014) (рис. 2).

• *Технологический прогресс.*

Технологический прогресс в данном случае выражается в создании новых технологий, позволяющих осуществлять разведку и разработку ресурсов в суровых климатических условиях, а также позволяющих исследовать новые пространства высоких широт. Яркими примерами технологических разработок, имеющих ключевое значение для Арктики, являются ледокольный флот, нефтяные платформы, позволяющие вести работы на арктическом шельфе, GPS-навигация в высоких широтах и пр.

Таким образом, изменение климата открыло новые возможности в Арктике — теперь в этом регионе традиционные отрасли экономки, такие как частное рыболовство, тюлений и китобойный промыслы, охота, более не занимают первое место. Совокупность таких факторов, как рост потребности в традиционных источниках энергии, изменение климата и технологический прогресс, привели

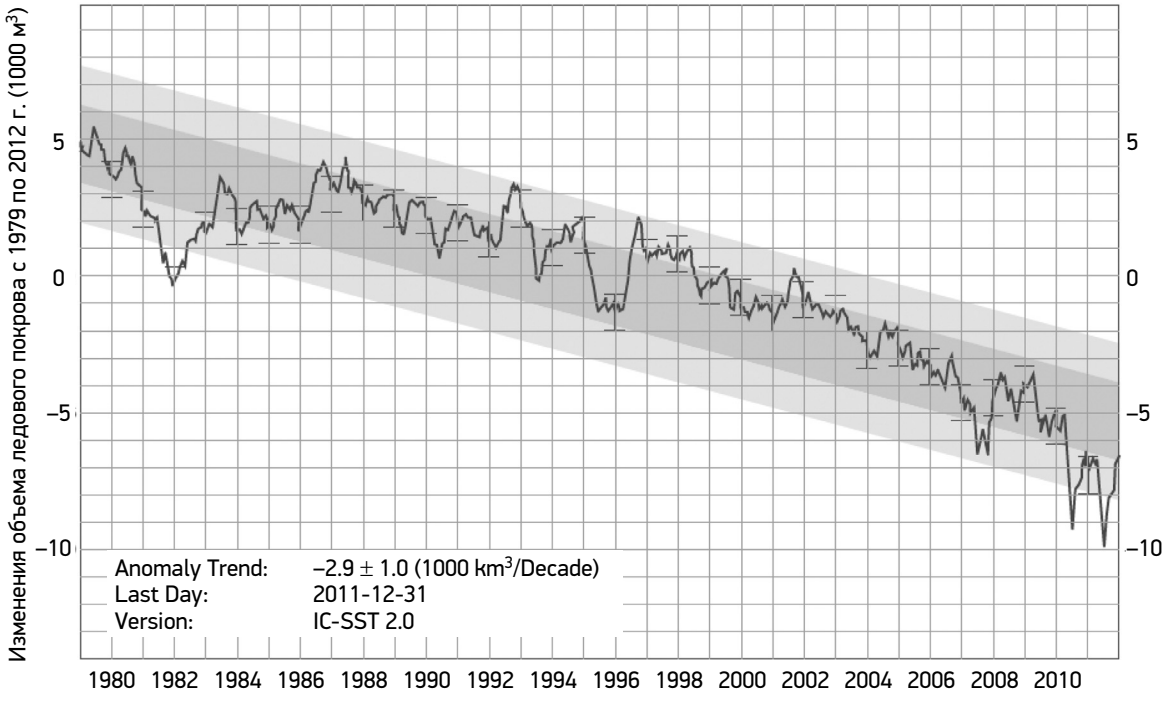


Рис. 2. Сокращение ледового покрова Арктики с 1979 по 2012 г.

к тому, что добыча полезных ископаемых, нефти и газа, коммерческое рыболовство, туризм стали более значимыми в разрезе экономического развития данного региона и обеспечения ресурсами. Самым основным направлением реализации экономических проектов в Арктике, безусловно, является разведка и разработка ресурсов, в особенности нефти и газа.

- *Новые риски в Арктике.*

Все вышеперечисленные экономические преимущества в Арктике могут быть достигнуты только в том случае, если компании смогут грамотно управлять рисками, которые присутствуют в Арктическом регионе.

Одним из немаловажных факторов риска является хрупкость арктических экосистем, когда, к примеру, популяция китов и белых медведей уменьшается из-за сокращения ледового покрова, а закисление Северного Ледовитого океана из-за увеличения выбросов диоксида углерода приводит к нарушению функционирования водных экосистем (Mathis, 2011). Влияние на арктические экосистемы также оказывают стойкие органические загрязнители (англ. POPs, persistent organic pollutants), которые появляются в атмосфере в результате выбросов углеродной сажи (англ. Black carbon) как вследствие работы ледоколов, так и различных производственных объектов, расположенных по берегам Арктической зоны (AMAP, 2015). Негативное воздействие также может быть оказано на развитие арктических экосистем посредством реализации таких проектов, как:

- строительство нефтепроводов и дорог;
- шумовое загрязнение от процессов бурения, сейсморазведочной активности, морского судоходства;
- нарушение морского дна в процессе бурения;
- вскрытие ледового покрова (Lloyd's, 2012).

К рискам экономической деятельности в Арктике также можно отнести суровый климат и географическую удаленность. Большая часть арктических территорий географически изолирована, что требует большого количества операционных издержек на ведение экономической деятельности в регионе, а также усугубляет последствия реализации рисковых событий. Важно отметить, что в рамках управления техногенными рисками в Арктике в 2011 г. арктическими странами было подписано Соглашение о сотрудничестве в авиационном и морском поиске и спасании в Арктике (http://www.szrf.ru/doc.phtml?nb=edition02&issid=2013009000&docid=16), которое подтверждает приверженность стран на государственном уровне предоставлять все необходимые ресурсы для осуществления поиска и спасания в Арктическом регионе. На локальном уровне риск разливов нефти и иных экологических катастроф остается высоким из-за недостаточного совершенства необходимых для предотвращения разливов технологий, а также из-за того, что высокочастотное радио и GPS работают недостаточно эффективно в районах выше 70—72° северной широты, что может препятствовать осуществлению своевременного реагирования (Lloyd's, 2012).

Успешными в Арктическом регионе могут быть только те компании, которые со всей ответственностью подходят к вопросам заботы об окружающей среде и обществе, взаимодействуют с заинтересованными сторонами и управляют рисками, включая социальные и экологические риски, обеспечивая, таким образом, устойчивое развитие региона.

1. Управление рисками и ответственность компаний в Арктике

Существуют различные инструменты по эффективному управлению вышеперечисленными рисками в Арктике. К ним можно отнести инвестиции в разработку и приобретение специфичных для Арктики технологий, внедрение лучших практик операционной безопасности и эффективности, следование стандарту ISO 19906 «Нефтяная и газовая промышленность: сооружения арктического шельфа» (ISO 19906:2010), проведение учений по поиску и спасанию в Арктике, проведение учений по предотвращению разливов нефти, реализацию проектов в области экологического страхования и пр.

Управление рисками критически важно для нефтегазовых компаний в Арктике, которые стремятся осуществлять свою деятельность в данном регионе безопасно, надежно, устойчиво и эффективно. В данном случае не столь важно менять систему управления рисками в компании, подстраивая ее под контекст Арктики, сколь важно, чтобы уже су-

ществующая система управления рисками учитывала сложную и быстроменяющуюся природу Арктического региона.

Любая компания, ведущая экономическую деятельность в Арктике, должна учитывать вышеперечисленные тенденции, четко анализировать существующие возможности и риски и эффективно управлять рисками с целью сохранения природного и культурного наследия для будущих поколений, создания общественной ценности в долгосрочной перспективе и, в конечном счете, достижения устойчивого развития в регионе. Это возможно благодаря реализации практик КСО, активному взаимодействию с заинтересованными сторонами, грамотному управлению социальными и экологическими рисками.

Призыв к осуществлению ответственной экономической деятельности в Арктическом регионе также был объявлен Арктическим советом[2], а именно Рабочей группой по устойчивому развитию в Арктике (Sustainable Development Working Group, SDWG, http://www.sdwg.org/). Так, в 2012 г. была создана Инициатива по корпоративной социальной ответственности (Initiative on Corporate Social Responsibility) и открыта платформа для постоянного диалога представителей бизнес-сообществ, действующих в Арктическом регионе, которая носит название «Арктический экономический совет» (http://arcticeconomiccouncil.com/). Инициатива Арктического совета по КСО создана для объединения компаний различных отраслей с целью вовлечения их в диалог для достижения устойчивого развития и ответственного использования природных ресурсов в Арктике (http://www.kas.de/wf/doc/kas_39168-1522-2-30.pdf?141112150837).

2. Российские нефтегазовые компании: проекты в Арктике

Главный вопрос данного исследования заключается в том, каким образом российские нефтегазовые компании, действующие в Арктике, управляют рисками, в особенности социальными и экологическими.

В рамках данного исследования проанализированы системы управления рисками шести российских нефтегазовых компаний, которые реализуют проекты по разведке и разработке ресурсов в Арктике. К исследуемым компаниям относятся Газпром нефть, ЛУКОЙЛ, Роснефть, Зарубежнефтегаз, Сургутнефтегаз и НОВАТЭК.

Данные компании реализуют проекты в различных регионах России и мира, при этом каждая из них осуществляет деятельность по разведке и разработке нефти и/или газа в Арктике.

В табл. 1 представлена краткая сравнительная характеристика изучаемых компаний.

В рамках данного исследования анализируются крупные нефтегазовые компании с годовой выручкой от 31 млрд руб. до 8 трлн руб., среднесписочная численность персонала которых варьируется от 12 до 249 тыс. чел. Четыре компании из шести ведут деятельность по добыче ресурсов не только на территории России (Газпром нефть, ЛУКОЙЛ, Роснефть, Зарубежнефть).

Все исследуемые компании ведут экономическую деятельность в Арктическом регионе. Особенно хочется уделить внимание следующим проектам. Газпром нефть в 2014 г. впервые вывела на мировой рынок нефть арктического сорта ARCO, добытую на Приразломном месторождении в Печорском море и Novy Port с Новопортовского месторождения на полуострове Ямал. Приразломное месторождение — самый первый в России проект по добыче на арктическом шельфе (Газпром нефть, 2014). В 2014 г. ОАО «Роснефть» в стратегическом альянсе с ExxonMobil открыло новое нефтегазовое месторождение «Победа» на шельфе Карского моря, что стало результатом бурения самой северной в мире арктической скважины «Университетская-1». Нефтегазоносная провинция в Карском море получила название «Победа» потому, что ее разведанные ресурсы по своим объемам сопоставимы с запасами всей Саудовской Аравии (Роснефть, 2014). Компания НОВАТЭК начала реализовывать проект «Ямал СПГ» — строительство завода по сжижению газа на Южно-Тамбейском месторождении ЯНАО (НОВАТЭК, 2014).

[2] Арктический совет — международный форум, созданный в 1996 г. по инициативе Финляндии для защиты уникальной природы северной полярной зоны. В Арктический совет входят восемь постоянных стран-участниц: Дания, Исландия, Канада, Норвегия, Россия, США, Финляндия и Швеция, а также 12 стран-наблюдателей.

Сравнительная характеристика российских нефтегазовых компаний *Таблица 1*

№	Компания	Годовая выручка от реализации, млн руб., 2014 г.	Среднесписочная численность персонала, чел., 2014 г.	Регионы присутствия	Значимые проекты в Арктике
1	Газпром нефть	1 408 238	57 515	Россия, Ирак	Приразломное месторождение (оператор ООО «Газпром нефть шельф»), месторождения в ЯНАО (Новый порт)
2	ЛУКОЙЛ	8 650 020	110 300	Россия, Ирак, Египет, Саудовская Аравия, Казахстан, Узбекистан, Болгария, Румыния	Имилорско-Источный участок (Западная Сибирь), месторождения в Тимано-Печоре
3	Роснефть	5 503 000	249 000	Россия, Вьетнам, Венесуэла, Куба, Эквадор	Месторождение «Победа» (Карское море) — стратегический альянс Роснефть и ExxonMobil
4	Зарубежнефть	31 000	12 698	Россия, Куба, Вьетнам, Босния и Герцеговина	Месторождения СК «РУСВЬЕТПЕТРО» в Ненецком АО
5	Сургут-нефтегаз	862 600	115 500	Россия	Западно-Сибирская, Восточно-Сибирская, Тимано-Печорская нефтегазоносные провинции
6	НОВАТЭК	357 643	6749	Россия	Ямало-Ненецкий АО, проект «Ямал СПГ»

3. Методология анализа систем управления рисками

Анализ существующих в компаниях систем управления рисками основывается на официальной публичной годовой нефинансовой отчетности компаний за 2014 г.[3]

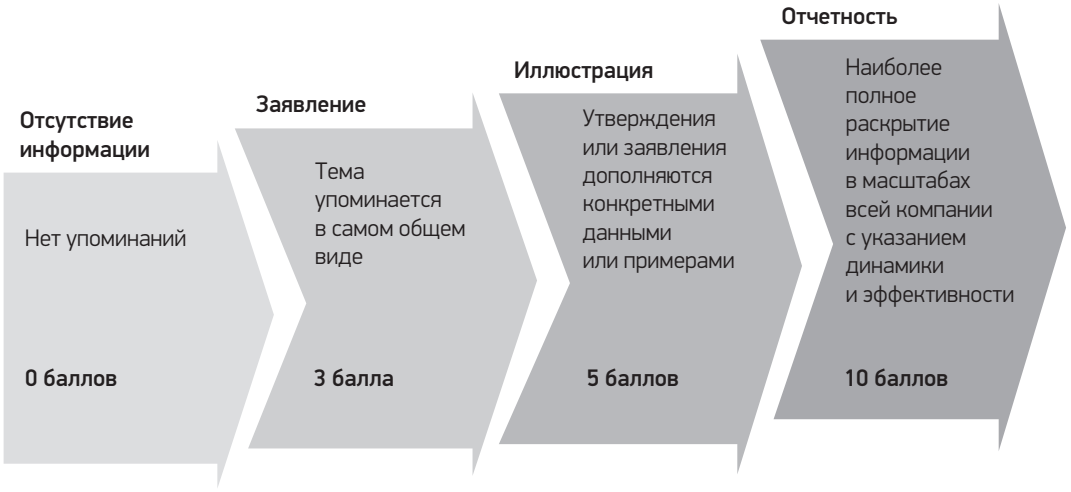
Публичная нефинансовая отчетность — это отчетность, охватывающая одновременно экономические, экологические и социальные аспекты деятельности компании, раскрывающая информацию об ее нефинансовых инициативах и вкладе в устойчивое развитие окружающего мира (http://www.npg.ru/?page=services&subpage=nonfinance). Нефинансовая отчетность не имеет ничего общего со стандартной финансовой (бухгалтерской) отчетностью по стандартам РСБУ (Российские стандарты бухгалтерской отчетности) и МСФО (Международные стандарты финансовой отчетности), которая является обязательной. Нефинансовая отчетность является добровольной и создана для того, чтобы понятным языком донести ключевую информацию по экологическим, социальным и экономическим результатам деятельности компании за год для всех ее заинтересованных сторон. Термин «нефинансовая отчетность» не означает, что в отчете нет данных по годовым финансовым результатам компании, термин означает тот факт, что данная отчетность не относится к стандартной бухгалтерской.

Публичная нефинансовая отчетность играет существенную роль в повышении прозрачности деятельности компаний, что является показателем высоких стандартов управления компанией и ее инвестиционной привлекательности. Публичная нефинансовая отчетность может также называться *Годовой нефинансовой отчетностью*, отчетностью в области устойчивого развития, социальной и экологической отчетностью, отчетностью в области корпоративной социальной ответственности, интегрированной отчетностью.

Таким образом, годовая нефинансовая отчетность — это достоверный источник информации о реализуемых компанией практиках в социальной, экологической и экономической областях.

[3] В рамках данного исследования за основу взята годовая нефинансовая отчетность российских нефтегазовых компаний за 2014 г. вследствие наибольшей актуальности информации на момент написания исследования (нефинансовый отчет компаний за прошлый год обычно публикуется во второй половине текущего года).

Методология оценки раскрытия информации об управлении социальными и экологическими рисками *Таблица 2*



Информация, представленная в годовой нефинансовой отчетности исследуемых российских нефтегазовых компаний, анализируется и оценивается в соответствии с разработанной авторами методологией оценки раскрытия информации об управлении социальными и экологическими рисками.

По разработанной балльной шкале оцениваются разработанные авторами показатели в области управления рисками (RM, Risk Management), которые представлены в табл. 3.

Каждый показатель получает от 0 до 10 баллов в зависимости от качества раскрытия информации по уровням «Отсутствие информации» — 0 баллов, «Заявление» — 3 балла, «Иллюстрация» — 5 баллов и «Отчетность» — 10 баллов, как показано в табл. 2.

В результате сравнительного анализа представленной в нефинансовой отчетности информации о системе управления рисками выявляется лидер в области управления рисками, включая социальные и экологические, среди исследуемых российских нефтегазовых компаний.

4. Сравнительный анализ систем управления рисками в российских нефтегазовых компаниях в Арктике

Управление рисками является одной из ключевых и наиболее важных составляющих системы управления в сфере устойчивого развития, социальной и экологической ответственности компаний. Рассмотрим подробнее то, каким образом раскрываются показатели в области управления рисками в годо-

Показатели в области управления рисками (RM) *Таблица 3*

№	Показатель	Описание
	Управление рисками (RM)	
1	Система управления рисками	Наличие в отчете информации о действующей в компании системе управления рисками (СУР), которая позволяет идентифицировать, оценивать риски и управлять ими, а также осуществлять мониторинг эффективности данных мероприятий с целью минимизации рисков
2	Реестр ключевых рисков компаний	Представление в отчете реестра ключевых рисков компании с указанием мер по управлению данными рисками, которые предпринимает компания
3	Социальные и экологические риски	Наличие социальных и экологических рисков в реестре ключевых рисков компаний
4	Карта рисков	Наличие карты рисков, в которой риски распределены по вероятности возникновения и масштабу ущерба

вой нефинансовой отчетности исследуемых компаний и какая компания является лидером в области управления рисками.

Показатель «Система управления рисками»

Во всех исследуемых компаниях создана и функционирует Система управления рисками, как показано на рис. 3.

Во всех исследуемых компаниях разработан и действует единый подход к процессу управления рисками, который зафиксирован в корпоративных стандартах и политиках. Так, например, в компании Газпром нефть действует «Политика в области управления рисками», которая определяет общие цели, задачи и принципы управления рисками для повышения гарантии надежности деятельности компании в краткосрочной и долгосрочной перспективе (Газпром нефть, 2014). Также в компании Газпром нефть разработан и действует единый подход к процессу управления рисками, который представлен в корпоративном стандарте «Интегрированная система управления рисками (ИСУР)» и является непрерывным процессом выявления, оценки и управления рисками. Важно также отметить, что в компании Газпром нефть в настоящий момент осуществляется интеграция процесса оценки рисков с бизнес-планированием и управлением проектами, как показано на рис. 4.

Интересный кейс представлен в годовом отчете Газпром нефти в 2014 г. Газпром нефть совместно с одним из ведущих технических консультантов для нефтегазовой отрасли — Det Norske Veritas — организовала семинар по управлению рисками арктических шельфовых проектов (Газпром нефть, 2014). В рамках данного семинара были рассмотрены риски и проблемные аспекты бурения в арктических водах, вопросы соблюдения охраны труда, безопасности и защиты окружающей среды.

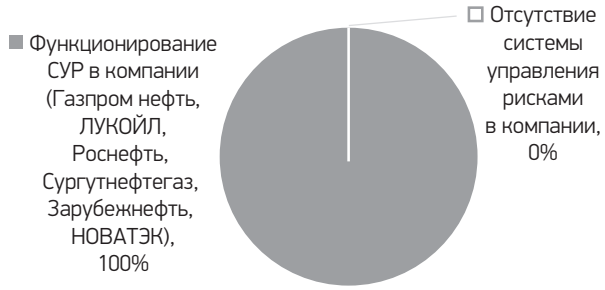


Рис. 3. Наличие действующей Системы управления рисками в российских нефтегазовых компаниях

По методологии оценки качества раскрытия информации Газпром нефть получает 10 баллов (уровень раскрытия «Отчетность»).

В компании ЛУКОЙЛ также действует корпоративная система управления рисками (ERM) в соответствии с лучшими мировыми практиками — на постоянной основе проводятся идентификация, оценка, мониторинг рисков, а также мероприятия по управлению ими (ЛУКОЙЛ, 2014), как представлено на рис. 5. В компании существуют все необходимые нормативные документы и эффективно действующая структура по управлению рисками (Комитет по рискам, назначены владельцы рисков и пр.). По методологии оценки раскрытия информации по данному показателю ЛУКОЙЛ получает 5 баллов (уровень раскрытия «Иллюстрация»).

В компании Зарубежнефть также существует Система управления рисками и внутреннего контроля (ОСУР). Процесс управления рисками в компании разработан на основе международной общепризнанной модели управления рисками — COSO ERM — и осуществляется с учетом международной практики корпоративного управления, как указано на рис. 6. ОСУР охватывает все уровни управления, является непрерывной и направлена на достиже-

* В зависимости от критичности риска.

Рис. 4. Принципиальная схема процесса Интегрированной системы управления рисками (ИСУР) в Группе «Газпром нефть», 2014 г.

Рис. 5. Корпоративная система по управлению рисками в компании ЛУКОЙЛ, 2014 г.

ние долгосрочных целей компании (Зарубежнефть, 2014). В годовом отчете компании Зарубежнефть представлены как схема управления рисками в компании, так и участники процесса управления рисками и их функции, а также опубликована история развития Системы управления рисками, как представлено на рис. 7. Согласно методологии оценки качества раскрытия информации по данному показателю Зарубежнефть получает 10 баллов (уровень раскрытия «Отчетность»).

В компаниях Роснефть, Сургутнефтегаз и НОВАТЭК также внедрена и совершенствуется система управления рисками.

Так, в компании Роснефть внедрена и непрерывно совершенствуется Система внутреннего контроля и управления рисками (СВКиУР), цели данной системы определены в Политике СВКиУР. В годовом отчете компании Роснефть представлена информация о субъектах СВКиУР, начиная с Совета директоров и заканчивая Департаментом рисков. По методологии оценки качества раскрытия информации по данному показателю Роснефть получает 5 баллов (уровень раскрытия «Иллюстрация»).

В годовом отчете Сургутнефтегаз информация о системе управления рисками представлена очень кратко — дано определение цели внедрения данной системы. Согласно методологии данный показатель компании получает 3 балла (уровень раскрытия «Заявление»).

В компании НОВАТЭК в 2014 г. было утверждено Положение о системе управления рисками и внутреннего контроля (НОВАТЭК, 2014). В годовом отчете НОВАТЭК отмечен данный факт, однако более подробная информация о системе управления рисками не представлена. По данному показателю НОВАТЭК получает 3 балла (уровень раскрытия «Заявление»).

Проведенная авторами оценка раскрытой информации в отчетах о системе управления рисками согласно методологии приводит к следующим результатам, показанным в табл. 4.

Показатель «Реестр ключевых рисков компаний»

Наличие реестра ключевых рисков в годовых отчетах показывает, насколько эффективна система управления рисками в компании на настоящий момент — насколько эффективно осуществляются идентификация рисков, их оценка и управление ими, мониторинг мероприятий по управлению рисками, какие риски относятся к ключевым.

Реестр ключевых рисков приведен в годовых отчетах пяти исследуемых компаний — Газпром нефть, ЛУКОЙЛ, Зарубежнефть, Сургутнефтегаз

Рис. 6. Схема процесса управления рисками в ОАО «Зарубежнефть»

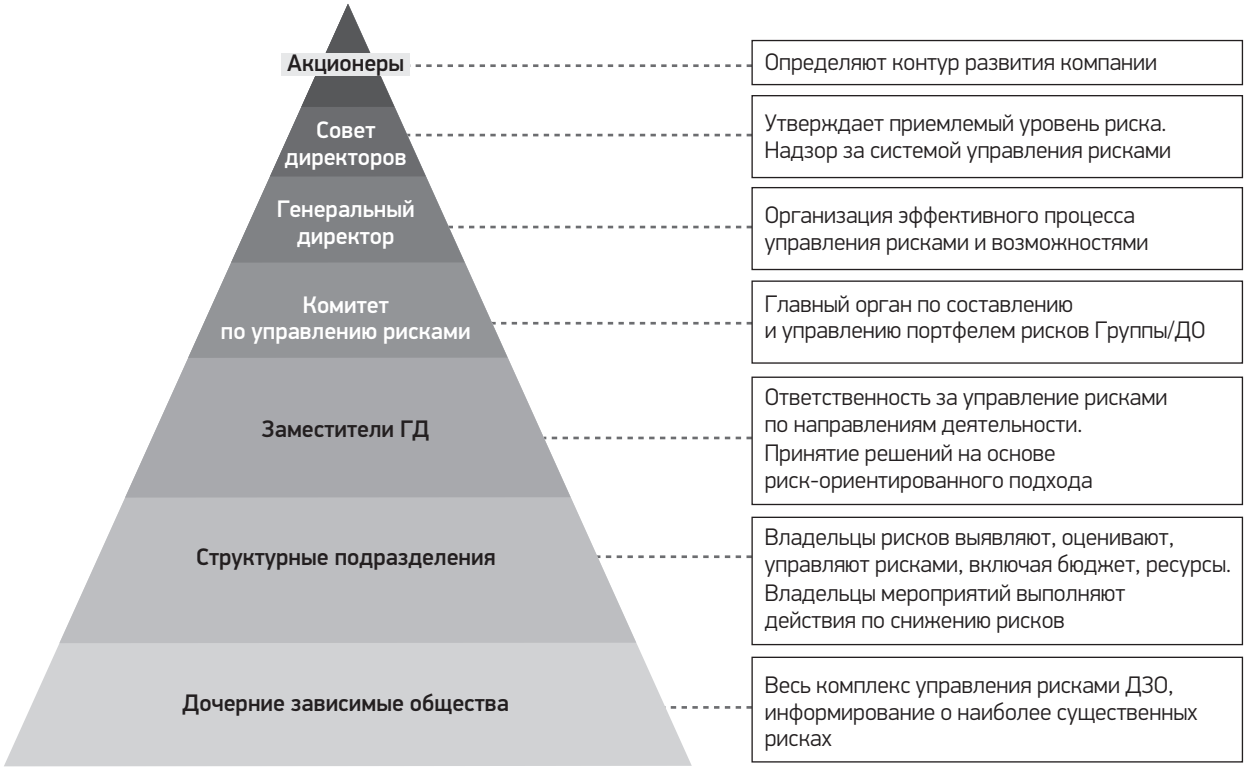


Рис. 7. Участники процесса управления рисками в ОАО «Зарубежнефть»

Оценка раскрытия информации по показателю «Система управления рисками» *Таблица 4*

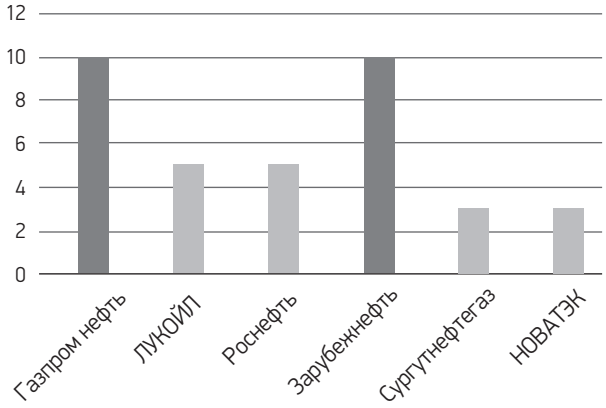


Рис. 8. Наличие реестра ключевых рисков в годовом отчете компании

и НОВАТЭК. Все пять компаний в реестре рисков не только приводят описание рисков, но также отражают меры по управлению данными рисками, как показано на рис. 8. В годовом отчете компании Роснефть реестр рисков не представлен.

Так как у компании Газпром нефть отчет имеет тип «двухтомник»[4], что означает, что компания выпустила два отчета — один годовой отчет, второй — отчет об устойчивом развитии, то информация о рисках представлена в двух отчетах. В годовом отчете приведен полный реестр ключевых рисков, куда помимо социальных и экологических входят также финансовые, операционные, правовые и пр. Социальные и экологические риски подробно раскрываются в отчете об устойчивом развитии ОАО «Газпром нефть» (Газпром нефть, 2014).

В годовом отчете компании ЛУКОЙЛ выделяются 12 групп ключевых рисков, куда входят макроэкономические, страновые, отраслевые риски, риски роста тарифов и цен поставщиков, финансовые и валютные риски, риски ликвидности, правовые риски и т. д. (ЛУКОЙЛ, 2014).

Зарубежнефть управляет следующими категориями рисков в соответствии с разработанной концепцией ОСУР: стратегические риски, операционные риски, риски, связанные с подготовкой отчетности и управлением финансовыми потоками, риски соответствия требованиям законодательства и регулирующих органов (Зарубежнефть, 2014).

В отчете Сургутнефтегаз риски представлены не в виде реестра, а сплошным текстом, несмотря на это, в отчете указаны мероприятия, предпринимаемые компанией по управлению ими (Сургутнефтегаз, 2014). В годовом отчете выделены такие группы рисков, как отраслевые, страновые и региональные, правовые, репутационные и стратегические.

В годовом отчете НОВАТЭК приведены такие группы рисков, как операционные, финансовые и правовые (НОВАТЭК, 2014).

У компании Роснефть в годовом отчете отсутствует реестр рисков, что может свидетельствовать о недостаточном внимании со стороны руководства компании к данному аспекту (Роснефть, 2014).

Так как в годовых отчетах Газпром нефть, ЛУКОЙЛ, Зарубежнефть представлены реестры рисков, в которых описаны как риски, так и мероприятия по управлению ими, по данным показателям компании получают 10 баллов (уровень раскрытия «Отчетность»). Роснефть за данный показатель получает 0 баллов (уровень раскрытия «Отсутствие информации»).

В результате оценки раскрытия информации по показателю «Реестр ключевых рисков» компаниям присвоены следующие баллы, указанные в табл. 5.

[4] Двухтомник — тип публичного нефинансового отчета, который состоит из двух частей: годового отчета, в котором кратко представлены как финансовые, так и нефинансовые показатели, а также отчета об устойчивом развитии, в котором представлена информация преимущественно нефинансового характера, с акцентом на социальные и экологические аспекты деятельности компании.

Оценка раскрытия информации по показателю «Реестр ключевых рисков» *Таблица 5*

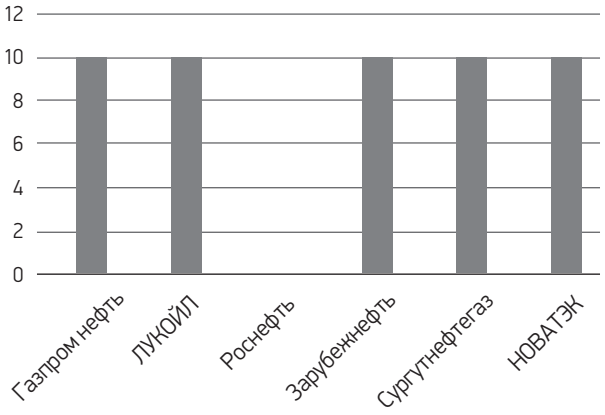


Рис. 9. Наличие социальных и экологических рисков в реестре ключевых рисков компаний

Показатель «Социальные и экологические риски»

Наличие социальных и экологических рисков в реестре ключевых рисков компаний свидетельствует о понимании важности управления данными рисками руководством компании.

Так, социальные и экологические риски присутствуют в годовых отчетах компаний Газпром нефть, Зарубежнефть, Сургутнефтегаз и НОВАТЭК. Социальные и экологические риски отсутствуют в реестре ключевых рисков компаний ЛУКОЙЛ и Роснефть, как представлено на рис. 9.

Газпром нефть выделяет такие ключевые социальные и экологические риски, как риски, связанные с кадровыми ресурсами (нехватка квалифицированного рабочего персонала, в частности в инженерных и технологических областях), риски, связанные с промышленной безопасностью, и экологические риски. Соответственно, мероприятия по управлению данными рисками следующие: конкурентоспособное вознаграждение, социальный пакет, обучение и развитие персонала, обеспечение соблюдения техники безопасности и безопасных условий труда для сотрудников, соблюдение требований экологического законодательства и проведение природоохранных мероприятий (Газпром нефть, 2014). Газпром нефть за раскрытие информации по данному показателю получает 10 баллов (уровень раскрытия «Отчетность»).

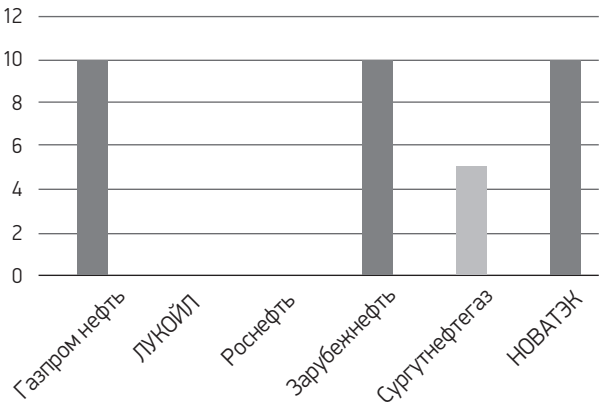
В годовом отчете компании Зарубежнефть экологические (аварии и загрязнение окружающей среды) и социальные (охрана труда и промышленная безопасность) риски включены в такие подразделы, как операционные риски и риски соответствия законодательству и требованиям регулирующих органов (Зарубежнефть, 2014). По данному показателю Зарубежнефть получает 10 баллов (уровень раскрытия «Отчетность»).

В разделе годового отчета, посвященном ключевым рискам компании Сургутнефтегаз, экологические риски включены в группу отраслевых рисков, в отчете также представлены мероприятия по управлению рисками (Сургутнефтегаз, 2014). Социальные риски в списке ключевых не обозначены, Сургутнефтегаз получает 5 баллов за раскрытие информации по данному показателю (уровень раскрытия «Иллюстрация»).

Компания НОВАТЭК в годовом отчете указывает следующие группы рисков: операционные (куда входят экологические и социальные), финансовые и правовые риски. В отчете подробно представлены как сами риски, так и мероприятия и управлению ими. НОВАТЭК по данному показателю получает 10 баллов (уровень раскрытия «Отчетность»).

В годовых отчетах компаний Роснефть и ЛУКОЙЛ социальные и экологические риски в реестре ключевых рисков не представлены, поэтому компании получают 0 баллов (уровень раскрытия «Отсутствие информации»).

Оценка раскрытия информации по показателю «Социальные и экологические риски» *Таблица 6*



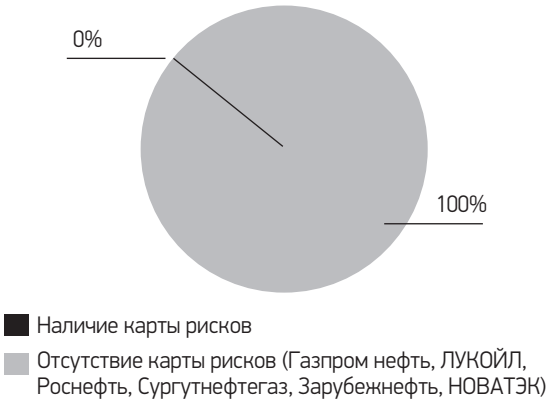


Рис. 10. Наличие карты рисков в годовых отчетах компаний

Оценка раскрытия в годовых отчетах исследуемых компаний информации по показателю «Социальные и экологические риски» приведена в табл. 6.

Показатель «Карта рисков»

Ни в одном годовом отчете исследуемых компаний не представлена карта рисков. Читателю не раскрывается информация о том, какие риски наиболее критичны для компании, какие менее, не указана вероятность наступления тех или иных рисков, и не указан вероятный ущерб при реализации рисков.

По данному показателю оценка раскрытия информации для всех исследуемых компаний составляет 0 баллов (уровень «Отсутствие информации), как показано на рис. 10.

Заключение

В результате сравнительного анализа и оценки раскрытой информации выделяются два лидера.

Так, к лидерам в области управления рисками, включая социальные и экологические, среди российских компаний нефтегазового сектора, реализующих проекты в Арктике, относятся Газпром нефть и Зарубежнефть. Данные компании наиболее подробно раскрыли информацию о функционирующей системе управления рисками, представили реестр рисков с описанием как самих рисков, так и мер по управлению ими, раскрыли информацию об управлении социальными и экологическими рисками, включая риски, которые касаются ведения

Сравнительная таблица уровня раскрытия информации в годовых отчетах российских нефтегазовых компаний по показателям *Таблица 7*

	Система управления рисками	Реестр ключевых рисков	Социальные и экологические риски	Карта рисков	Итого
Газпром нефть	10	10	10	0	30
ЛУКОЙЛ	5	10	0	0	15
Роснефть	5	0	0	0	5
Зарубежнефть	10	10	10	0	30
Сургутнефтегаз	3	10	5	0	18
НОВАТЭК	3	10	10	0	23

экономической деятельности в Арктике, как показано в табл. 7.

В заключение необходимо отметить, что данный анализ базируется на публичной нефинансовой отчетности компаний за 2014 г. и характеризует то, каким образом руководство компаний стремится показать деятельность по управлению рисками читателям отчетов, какие показатели стремится раскрыть, на что стремится обратить внимание читателя. Данное исследование является частью исследования системы социальной и экологической ответственности российских нефтегазовых компаний в Арктике, в которую помимо аспекта управления рисками также входят процессы взаимодействия с заинтересованными сторонами, изучение социальных и экологических проектов. Изучение системы социальной и экологической ответственности позволит понять, какие существуют области для совершенствования и развития в области корпоративной ответственности российских нефтегазовых компаний, реализующих проекты в Арктике.

Литература

1. Газпром нефть. Отчет об устойчивом развитии 2014. Стремиться к большему. 2014. URL: http://ir.gazprom-neft.ru/fileadmin/user_upload/documents/annual_reports/gpn_sr_2014_rus_web.pdf
2. Зарубежнефть, 2014. Годовой отчет 2014. Стратегия роста. URL: http://www.nestro.ru/ru/press-centr/novosti/249/
3. ЛУКОЙЛ, 2014. Годовой отчет 2014. Всегда в движении. URL: http://media.rspp.ru/document/1/f/f/ffd017da27cddfcf040fc321ff8378c0.pdf
4. Нефинансовая отчетность. ЭНПИ Консалт. URL: http://www.npg.ru/?page=services&subpage=nonfinance
5. НОВАТЭК, 2014. Годовой отчет 2014. Новое качество роста. URL: http://www.dex.ru/design/portfolio/annual_reports/novatek/
6. Основы государственной политики Российской Федерации в Арктике на период до 2020 года и дальнейшую перспективу [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/98.html
7. Роснефть, 2014. Годовой отчет 2014. Победа, эффективность, ответственность. URL: http://www.rosneft.ru/docs/report/2014/main.html
8. Соглашение о сотрудничестве в авиационном и морском поиске и спасании в Арктике. 2011. URL: http://www.szrf.ru/doc.phtml?nb=edition02&issid=2013009000&docid=16
9. Сургутнефтегаз, 2014. Годовой отчет 2014. URL: http://www.surgutneftegas.ru/investors/reports/annual/
10. Arctic Climate Issues 2015: Short-lived Climate Pollutants, AMAP, Summary for Policy-makers Arctic Monitoring and Assessment Program (AMAP), 2015. Summary for Policymakers: Arctic Climate Issues 2015. Oslo, Norway. 2015. 16 p.
11. ArcticEconomicCouncil.URL:http://arcticeconomiccouncil.com/
12. Ernst & Young. Arctic oil and gas. London. 2013. 2 p.
13. IPCC Climate change 2014: Synthesis Report https://www.ipcc.ch/pdf/assessment-report/ar5/syr/SYR_AR5_FINAL_full_wcover.pdf IPCC, 2014. Climate Change 2014: Synthesis Report. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change [Core Writing Team, R.K. Pachauri and L.A. Meyer (eds.)]. IPCC. Geneva. Switzerland. 151 p.
14. ISO 19906: 2010 Petroleum and natural gas industries — Arctic offshore structures.
15. Lloyd's report. Arctic Opening: Opportunity and Risk in the High North. Lloyd's, London: Chatham House. 2012. 60 p.
16. Mathis J.T. The extent and controls on ocean acidification in the western Arctic Ocean and adjacent continental shelf seas. Arctic Report Card, Update for 2011. URL: http://www.arctic.noaa.gov/report11/ArcticReportCard_full_report.pdf
17. Opportunities and challenges for Arctic oil and gas development. Eurasia Group report for the Wilson Center. Washington, D.C., 2014. http://dx.doi.org/10.4043/24586-MS0
18. Rover C., Ridder-Strolis K. A sustainable Arctic: preconditions, pitfalls and potentials. October 2014. Norway. URL: http://www.kas.de/wf/doc/kas_39168-1522-2-30.pdf?141112150837
19. Sustainable Development Working Group of the Arctic Council. URL: http://www.sdwg.org/
20. U.S. Department of Energy, Energy Information Administration, "Arctic Oil and Gas Potential", October 2009.

Сведения об авторах

Бобылев Сергей Николаевич: доктор экономических наук, заведующий кафедрой экономического факультета МГУ им. М.В. Ломоносова, академик РАЕН
Количество публикаций: 263
Область научных интересов: устойчивое развитие, экономика использования природных ресурсов и охраны окружающей среды
Контактная информация:
Адрес: 119991, г. Москва, Ленинские горы, д. 1, стр. 46
Тел.: +7 (916) 586-69-55
E-mail: snbobylev@yandex.ru

Никоноров Сергей Михайлович: доктор экономических наук, ведущий научный сотрудник кафедры экономики природопользования экономического факультета МГУ им. М.В. Ломоносова
Количество публикаций: 103
Область научных интересов: природопользование, экономика природопользования, проектный анализ в природопользовании
Контактная информация:
Адрес: 119991, г. Москва, Ленинские горы, д. 1, стр. 46
Тел.: +7 (963) 723-07-35
E-mail: nico.73@mail.ru

Корнилова Анастасия Вячеславовна: аспирант кафедры экономики природопользования экономического факультета МГУ им. М.В. Ломоносова
Количество публикаций: 11
Область научных интересов: устойчивое развитие, экономика природопользования, управление социальными и экологическими рисками, корпоративная ответственность
Контактная информация:
Адрес: 119991, г. Москва, Ленинские горы, д. 1, стр. 46
Телефон: +7 (905) 534-03-47
E-mail: terrarctic@gmail.com

Онлайн-подписка на сайте podpiska.pochta.ru

Подписной индекс журнала «Проблемы анализа риска» П3448

УДК 338.012

ISSN 1812-5220

Идентификация рисков в международной транспортно-экспедиторской деятельности

Е. В. Ценина,
Российский экономический университет им. Г. В. Плеханова, г. Москва

Т. Т. Ценина,
Санкт-Петербургский государственный экономический университет

Аннотация

В статье рассматриваются основные виды рисков транспортно-экспедиторской деятельности. Сбой в одном из звеньев логистической цепи автоматически повышает вероятность рисковой ситуации на всем протяжении цепи, поэтому необходимо строить логистическую цепь исходя из оценки устойчивости каждого звена, понимая, какова вероятность возникновения рисков в тех или иных операциях.

Ключевые слова: транспортно-экспедиторская компания, транспортно-экспедиторские услуги, управление рисками.

Содержание

Введение

Специфика правовых и экономических международных торговых отношений, неодинаковые внутригосударственные условия поставок товаров, различный уровень сервиса и информационного обеспечения перевозок, своеобразие транспортного законодательства и таможенных процедур в каждой стране усложняют связи между участниками транспортно-экспедиторской деятельности, что приводит к появлению рисковых ситуаций. Анализ и контроль рисковых ситуаций на каждом этапе перевозочного процесса являются одними из важнейших этапов менеджмента. Это связано с тем, что все транспортно-экспедиторские процессы взаимосвязаны и сбой в одном из процессов автоматически влияет на всю логистическую цепочку.

Транспортно-экспедиторский риск рассматривается как риск нарушения координации оптимальной работы участников перевозочного процесса в транспортно-экспедиторской деятельности, которое приводит к непредвиденным затратам (ущерб) или упущенной прибыли. Интересно, что, как показывают исследования, инструментарий, применяемый в практике управления субъектами хозяйствования в цепях поставок, в большинстве своем ориентирован на анализ

и оптимизацию затрат. Это отвечает основной цели логистики, выполнению правила: «с минимальными затратами нужный товар в нужное место и нужное время при должном уровне сервиса» [1]. Кроме того, если мы говорим о международных перевозках, то неопределенность, связанная с их организацией, может быть значительно выше, чем в пределах одного государства. Риски связаны с нестабильным спросом, сроками поставок, уровнями товарных запасов и заказов, производственными возможностями, спецификой таможенного администрирования, временем транспортировки, природными и человеческими факторами и т. д. Для того чтобы их снизить и обеспечить высокий уровень обслуживания, необходимо устранить источники нестабильности и неопределенности [2—4].

1. Комплексное рассмотрение рисков

При оказании экспедиторских услуг в полном объеме транспортная экспедиция подразумевает организацию перевозки грузов от двери склада грузоотправителя до двери склада грузополучателя (используется термин «от двери до двери»). В этом случае полный комплекс услуг по доставке груза включает:

- доставку от склада грузоотправителя на грузовую железнодорожную станцию, в порт, в аэропорт;
- погрузку в транспортное средство (автомобиль, вагон, корабль, самолет);
- оплату по тарифу за перевозку грузов;
- выгрузку из транспортного средства, например вагона на станции назначения;
- доставку груза автомобильным транспортом до склада грузополучателя.

В перечень транспортно-экспедиторских услуг входят:

- разработка по поручению клиента маршрута перевозки груза при перевозках несколькими видами транспорта (смешанные или так называемые мультимодальные и интермодальные перевозки);
- заключение договоров с другими экспедиторами и участниками перевозочного процесса для фрахтования морских и речных судов, самолетов, вагонов и автомобилей;
- оформление транспортных документов: транспортных накладных, коносаментов и других документов, необходимых для доставки грузов по назначению;
- оплата тарифов за перевозку и других платежей и сборов;
- страхование грузов, участие в оформлении документов при повреждении, порче или недостаче грузов (так называемые несохранные перевозки) [5];
- выполнение обязанностей таможенного брокера при перевозках экспортно-импортных грузов;
- информирование грузоотправителей о продвижении грузов, розыск грузов в случае их потери;
- организация при необходимости переадресовки грузов в пути следования;
- получение разрешений и оформление документов на перевозку опасных, крупногабаритных и тяжеловесных грузов;
- другие услуги по поручению клиентов.

Рассмотренные выше функции и операции являются основными рычагами деятельности транспортно-экспедиторской компании. Современные тенденции приводят к тому, что работа компании зависит от грамотной синхронизации всех участников перевозочного процесса.

Каждое звено логистической цепи подвержено рискам. Особенность состоит в том, что данные риски нельзя рассматривать отдельно друг от друга. В современной деловой среде, где организации и рынки образуют сложную взаимосвязанную глобальную сеть, риски могут возникать быстро, провоцируя цепную реакцию на других рынках, кроме того, существует взаимное влияние рисков друг на друга [3, 6]. Подобный эффект определяется термином «логистическая синергия» [7]. На степень общего транспортно-экспедиторского риска оказывают влияние многие процессы, происходящие во время перевозки. Так, введение санкций Евросоюзом значительно повлияло на конфигурацию и функционирование цепей поставок. Многие участники были вынуждены переориентировать свои цепи поставок в сторону Азии или приостановить движение материальных потоков [8].

Необходимо научиться оценивать общий риск и минимизировать его, выявляя слабые звенья в логистической цепи.

Сбой в одном из звеньев логистической цепи автоматически повышает вероятность рисковой

ситуации на всем протяжении цепи. Именно поэтому необходимо уметь строить логистическую цепь исходя из оценки устойчивости каждого звена [3, 7].

2. Выявление слабого звена цепи поставок

Однако для того чтобы определять степень уязвимости звена и всей цепи поставок в целом, необходимо уметь проводить оценку рисков всех процессов, протекающих в цепи. Точность результата будет зависеть от количества процессов [5, 9].

В таблице представлены риски с соответствующими процессами, в которых они могут возникать во время транспортно-экспедиторского обслуживания. Стоит подчеркнуть, что некоторые из причин их возникновения не зависят от решения менеджмента (ДТП, задержка рейса), однако реализация такого риска становится причиной появления риска повреждения груза или его задержки, что относит их к транспортно-экспедиторским. Таким образом, транспортно-экспедиторский риск не просто сопровождает логистические операции транспортировки, но и напрямую влияет на эффективность работы цепи поставок.

Выделим основные виды рисков, встречающихся при организации перевозочного процесса (см. таблицу).

Основные виды транспортно-экспедиторского риска *Таблица*

Этап	Функции	Характер услуг	Риск
I. Подготовка к процессу грузоперевозки	Консультации	1. Предоставление клиенту информации о возможности перевозки. 2. Разработка оптимальных маршрутов и оценка стоимости перевозки. 3. Информационная поддержка по таможенному оформлению. 4. Иные справочные данные	1. Получение недостоверной/неполной информации о грузе. 2. Неправильная оценка затрат на доставку груза. 3. Недостоверное информирование клиента по вопросам перевозки/таможенного оформления
	Подготовка документов к перевозке	5. Заполнение поручения экспедитору (заявки). 6. Подготовка необходимых для транспортировки документов. 7. Подготовка необходимых документов для таможенного оформления. 8. Расчет таможенных платежей	4. Указание недостоверных/неправильных данных в перевозочных документах. 5. Несоблюдение сроков предоставления документов в процессе перевозки
	Согласование форм оплаты с клиентом	9. Выбор формы оплаты (предоплата, постоплата, залог и т. д.)	6. Риск коррекции счета в процессе транспортировки. 7. Риск неоплаты
	Информирование агента в стране назначения об отправке груза	10. Предоставление агенту информации о грузе, схеме перевозки, деталях таможенного оформления	8. Риск неуведомления принимающего офиса. 9. Несоответствие документов требуемым в стране
II. Подготовка груза к основной отправке	Доставка груза от отправителя на консолидационный склад	11. Согласование времени подачи машины на склад отправителя. 12. Прием товара по количеству. 13. Заполнение документов. 14. Физическое перемещение груза до консолидационного склада	10. Опоздание машины. 11. Ошибка в заполнении экспедиторской расписки. 12. Повреждение груза во время транспортировки
	Обработка груза на консолидационном складе	15. ПРР автомобиля. 16. Пересчет, взвешивание товара и сверка с документами. 17. Внесение фактических данных о грузе в информационную базу. 18. ПРР на складе. 19. Палетирование, маркировка. 20. ПРР на автотранспорт. 21. Подготовка транспортных документов	13. Повреждение груза при ПРР. 14. Ошибка при занесении данных в информационную базу. 15. Повреждение, воровство и т. д. на складе. 16. Некачественное выполнение упаковки, маркировки т. д. 17. Неправильное распределение груза в автомобиле

Таблица (*окончание*)

Этап	Функции	Характер услуг	Риск
	Оформление основных транспортных документов	22. Бронирование на рейс. 23. Оформление транспортных накладных	18. Несоответствие бронирования информации по срокам, предоставленной клиенту. 19. Ошибка при заполнении либо несоответствие документов требованиям правил международных перевозок грузов
	Доставка груза в порт, аэропорт, ж/д станцию для основной отправки	24. Физическое перемещение груза до места отправки. 25. ПРР в порту, аэропорту и сдача груза на склад	20. Повреждение груза при доставке, ПРР. 21. Несоответствие документов для въезда машины, ПРР в порт, аэропорт и т. д.
	Оформление экспортных таможенных документов	26. Предоставление в таможенные органы комплекта документов для экспорта	22. Таможенные риски. 23. Риск сверхнормативного хранения груза на терминале
III. Основная отправка	Перевозка груза ж/д, авиа-, авто-, морским транспортом	27. ПРР на борт судна. 28. Физическое перемещение. 29. ПРР в порту назначения	24. Повреждение груза. 25. Несоответствие условиям перевозки данного груза. 26. Потеря груза при консолидации в других портах
	Размещение на терминале назначения	30. ПРР на терминале. 31. Фитосанитарный контроль. 32. Размещение на терминале и подготовка документов	27. Повреждение груза. 28 Риск непрохождения фитосанитарного и радиоактивного таможенного контроля. 29. Потеря документов на груз. 30. Сверхнормативное хранение груза на терминале
IV. Подготовка груза к финальной доставке	Таможенное оформление импортного груза	33. Получение у получателя необходимых документов для регистрации и таможенного оформления груза. 34. Оплата пошлин, сборов, налогов и т. д.	31. Таможенный риск
	Доставка груза на консолидационный склад	35. Прием товара по количеству. 36. Заполнение документов. 37. Физическое перемещение груза до консолидационного склада	32. Повреждение груза
	Обработка груза на консолидационном складе	38. ПРР автомобиля. 39. Пересчет, взвешивание товара и сверка с документами. 40. Внесение фактических данных о грузе в информационную базу. 41. ПРР на складе. 42. Палетирование, маркировка. 43. ПРР на автотранспорт. 44. Подготовка транспортных документов	…
V. Финальная стадия доставки груза	Доставка до клиента		….
	Оплата		…
	Закрытие документов		….

Заключение

Транспортно-экспедиторский риск напрямую связан с предоставлением транспортно-экспедиторских услуг. Основной чертой транспортно-экспедиторского риска является тот факт, что его нельзя рассматривать отдельно в призме транспортного и экспедиторского риска. Это связано с тем, что компании, осуществляющие такого рода деятельность, должны анализировать данные области как единое целое с целью грамотной и синхронной координации перевозочного процесса. Необходимо стремиться к тому, чтобы чувствительность к рискам и их предотвращение обеспечивались за счет анализа и мониторинга в режиме реального времени. Управление рисками должно быть формализовано во всех звеньях цепи, но при этом должно оставаться гибким [9] и даже при незначительных изменениях в цепи поставок обеспечивать возможность быстрого реагирования и адаптации.

Литература

1. Киреева Н.С. Инструменты логистики в контексте концепции создания добавленной стоимости // Российское предпринимательство. 2013. №1 (223). С. 79—82.
2. Смирнова Е.А. Особенности управления трансграничными цепями поставок // Инновационная деятельность. 2014. № 2 (29). С. 66—69.
3. Ценина Е.В., Ценина Т.Т. Стратегия смягчения рисков в глобальных цепях поставок // Известия Санкт-Петербургского государственного экономического университета. 2014. № 5. С. 69—74.
4. Ценина Т.Т., Ценина Е.В. Развитие транспортно-логистических схем доставки внешнеторговых грузов // Логистика. 2016. № 5. С. 14—15.
5. Ценина Т.Т., Ценина Е.В. Организация и регулирование внешнеторговой деятельности: учеб. пособие. СПб.: Изд-во СПбГУЭФ, 2012. С. 155—230.
6. Ценина Е.В., Коробейников Ю.В. Риски в логистике снабжения (на примере компаний, работающих на российском рынке) // Известия Санкт-Петербургского государственного экономического университета. 2014. № 2. С. 73—78.
7. Ценина Т.Т. Бизнеса круг, риски вокруг, диверсификация рисков в сфере бизнеса // Российское предпринимательство. 2005. № 2. С. 125—130.
8. Гвилия Н.А. Кластеризация как вектор повышения конкурентоспособности логистической инфраструктуры корпораций в современных условиях // РИСК: Ресурсы. Информация. Снабжение. Конкуренция. Аналитический журнал. 2014. № 3. С. 60—65.
9. Ценина Т.Т., Ценина Е.В. Уровни сложности операций в цепях поставок и риск-менеджмент // Логистика: современные тенденции развития. Международной научно-практической конференции. 9—10 апреля 2015. СПб.: Изд-во ГУМРФ им. адм. С.О. Макарова, 2015. С. 367—369.

Сведения об авторах

Ценина Екатерина Владимировна: кандидат экономических наук, доцент кафедры предпринимательства и логистики РЭУ им. Г.В. Плеханова

Количество публикаций: 93, в том числе 1 монография и 3 учебных пособия

Область научных интересов: логистика, управление цепями поставок, управление рисками, оценка эффективности и оптимизация логистических систем, международные перевозки

Контактная информация:

Адрес: 117997, г. Москва, Стремянный пер., д. 36

Тел.: +7 (499) 236-80-30

E-mail: cakie@yandex.ru

Ценина Татьяна Тихоновна: кандидат экономических наук, доцент кафедры логистики и управления цепями поставок СПбГЭУ

Количество публикаций: 230 научных и учебно-методических работ, в т.ч. 161 научная работа и 69 учебно-методических работ, из них 18 учебных пособий

Область научных интересов: логистика, управление цепями поставок, управление рисками, организация и регулирование внешнеторговой деятельности, международные перевозки

Контактная информация:

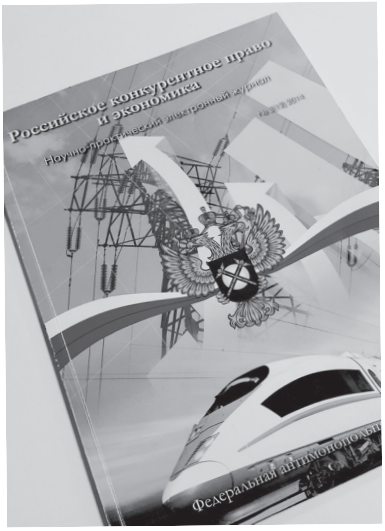
Адрес: 192007, г. Санкт-Петербург, ул. Прилукская, д. 3

Тел.: +7 (812) 766-45-83

E-mail: cakie@yandex.ru

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

«РОССИЙСКОЕ КОНКУРЕНТНОЕ ПРАВО И ЭКОНОМИКА»



Свидетельство о регистрации средства массовой информации ПИ № ФС77-60362 от 29.12.2014 г.

Ведущий научно-практический журнал в области конкурентного права и антимонопольного регулирования, выпускаемый ФАС России совместно с издательским домом «Деловой экспресс».

На страницах издания публикуются актуальные материалы, посвященные вопросам антимонопольного регулирования и защиты конкуренции: информация о деятельности ФАС России и развитии антимонопольного законодательства; анализ правоприменительной и судебной практик; результаты научных исследований в области конкурентного права и связанных с ним экономических вопросов; обобщение опыта эффективной организации работы антимонопольной службы и др. Также в журнале освещаются круглые столы, конференции, дискуссии по вопросам в сфере конкурентного права, аспекты международного сотрудничества. Особое внимание журнал уделяет практической применимости публикуемых материалов.

Издание адресовано сотрудникам антимонопольных органов, специалистам-практикам, представителям бизнес-сообщества, консультантам, специалистам научных организаций, учащимся и преподавателям учебных заведений, а также широкому кругу заинтересованных читателей.

Разъясняя государственную политику в области защиты конкуренции, журнал призван содействовать повышению уровня правовой культуры, а также осуществлять обратную связь с читателями, выявляя их мнения о состоянии конкуренции в Российской Федерации.

Издание зарегистрировано в РИНЦ и готовится к включению в перечень рецензируемых научных журналов, рекомендованных Высшей аттестационной комиссией Минобрнауки России (ВАК) для опубликования основных научных результатов диссертаций на соискание ученых степеней доктора и кандидата наук.

Издается в печатном и электронном виде с периодичностью раз в квартал.

УЧРЕДИТЕЛИ:

- Федеральное государственное автономное учреждение «Учебно-методический центр ФАС России» (г. Казань)
- Акционерное общество «Финансовый издательский дом «Деловой экспресс»

ГЛАВНЫЙ РЕДАКТОР:

Сушкевич Алексей Геннадьевич,
кандидат экономических наук,
заслуженный экономист РФ,
директор Департамента
антимонопольного регулирования ЕЭК

Издается: с 2011 года
Периодичность: ежеквартально
Распространение: подписка
Язык: русский
Издатель: АО ФИД «Деловой экспресс»
Телефон: (495) 787-52-26
Индекс «Пресса России»: 43225
Сайты: www.fas.gov.ru
www.dex.ru

ОСНОВНЫЕ РУБРИКИ:

- Антимонопольное законодательство
- Антимонопольное регулирование
- Антимонопольный контроль
- Региональная практика
- Судебная практика

РЕКЛАМА В ЖУРНАЛЕ:

Размещение рекламы в журнале «Российское конкурентное право и экономика» позволяет напрямую обращаться к целевой аудитории и в то же время дает возможность рассказать о технологиях, мероприятиях, услугах и продукции.

Информацию о стоимости размещения рекламного модуля в журнале можно узнать

- по телефону (495) 787-52-26
- или написать на почту journal@dex.ru.

ТЕРРИТОРИЯ РАСПРОСТРАНЕНИЯ:

Управления ФАС России, Государственная дума РФ, администрации субъектов РФ, комитеты и комиссии союза предпринимателей и промышленников России, государственные и муниципальные предприятия, ректораты и библиотеки вузов, руководители ведущих российских компаний и частные лица.

Стоимость подписки на 2017 год

Печатная версия	800 руб. — за полугодие;	1600 руб. — за год
Электронная версия	400 руб. — за полугодие;	800 руб. — за год

УДК 614.8

Возможные перспективы создания новых видов химического оружия и меры по снижению опасности от их применения

ISSN 1812-5220

В. П. Малышев,
ФКУ ЦСИ ГЗ МЧС России,
г. Москва

Аннотация

В настоящей статье на основе открытых литературных данных рассмотрены возможные направления создания новых видов химического оружия и предложены направления деятельности, позволяющие снизить риск от их применения. Для создания новых видов химического оружия могут быть использованы достижения в области биотехнологий, позволяющие в настоящее время с высокой степенью достоверности устанавливать механизмы действия опасных веществ на жизненно важные системы организма и тем самым определять принципиально новые способы поиска высокотоксичных соединений. По мнению автора, одним из реальных направлений создания новых видов химического оружия является использование достижений нанотехнологий, которые в состоянии обеспечить наиболее эффективную доставку опасных веществ к жизненно важным системам организма. Из-за малого размера наночастицы могут изменить физико-химические свойства веществ и обеспечить переход их от твердой фазы к паровой, что позволяет существенно повысить поражающие свойства отравляющих веществ и одновременно существенно расширить круг токсичных веществ, пригодных для создания новых видов химического оружия.

Ключевые слова: химическое оружие, отравляющие вещества, биотехнологии, нанотехнологии, международный контроль, средства и способы защиты от химического оружия.

Содержание

Введение

Создание новых видов химического оружия может быть достигнуто на основе использования высоких технологий, таких как биотехнологии и нанотехнологии. Достижения в биотехнологиях связаны в первую очередь с расшифровкой генома человека и ряда других организмов (животных, растений, бактерий, вирусов) и накоплением критического объема знаний в области исследования механизма действия физиологически активных веществ на жизненно важные системы организма. Получены серьезные результаты в исследованиях свойств и характери-

стик высокотоксичных химических и биологически активных веществ различной природы, методов их получения, механизмов взаимодействия на молекулярном и клеточном уровнях. Как следствие этих достижений появилась реальная возможность открытия особо опасных веществ, искусственных биологических макромолекул и простейших организмов. Методы генной и белковой инженерии позволяют получать и культивировать различные белково-нуклеотидные конструкции с определенными характеристиками, а существующие методы доставки в выбранные участки организма обеспечивают заданное воздействие на молекулярном уровне на жизненно важные системы организма.

Другим направлением может стать использование успехов в развитии нанотехнологий. Достижения нанотехнологий открывают беспрецедентные возможности технологического прогресса и приводят к появлению нового поколения техники или к новым способам производства, технологическим укладам, формированию новых отраслей, способных в том числе решать задачи обеспечения оборонной безопасности. Наночастицы, позволяющие вследствие малого размера придавать твердым веществам свойства парообразных веществ, успешно используются в токсикологии, микробиологии, медицине и сельском хозяйстве. С их помощью найдены подходы к решению многих проблем медицины и здравоохранения и могут быть обеспечены наиболее эффективные способы доставки опасных веществ к жизненно важным системам организма. К сожалению, эта их способность может быть использована для создания новых видов химического оружия.

В настоящей статье проведен анализ различных способов применения химического оружия, рассмотрены возможные направления его дальнейшего развития и предложены меры по парированию угроз создания новых видов химического оружия.

1. История создания и применения химического оружия

Рождение химического оружия (ХО) как средства ведения вооруженной борьбы в современном понимании следует отнести ко времени Первой мировой войны. Предпосылки к широкому применению в войне отравляющих веществ (ОВ) сложились в результате развития химической промышленности. К середине XIX века, когда химия достигла значительного развития, масштабы и возможности производства уже известных высокотоксичных веществ, например хлора, фосгена, резко возросли. В рамках синтеза и исследований физиологически активных веществ шел активный поиск отравляющих веществ, в качестве которых использовались не только хлор, фосген и дифосген, синильная кислота и иприт, но и большое количество иных соединений раздражающего и смертельного действия.

Отцом химического оружия стал немецкий ученый Фриц Габер, который накануне Первой мировой войны занялся проблемами использования на полях сражений токсичных химических веществ, причем в максимально больших масштабах. Из всех противостоящих стран только Германия обладала промышленным потенциалом, необходимым для крупномасштабного сжижения хлористого газа, и, по мере того как война приобретала затяжной характер, этот потенциал давал ей сравнительное преимущество в качестве одного из возможных способов покончить с окопной войной и с нехваткой боеприпасов.

Именно по предложению Фрица Габера и под его непосредственным техническим руководством 22 апреля 1915 г. на Западном фронте у г. Ипр (Бельгия) была проведена газовая атака. Эта химическая атака имела стратегический успех: 180 т газа, выпущенного из 5730 баллонов под давлением по направлению ветра в сторону противника, привели к поражению 15 тыс. французских, алжирских и канадских солдат, из которых около 5 тыс. погибло на поле боя. После чего все воюющие стороны стали широко применять снаряды и бомбы, начиненные различными отравляющими веществами. В результате применения химического оружия в ходе боевых действий Первой мировой войны число погибших достигло одного миллиона человек, а около 5 миллионов получили поражения различной степени тяжести.

Весь ход боевых действий во время Первой мировой войны продемонстрировал значительное преимущество применения ОВ по сравнению с фугасными средствами того времени. Химическое оружие было применено противоборствующими сторонами многократно и в больших объемах (около

120 тыс. т). Высокая эффективность применения ОВ против незащищенной живой силы и тяжелые последствия поражения стимулировали поиски новых, более эффективных ОВ и способов их применения в странах, проводящих агрессивную политику.

В период между Первой и Второй мировыми войнами ХО продолжало усиленно накапливаться в разных странах, шел поиск все более и более токсичных веществ. Наибольшие успехи в разработке ОВ связаны с исследованиями в области *эфиров фосфорной и алкилфосфиновых кислот.* В 1938 г. в лаборатории инсектицидов Герхард Шрадер получил диизопропиловый эфир фторфосфорной кислоты, оказавшийся весьма токсичным веществом. Независимо от Г. Шрадера этот диэфир был синтезирован Б. Синдерсом (Великобритания). Развивая успех, Г. Шрадер в 1939 г. синтезировал зарин — изопропиловый эфир метилфторфосфиновой кислоты. Зарин примерно в 5 раз превосходит табун по ингаляционной токсичности. С июня 1944 г. зарин начал изготовляться на опытной технологической установке. К концу войны запасы зарина в Германии составили 1260 т. В конце 1944 г. в Германии был получен структурный аналог зарина, названный зоманом. Зоман примерно в три раза токсичнее зарина. Зоман до конца войны находился на стадии лабораторных и технологических исследований и разработок. Всего было изготовлено около 20 т зомана.

СССР вступил в войну со следующими мощностями: по иприту порядка 50—60 тыс. т в год, по люизиту — 12 тыс. т. В военные годы (1941—1945) в СССР производились и снаряжались в боеприпасы и емкости иприт, люизит и их смеси. Кроме этого, производилось снаряжение боеприпасов синильной кислотой и фосгеном, выпускавшимися химической промышленностью как исходные вещества для органического синтеза. Эти производства существовали до 1 января 1946 г.

В ходе Второй мировой войны применение химического оружия носило ограниченный, в основном экспериментальный характер. В Африке против Эфиопии итальянская армия применила кожно-нарывное отравляющее вещество — иприт.

США и Советский Союз, захватив в качестве трофеев запасы табуна и зарина, снаряженные ими боеприпасы, а также технологическое оборудование заводов по их изготовлению, предприняли всевозможные меры по организации собственного производства этих ОВ. Советская армия обнаружила в восточной части Германии четыре специализированных завода по выпуску ОВ и снаряжению ими химических боеприпасов. Заводы по изготовлению табуна и технологическая установка по синтезу зарина были демонтированы и перевезены в Сталинград, где и было затем организовано изготовление ХО по немецкой технологии. В Сталинград было перевезено также оборудование химического завода по производству иприта (мощность 10 800 т в год).

Послевоенный промышленный выпуск в Советском Союзе фосфорорганических отравляющих веществ нервно-паралитического действия (ФОВ) связан с деятельностью завода в Сталинграде и вновь построенного в 1970-х гг. химкомбината в г. Новочебоксарске (Чувашия). Все производства располагались на семи предприятиях в пяти городах, главным образом в бассейне Волги (табл. 1) [1].

США на положении военнопленных отправили в Эджвудский арсенал немецких специалистов во главе с Г. Шрадером. При их участии США к 1952 г. закончили подготовительные разработки и приготовления и пустили на полную мощность вновь построенный завод по изготовлению зарина в составе армейского Рокки-Маунтинского арсенала (г. Денвер, штат Колорадо).

Успех немецких химиков, открывших табун, зарин и зоман, породил резкое расширение масштабов работ по поиску новых ОВ, проводимых в США, Советском Союзе и других странах. Результат не заставил себя долго ждать. Уже в 1952 г. в Великобритании сотрудником лаборатории химических средств защиты растений доктором Ренаджи Гошем было синтезировано еще более токсичное вещество из класса фосфорилтиохолинов.

В оборонных химических лабораториях США и Великобритании за короткое время были синтезированы сотни структурных аналогов полученного Р. Гошем фосфорилтиохолина. В США был сделан выбор в пользу О-этилового Б-2 (М, М-диизопропиламино) этилового эфира метилфосфоновой кислоты, получившего шифр Vx. В апреле 1961 г. в США, в г. Нью-Порте (штат Индиана), начал работать на полную мощность завод по производству

Перечень бывших объектов по производству химического оружия в СССР и их основные характеристики *Таблица 1*

Предприятие и город	Специализация	Год остановки/ликвидации
АО «Корунд», Дзержинск	Снаряжение боеприпасов фосгеном	1945/1949
	Снаряжение боеприпасов синильной кислотой	1946/1949
АО «Оргстекло», Дзержинск	Снаряжение боеприпасов синильной кислотой	1949/1991
АО «Сода», Березники	Иприт	1943/1959
АО «Капролактам», Дзержинск	Иприт	1957/1994
	Люизит	1946/1997
	Снаряжение боеприпасов ипритом/люизитом	1946/1992
АО «Средневолжский завод химикатов», Чапаевск	Иприт	1943/1957
	Люизит	1944/1993
	Снаряжение боеприпасов ипритом/люизитом	1946/1990
АО «Химпром», Волгоград	Иприт/люизит	1957/1957
	Снаряжение боеприпасов ипритом/люизитом	1951/1957
	Опытное производство ФОВ	1975/1975
	Зоман	1987/1993
	Снаряжение боеприпасов ФОВ	1987/1997
	DF	1987/1991
АО «Химпром», Новочебоксарск	Снаряжение боеприпасов Vx	1987/1997
	Снаряжение боеприпасов Vx и зоманом	1987/1997
	Vx	1978/1997

вещества Vx и снаряженных им боеприпасов. Годовая производительность завода в год при его пуске равнялась 5 тыс. т вещества.

В начале 1960-х гг. производство вещества Vx и соответствующих химических боеприпасов было создано и в Советском Союзе, вначале только на химическом комбинате в Волгограде, а затем и на новом заводе в г. Чебоксары на Средней Волге. Вещество Vx токсичнее зарина примерно в 10 раз при внутривенном введении, ингаляции и при накожной аппликации. Однако из-за низкой летучести это вещество может применяться в виде аэрозольной составляющей, что существенно ограничивает его поражающие свойства.

В арсеналы вооружений ведущих государств мира в конце 1960-х и начале 1970-х гг. поступило новое поколение ХО. Артиллерийские и авиационные химические боеприпасы, так же как и боевые химические части ракет ближнего и среднего радиуса действия, снаряженные нервно-паралитическими газами, позволяли наносить эффективные удары по любым целям в зоне боевых действий при любых погодных условиях и в любые сезоны года.

Высокая эффективность боевого применения химического оружия обусловила необходимость развертывания специальных исследований по поиску особо опасных химических веществ во многих странах мира. В результате развернутых работ были получены опасные химические вещества широкого спектра действия: нервно-паралитические, кожно-нарывные, удушающие, слезоточивые, психотропные. Параллельно совершенствовались средства применения отравляющих веществ с помощью авиационных бомб и артиллерийских снарядов,

а также выливных авиационных приборов. Наряду с гонкой химических вооружений с 30-х гг. прошлого столетия в ряде стран мира (Японии, США и Великобритании) развертываются работы по созданию токсинного оружия. Обнаруживаются наиболее опасные вещества биологической природы — токсины: ботулотоксин, рицин, токсин столбняка и другие. Характеристики токсичности опасных веществ и токсинов приведены на рис. 1 [2].

Из данного рисунка наглядно видно, что наиболее токсичные вещества имеют большой молекулярный вес и представляют собой твердые вещества. Однако, несмотря на то что токсины на несколько порядков превосходят по токсичности фосфорорганические отравляющие вещества, они существенно уступают им по эффекту боевого применения из-за невозможности создания устойчивого облака порошкообразных токсинов в приземном слое атмосферы. Как свидетельствует опыт применения химического оружия, наибольший эффект достигается в случае создания крупномасштабного облака отравляющих веществ в приземном слое атмосферы на высоте 1—2 м от поверхности земли. Возможность создания крупномасштаб-

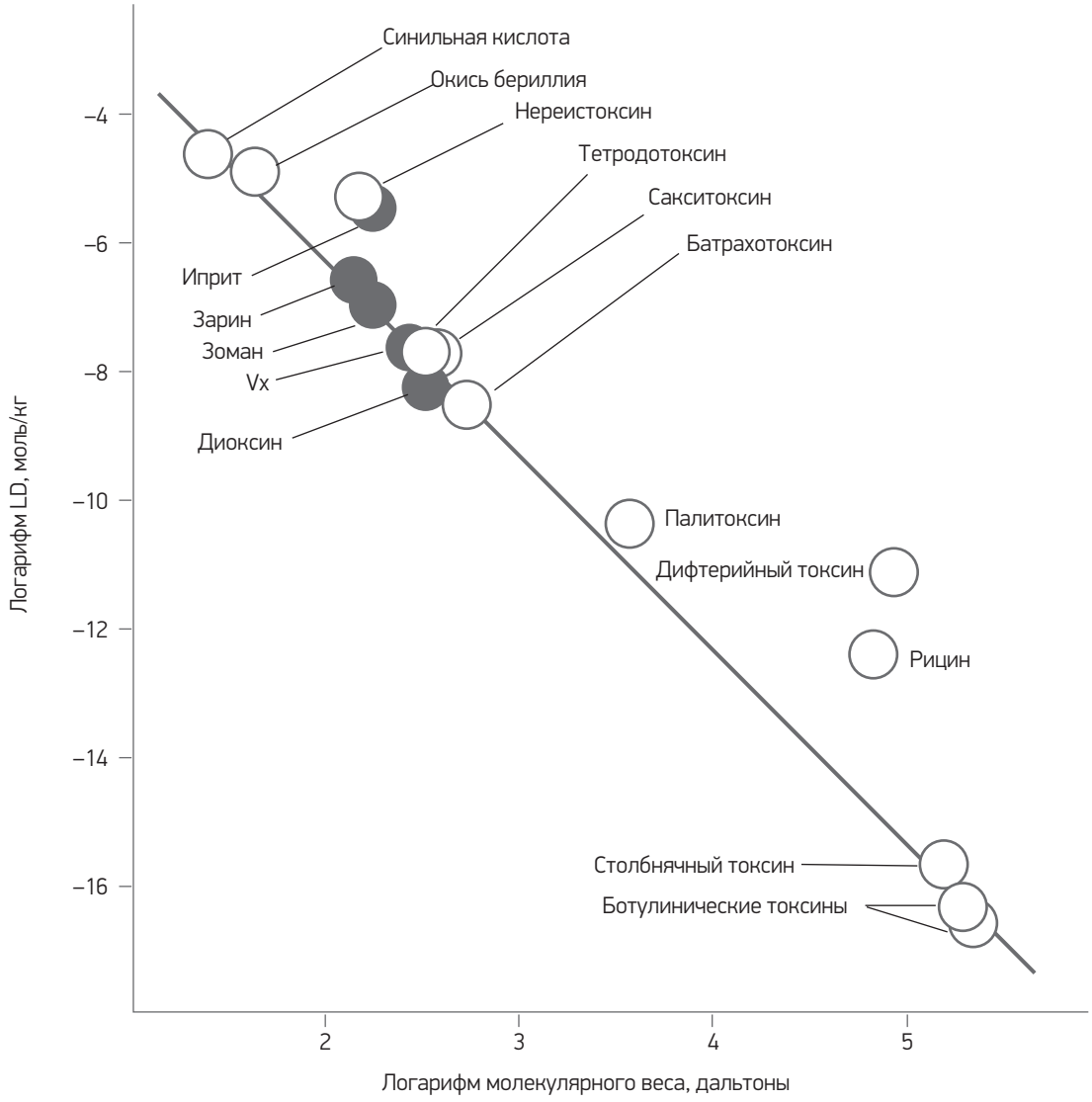


Рис. 1. Уровень токсичности наиболее опасных веществ

ного облака отравляющих веществ в приземном слое атмосферы зависит от их физико-химических свойств (желательно жидкое состояние и необходимая летучесть), метеоусловий (оптимальные условия: инверсия или изотермия, скорость ветра от 1 до 3 м в секунду) и ландшафтных особенностей местности (желательно равнинная местность, без плотной застройки и крупных лесных массивов). Предпринимаемые попытки в период с 1960 по 1990 г. создать более токсичные вещества с оптимальными физико-химическими свойствами не привели к желаемому результату. Таким образом, более токсичные ОВ так и не были получены. В настоящее время по своим физико-химическим свойствам зарин является наиболее эффективным отравляющим веществом, что подтверждается приведенной ниже статистикой его применения для поражения людей.

В то же время увеличилось число стран, располагающих химическим оружием. США в ходе боевых действий во Вьетнаме широко использовали временно выводящие из строя отравляющие вещества и средства борьбы с растительностью — фитотоксиканты. Массированное применение химического оружия, в первую очередь зарина, осуществляли вооруженные силы Ирака в ходе военного конфликта с Ираном [2]. В Сирии как правительственные войска, так и боевики террористической организации «Исламское государство» применяли химическое оружие — зарин и иприт. Благодаря участию Российской Федерации запасы химического оружия Сирийской Арабской Республики в количестве около 1000 т, в основном зарин и иприт, были уничтожены под контролем Организации по запрещению химического оружия.

Отдельные инциденты с применением отравляющих веществ, а также угрозы использования химических отравляющих веществ имели место:

- в начале 70-х гг. прошлого столетия проарабские террористические группировки планировали применить отравляющие вещества в Европе против американского посольства и складов хранения ядерного оружия;
- в 1972 г. в США была пресечена попытка националистической группы «Минитмены» с помощью синильной кислоты заразить систему кондиционирования воздуха в здании ООН в Нью-Йорке;
- в середине 70-х гг. прошлого века антикастровские группировки в США получали от чилийской спецслужбы DINA зарин для использования против противников хунты;
- в 1978 г. палестинские террористические группировки организовали заражение ртутью партий апельсинов, поставляемых из Израиля в страны Европы. Заражение сельскохозяйственной продукции с целью нанесения экономического ущерба фирмам или государству имело место на Филиппинах и Цейлоне. С угрозами террористов и вымогателей заразить химическими веществами сельскохозяйственную продукцию или источники водоснабжения сталкивались в последние годы правительства Великобритании, Германии, Австралии и Кипра;
- в 1988 г. был отмечен случай заражения цианидами партий винограда, поставленного в Европу из Чили;
- в 1991 г. американские неонацисты пытались применить синильную кислоту в синагоге;
- в качестве одной из причин появления «синдрома войны в Персидском заливе» могло быть поражение военнослужащих США и Великобритании отравляющими веществами, которые могли применить подразделения специального назначения иракской армии. Численность военнослужащих, подвергшихся воздействию ОВ, оценивается в 25 тыс. человек;
- в 1995 г. чилийская правоэкстремистская группировка угрожала применением зарина в метро г. Сантьяго, если не будет выпущен на свободу генерал Контрерас.

Однако наиболее крупномасштабные теракты с применением отравляющих веществ были осуществлены членами религиозной секты «Аум Сенрике» в Японии. В г. Мицумото (префектура Нагано) 27 июня 1994 г. в результате применения отравляющего вещества зарин 7 человек погибли, 144 человека получили поражения различной степени тяжести. К сожалению, японской полиции в то время выявить организаторов акции не удалось. 3 марта 1995 г. неизвестным ядовитым веществом были отравлены несколько пассажиров электропоезда в городе Иокагама, что, по мнению экспертов, было репетицией последующей крупномасштабной акции в токийском метро.

20 марта 1995 г. террористы из секты «Аум Сенрике» практически одновременно, в 8 часов утра, на 5 линиях токийского метро применили отравляющее вещество зарин. В результате хорошо спланированного и исполненного террористического акта было заражено 16 подземных станций метро. Учитывая, что используемое отравляющее вещество было невысокого качества, смертельные поражения получили только 12 человек и около 4 тыс. человек получили отравления разной степени тяжести.

Государства, обладающие большими запасами ХО (к ним относятся прежде всего Россия и США), оказались перед дилеммой: хранить и продолжать его накапливать или приступить к уничтожению, поскольку и то, и другое связано с определенной опасностью.

С начала 70-х гг. прошлого столетия начались многосторонние переговоры в рамках ООН о запрещении биологического, токсинного и химического оружия. Эти переговоры закончились принятием Конвенции о запрещении применения этих видов оружия. В настоящее время в соответствии с Конвенцией о запрещении химического оружия и его уничтожении в США и России осуществляется процесс уничтожения запасов химического оружия.

При этом необходимо отметить, что химические боеприпасы России в силу их конструктивных особенностей обладали большей стойкостью при длительном хранении. В то время как американские боеприпасы из-за конструктивного просчета (использование тонкостенных алюминиевых корпусов) начали подтекать, создавая аварийные ситуации на базах хранения. Именно эти технологические причины заставили Соединенные Штаты создать к концу 80-х гг. прошлого столетия два объекта по уничтожению ХО: пилотную установку в г. Туэль и полномасштабный объект на атолле Джонсон.

Наибольшими запасами ХО в мире обладали Россия и США, объявившие их количество в связи с планами по уничтожению: соответственно 40 и 32 тыс. т. Последовательное выполнение требований «Конвенции о запрещении разработки, производства, накопления и применения химического оружия и его уничтожении» странами, обладавшими запасами химического оружия, дает определенную уверенность в том, что в ближайшие 10—15 лет химическое оружие в современных войнах и вооруженных конфликтах широкомасштабно по населению применяться не будет. Эти страны уничтожили имеющиеся запасы химического оружия более чем на 90% и ликвидировали промышленную базу по получению отравляющих веществ и производству средств их применения.

В то же время не исключается возможность использования в ходе военных конфликтов в качестве нелетального оружия отравляющих веществ раздражающего действия, которые не попадают под запрет «Конвенции о запрещении разработки, производства, накопления и применения химического оружия и его уничтожении». Однако эти варианты применения химического оружия будут носить ограниченный характер и не потребуют создания значительных запасов средств индивидуальной защиты (СИЗ) для населения.

На взгляд многих отечественных и зарубежных специалистов, возможно несанкционированное применение отравляющих веществ и агентов в террористических целях. Особую опасность представляет применение быстродействующих фосфорорганических отравляющих веществ в замкнутом объеме помещений с приточно-вытяжной вентиляцией на станциях метрополитена и в крупных торговых центрах. Большие скорости распространения воздушных потоков с отравляющими веществами в местах скопления больших масс людей могут привести к колоссальному числу жертв.

2. Перспективы создания новых видов химического оружия

Для создания новых видов химического оружия могут быть использованы достижения в области биотехнологий, позволяющие в настоящее время с высокой степенью достоверности устанавливать механизмы действия опасных веществ на жизненно важные системы организма и тем самым определять принципиально новые способы получения высокотоксичных соединений. В последние годы в области биотехнологий уже удалось разработать методики получения обширного спектра физиологически активных белков, влияющих на болевую чувствительность и психосоматические реакции млекопитающих. Исследования таких биорегуляторов находятся на различных стадиях, вплоть до клинических испытаний на человеке [8].

Согласно имеющимся данным в организме человека используется в настоящее время 417 мишеней

(как правило, белков) для современной лекарственной терапии. Эти мишени могут быть использованы для воздействия токсичных веществ. Из всех известных болезней, учитывая тяжесть их течения и широту распространения, пока только около 100 могут считаться достаточно серьезными. Предполагается, что наиболее распространенные болезни — сердечные, астма, остеопороз, рак, диабет и гипертензия — определяются нарушениями процессов, управляемых всего 5—10 генами [5]. Однако исследования генома показывают, что как минимум 1000 генов из предполагаемых 100 тыс. могут быть непосредственно связаны с заболеваниями и при мутациях могут быть как фармацевтическими мишенями, так и уязвимыми точками при действии «генетического» оружия [4].

Достижения в области биотехнологий, обусловленные расшифровкой генома человека и других живых организмов, позволяют в настоящее время с высокой степенью достоверности устанавливать механизмы действия опасных веществ и материалов на жизненно важные системы организма и тем самым определять принципиально новые направления создания средств медико-биологической защиты [3].

Развитие методов генной инженерии позволяет получить белковые и другие вещества, в том числе высокотоксичные соединения с заранее заданными свойствами. Генная инженерия позволяет также создавать копии ДНК — на этом принципе строятся все эксперименты по клонированию, вызывающие наибольшие споры и неприятие со стороны общественности и церкви. Особым видом генного оружия является так называемое этническое оружие — оружие с избирательным генетическим фактором. Оно рассчитано на поражение прежде всего определенных этнических и расовых групп населения. Возможность разработки и последующего применения такого оружия исходит из генетических различий разных рас и этнических групп людей [7].

Анализ деятельности федеральных агентств США по развитию способов и средств биозащиты показывает резкий рост объемов НИОКР, при этом в открытой печати не приводится никаких сведений об этих программах. Огромная программа в США по защите от терроризма, использующего оружие массового поражения (прежде всего биологическое), предусматривает максимально широкое использование генной инженерии и других достижений биохимической науки как для создания эффективных средств защиты и лечения, так и новых видов токсинного оружия.

Современный уровень развития биотехнологий, характеризующийся доступностью масштабного производства биомассы микроорганизмов и токсических продуктов их жизнедеятельности, определяет возможность несанкционированной наработки токсинов в количествах, достаточных для их использования в военных целях. Ничтожно малые инфицирующие дозы, отсутствие высокочувствительных и специфических методов и средств экспресс-индикации микроорганизмов в пробах из окружающей среды, недостаточная эффективность средств общей и экстренной профилактики и патогенетического лечения определяют потенциальную угрозу использования поражающих агентов в ходе вооруженной борьбы [9].

Поэтому развитие генной инженерии и биотехнологий является обязательным стратегическим приоритетом любой страны, стремящейся обеспечить для себя безопасное и благополучное будущее [10].

Использование достижений нанотехнологий — биочипов и биологических сенсоров — позволит обеспечить доставку опасных веществ и материалов к жизненно важным системам организма. Наночастицы и наноматериалы обладают комплексом физических, химических свойств и биологическим действием (в том числе токсическим), которые часто радикально отличаются от свойств этого же вещества в форме сплошных фаз или макроскопических дисперсий (табл. 2) [12].

В передовых странах Запада деятельность, связанная с определением уровня безопасности нанотехнологий и наноматериалов для животных, человека и окружающей среды, интенсивно развивается. Так, в 2000 г. в США сформирована Национальная нанотехнологическая инициатива, координирующая работу 26 федеральных агентств. Это межведомственная программа для оценки опасных для здоровья людей химических агентов по результатам современных токсикологических тестов. В 2008 г. NNI получила бюджет в размере 1,44 млрд долл., что более чем в 3 раза превосходит расходы стартового (в 2001 г. 464 млн долл.) и на 13% выше бюджета 2007 г.

Свойства наноматериалов *Таблица 2*

Физико-химические особенности поведения веществ в наноразмерном состоянии	Изменения физико-химических свойств и биологического (в т. ч. токсического) действия
Увеличение химического потенциала веществ на межфазной границе большой кривизны	Изменение топологии связи атомов на поверхности приводит к изменению их химических потенциалов, изменению растворимости, реакционной и каталитической способности наночастиц и их компонентов
Высокая удельная поверхность наноматериалов (в расчете на единицу массы)	Увеличение адсорбционной емкости, химической реакционной способности и каталитических свойств может приводить к увеличению продукции свободных радикалов и активных форм кислорода и далее к повреждению биологических структур (липиды, белки, нуклеиновые кислоты, в частности ДНК)
Небольшие размеры и разнообразие форм наночастиц	Возможно связывание с нуклеиновыми кислотами (вызывая образование аддуктов ДНК), белками, встраивание в мембраны, проникновение в клеточные органеллы и, как результат, изменение функции биоструктур. Процессы переноса наночастиц в окружающей среде с воздушными и водными потоками, их накопления в почве, донных отложениях могут также значительно отличаться от поведения частиц веществ более крупного размера
Высокая способность к аккумуляции	Возможно, что из-за малого размера наночастицы могут не распознаваться защитными системами организма, не подвергаться биотрансформации и не выводиться из организма, что ведет к накоплению наноматериалов в растительных, животных организмах, а также в микроорганизмах, к передаче по пищевой цепи и в результате — к увеличению их поступления в организм человека

В зоне ответственности Управления по контролю за продуктами и лекарствами США лежит обеспечение безопасности, эффективности и надежности лекарств, медицинских приборов, биотехнологических продуктов, тканевых продуктов, вакцин, косметики и лекарственных препаратов, созданных для человека и животных с использованием нанотехнологий. В 2006 г. образована комиссия FDA по нанотехнологиям. Пока FDA не предъявляет дополнительных требований по безопасности нанотехнологических продуктов, поскольку не установлен их статус и отсутствует перечень данных, предоставляемых производителями, то есть оценка новинок происходит аналогично обычным препаратам. FDA заявило, что с учетом скорости развития и огромных потенциальных возможностей нанотехнологий в фармацевтической сфере законодательная база их регулирования должна быть создана в максимально сжатые сроки. Нанотехнологии в фармацевтике используются для следующих целей [6]:

- биологический скрининг, то есть поиск активных молекул (1—10 нм), взаимодействующих с биомишенью (белок или система белков размером до 100 нм);
- изучение механизма действия (поиск биомишени и выявление механизма взаимодействия с ней активной молекулы);
- компьютерный дизайн потенциально активных соединений путем расчета энергий взаимодействия молекул-кандидатов и биомишени (белка) на расстоянии нескольких нанометров;
- целенаправленный контроль и модификация формы, размера, взаимодействия и интеграции составляющих наномасштабных элементов (лиганд-биомишень, около 1—100 нм), что приводит к улучшению либо появлению дополнительных эксплуатационных и/или потребительских характеристик и свойств получаемых продуктов (повышение эффективности, биодоступности, уменьшение токсичности и побочных эффектов получаемых инновационных лекарственных препаратов);
- производство наноразмерных готовых лекарственных форм (липосомальные формы, биодеградируемые полимеры, наночастицы для направленного транспорта и т. д.).

В качестве переносчиков лекарственных веществ используются наночастицы, приведенные на рис. 2 [10].

Уже давно известны различные однокомпонентные и многокомпонентные **липосомы**, образующиеся в растворах липидов. Интерес для практических целей могут представлять липосомы размером не более 20—50 нм, которые и используются как средства доставки лекарственного средства к био-

логической мишени. Кроме того, сама природа заблаговременно подготовила большой набор наноперенощиков, например **вирусов**. Обработанные определенным образом аденовирусы могут быть эффективно использованы для вакцинации через кожу. К искусственным биогенным наночастицам, способным к направленной доставке, помимо липосом относят также липидные нанотрубки, наночастицы и наноэмульсии липидного происхождения, некоторые циклические пептиды, хитозаны, наночастицы из нуклеиновых кислот.

Наносферы и нанокапсулы относятся к семейству **полимерных наноструктур**. Если наносферы являются цельными матрицами, на полимерной поверхности которых распределяется активное вещество, то в нанокапсулах полимерная оболочка образует полость, наполненную жидкостью. Вследствие этого активное вещество выделяется в организм по различным механизмам — из наносфер высвобождение носит экспоненциальный характер, а из нанокапсул происходит с постоянной скоростью в течение длительного времени. Полимерные наночастицы можно получить из естественных либо синтетических полимеров, каковыми являются полисахариды, полимолочная и полигликолевая кислоты, полилактиды, полиакрилаты, акрилполимеры, полиэтиленгликоль (ПЭГ) и его аналоги и др. Полимерные материалы характеризуются набором ценных свойств для лекарственного транспорта, такими как биосовместимость, способность к биодеградации, функциональная совместимость.

Особый интерес вызывают **дендримеры**. Они представляют собой новый тип полимеров, имеющих не привычное линейное, а ветвящееся строение. Первый образец был получен еще в 50-е годы, а основные методы их синтеза разработаны в 80-е годы прошлого столетия. Термин «дендримеры» появился раньше, чем термин «нанотехнология», и первое время между собой они не ассоциировались. Однако в последнее время дендримеры все чаще упоминаются именно в контексте их нанотехнологических и наномедицинских применений. Дендримеры являются уникальным классом полимеров, поскольку их размер и форма могут быть очень точно заданы при химическом синтезе, что крайне важно для наноперенощиков. Дендримеры получают из мономеров, проводя последовательные

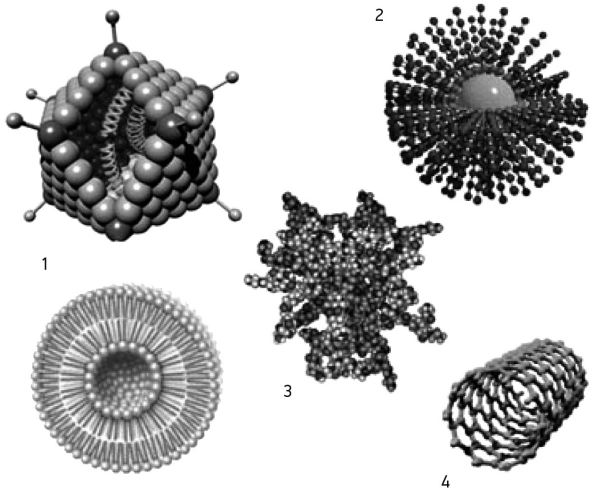


Рис. 2. Наночастицы, используемые для доставки лекарств:

1 — липосома и аденовирус; 2 — полимерная наноструктура; 3 — дендример; 4 — углеродная нанотрубка

конвергентную и дивергентную полимеризации (в том числе используя методы пептидного синтеза), задавая таким способом характер ветвления. Типичными мономерами, используемыми в синтезе, служат полиамидоамин и аминокислота лизин. Целевые молекулы связываются с дендримерами либо путем образования комплексов с их поверхностью, либо встраиваясь глубоко между их отдельными цепями. Кроме того, на поверхности дендримеров можно стереоспецифически расположить необходимые функциональные группы, которые с максимальным эффектом будут взаимодействовать с вирусами и клетками. Примером создания активного вещества на основе дендримера является препарат Vivigel — гель, способный защитить от ВИЧ-инфекции.

Среди углеродных наночастиц, образованных только атомами углерода, наиболее широко распространены **фуллерены** и **нанотрубки**, которые можно получить с помощью разнообразных химических или физико-химических методов. Например, в промышленных масштабах фуллерены получают термическим распылением углеродсодержащей сажи в атмосфере инертного газа, при пониженном давлении, в присутствии катализатора. Фуллерены, по мнению

экспертов, могут стать основой не только для систем доставки, но и для нового класса лекарственных средств. Главная особенность — их каркасная форма: молекулы выглядят как замкнутые, полые внутри оболочки. Самая знаменитая из углеродных каркасных структур — это фуллерен C_{60}, абсолютно неожиданное открытие которого в 1985 г. вызвало целый бум исследований в этой области (Нобелевская премия по химии за 1996 г. была присуждена именно первооткрывателям фуллеренов). После разработки методики получения фуллеренов в макроколичествах было обнаружено множество других, более легких либо более тяжелых фуллеренов: начиная от C_{20} и до C_{70}, C_{82}, C_{96} и выше. На основе фуллеренов разрабатываются средства доставки препаратов для лечения ВИЧ-инфицированных пациентов и онкологических больных.

В 1991 г. были обнаружены длинные, цилиндрические углеродные образования, получившие названия **нанотрубок** [11]. Они характеризуются разнообразием форм: большие и маленькие, однослойные и многослойные, прямые и спиральные; уникальной прочностью; демонстрируют целый спектр самых неожиданных электрических, магнитных, оптических свойств. Вообще-то нанотрубки можно использовать как микроскопические контейнеры для транспорта многих химически или биологически активных веществ: белков, ядовитых веществ, компонентов топлива и даже расплавленных металлов. Для нужд медицины нанотрубки обладают важным повышенным сродством к липидным структурам, они способны образовывать стабильные комплексы с пептидами и ДНК-олигонуклеотидами и даже инкапсулировать эти молекулы. Совокупность указанных свойств обуславливает их применение в виде эффективных систем доставки вакцин и генетического материала.

К **неорганическим наночастицам**, одному из важнейших классов наноперенощиков, относятся соединения оксида кремния, а также различных металлов (золото, серебро, платина). Часто такая наночастица имеет кремниевое ядро и внешнюю оболочку, сформированную атомами металла. Использование металлов позволяет создавать переносчики, обладающие рядом уникальных свойств. Так, их активность (и в частности высвобождение терапевтического агента) может быть модулирована термическим воздействием (инфракрасное излучение), а также изменением магнитного поля. В случае гетерогенных твердофазных композитов, например наночастиц металла на поверхности пористого носителя, вследствие их взаимодействия появляются новые свойства.

Наномедицина поднимает целый пласт социальных вопросов. По мнению экспертов группы по этике в науке и новых технологиях Европейской комиссии, при использовании наномедицины вопрос согласия пациента (врача) на основе полной информации очень сложен. Реально дать информацию о последствиях и оценке рисков в быстроразвивающейся области исследований на фоне многих неизвестных факторов чрезвычайно сложно.

Несмотря на огромный потенциал наномедицины и значительное финансирование, исследования этических, юридических и социальных значений применения наномедицины невелики. Как и с нанотехнологией вообще, есть опасность использования достижений наномедицины для преступных целей, если исследование этических, юридических и социальных аспектов критически отстанет от научного развития. Нехватка знаний о том, как наночастицы будут использоваться для регулирования жизненно важных процессов в человеческом организме, доставляет особое беспокойство. В недавней статье в *Medical Journal of Australia* говорится, что правила безопасности для нанопрепаратов могут потребовать уникальные оценки риска, учитывая новизну и разнообразие продуктов, высокую подвижность и реакционную способность проектируемых наночастиц. Обнаружено, что наночастицы полиамидоаминдендримеров (PAMAMs), используемые как агенты доставки лекарств, вызывают клеточные повреждения в тканях легких, результаты опубликованы в журнале *Journal of Molecular Cell Biology*. В серии экспериментов, проведенных в Китайской академии медицинских наук над мышами, обнаружено, что наночастицы PAMAMs запускают программу «клеточной смерти», известную как аутофагия. Руководители проекта сразу же призвали научное сообщество обратить особое внимание на безопасность использования нанотехнологий в медицине [12].

Наиболее широко используемым как в чистом виде, так и в составе наноматериалов является оксид титана (TiO_2). Токсикологические исследова-

ния ультратонких (20 нм) частиц TiO_2 при ингаляционном введении крысам показали, что частицы способны накапливаться в лимфоидных тканях, обладают повреждающим действием по отношению к ДНК лимфоцитов и клеток мозга. Основным механизмом токсического действия наночастиц TiO_2 оказалась индукция активных форм кислорода. Сильными токсическими свойствами обладают наночастицы алюминия, которые способны подавлять синтез м-РНК, вызывать пролиферацию клеток, индуцировать проатерогенное воспаление, нарушение функций митохондрий.

Эксперты указывают, что **область нанотехнологий могут счесть рискованной, опасной и сомнительной для инвестиций**, если при проведении исследований не будут учтены важные проблемы безопасности и здоровья людей. Наноматериалы, как правило, легче вступают в химические превращения, чем более крупные объекты того же состава, поэтому они способны образовывать комплексные соединения с не известными ранее свойствами. Наночастицы благодаря своим малым размерам легко проникают в организм человека и животных через защитные барьеры (эпителий, слизистые и т. д.), респираторную систему и желудочно-кишечный тракт. Абсорбирующие свойства наноэлементов значительно выше, чем у других молекул.

Один из ведущих экспертов в области здоровья и окружающей среды профессор Э. Ситон (Эдинбургский университет, Великобритания) считает, что наночастицы фармпродуктов могут вызвать у человека проблемы с органами дыхания, сердцем, иммунной системой и пр. Профессор Г. Обердерстер (Рочестерский университет, США) показал, что наночастицы углерода диаметром 35 нм способны проникать в мозг непосредственно по чувствительным нервным волокнам. Специалисты Национального аэрокосмического агентства США сообщают, что нанотрубки при вдыхании в большом количестве приводят к воспалению легких. Выявлено, что нанотрубка, представляющая собой соединение сверхтонких игл, имеет структуру, схожую с асбестом, а этот материал при вдыхании вызывает повреждение легких. Вдыхание наночастиц полистирола также вызывает воспаление легочной ткани и к тому же провоцирует тромбоз кровеносных сосудов. Есть сведения о том, что углеродные наночастицы могут вызывать расстройства сердечной деятельности и подавлять активность иммунной системы.

Кроме того, ученые обращают внимание на очень важный факт возможного **изменения свойств** наночастиц после их проникновения в организм, например покрытие белками при попадании в физиологические жидкости (кровь, плазма). В зависимости от свойств и концентрации использованных наночастиц при их проникновении в организм мы можем получить широкий спектр внутриклеточных изменений.

В заключение заметим, что подробнейшее изучение всех аспектов действия нанолекарств на жизненно важные системы человеческого организма представляет огромный интерес для специалистов в области военной химии. Напомним, что в ходе становления фармацевтической индустрии и получения классических лекарств были синтезированы многие отравляющие вещества и этот путь стоил человечеству немалых потерь. И если эти направления исследований смогут обеспечить создание новых видов химического оружия, то вряд ли существующие международные запреты смогут их остановить. Как неоднократно отмечалось во многих западных источниках, «еще не было в истории человечества государства, которое отказалось бы от возможности получить решающее преимущество под противником с помощью новых технологических достижений».

3. Меры по парированию угроз создания новых видов химического оружия

Принятие в 1993 г. Конвенции по запрещению химического оружия позволило сформировать более эффективную систему международного контроля за счет создания международного органа — Организации по запрещению химического оружия (ОЗХО), которая была создана в 1997 г.

За прошедшие годы членский состав ОЗХО расширился почти до 200 государств. Организация успешно выполняет задачи обеспечения контроля за соблюдением запрета химического оружия, ликвидации его запасов, уничтожения или конверсии бывших мощностей по его производству. В соответствии с Конвенцией в задачи ОЗХО входит

также содействие развитию международного сотрудничества в области мирной химии, помощь государствам в обеспечении защиты от химического оружия в случае его применения против них. Важнейшее направление деятельности ОЗХО — обеспечение нераспространения химического оружия. Для решения этой задачи ключевое значение имеет достижение универсальности Конвенции и осуществление контроля в химической промышленности, призванного исключить ее использование в целях, запрещенных по Конвенции. За успешное осуществление уничтожения химического оружия, накопленного в Сирийской Арабской Республике, ОЗХО присуждена Нобелевская премия мира.

В соответствии с Конвенцией Организация по запрещению химического оружия имеет три основных органа. Это Конференция — Главный орган ОЗХО государств-участников, Исполнительный совет и Технический секретариат.

В Конференцию государств-участников входят все члены Организации, она собирается один раз в год, а при необходимости и чаще. Конференция рассматривает любые вопросы в рамках сферы охвата Конвенции. Соответственно, она может давать рекомендации и принимать решения по любым вопросам, касающимся Конвенции. Конференция осуществляет надзор за осуществлением Конвенции, принимает меры для содействия реализации ее предмета и целей, а также рассматривает ее соблюдение. Конференция также осуществляет надзор за деятельностью Исполнительного совета и Технического секретариата. Один раз в пять лет Конференция собирается на специальную сессию для рассмотрения действия Конвенции.

Исполнительный совет ОЗХО является исполнительным органом Организации. Он подотчетен Конференции. Исполнительный совет действует в соответствии с решениями Конференции и обеспечивает их надлежащее выполнение. В задачу Исполнительного совета входят содействие эффективному осуществлению и соблюдению Конвенции, а также надзор за деятельностью Технического секретариата [13].

Технический секретариат является постоянно действующим органом. Он помогает Конференции и Исполнительному совету в выполнении их функций. Технический секретариат путем проведения инспекций осуществляет предусмотренные Конвенцией меры проверки ее соблюдения, получает и систематизирует первоначальные и ежегодные объявления государств-участников (информация о запасах химического оружия, о бывших объектах по его производству, их уничтожении и конверсии, о деятельности химической промышленности, о передачах химикатов и т. д.). Технический секретариат поддерживает постоянную связь с национальными органами государств-участников по выполнению Конвенции, оказывает им помощь в разработке национального законодательства, регулирующего выполнение Конвенции на национальном уровне.

Инспекторат является подразделением Технического секретариата. Он действует под надзором Генерального директора. В задачи инспектората входит проведение международных инспекций в государствах — участниках Конвенции с целью проверки ее соблюдения.

Технический секретариат ОЗХО осуществляет инспекционную деятельность в государствах-участниках. За подготовку, планирование и анализ результатов инспекций отвечает отдел проверки Технического секретариата. Непосредственно осуществляет инспекции отдел инспектората, укомплектованный квалифицированными инспекторами, проходящими регулярную специальную подготовку.

Большая часть инспекционной деятельности (около 60% инспекций) осуществляется на объектах, которые могут иметь отношение к химическому оружию. На объектах по уничтожению химического оружия (ОУХО) в период их функционирования обеспечивается постоянное присутствие инспекторов (на ротационной основе).

Одной из важнейших целей Конвенции является противодействие распространению химического оружия. В рамках деятельности на этом направлении, а также для обеспечения того, чтобы предприятия химической промышленности не использовались для целей, запрещенных по Конвенции, проводится инспектирование промышленных химических объектов.

Конвенция о запрещении химического оружия предусматривает возможность проведения инспекций по запросу. Инспекция по запросу может проводиться в любом государстве-участнике по запросу другого государства-участника без права от-

каза с целью прояснения или разрешения любого вопроса, касающегося возможного несоблюдения Конвенции. Запрашивающее инспекцию государство обязано ограничивать запрос на инспекцию рамками Конвенции и представлять в запросе всю соответствующую информацию, на основе которой возникла озабоченность.

Опыт, накопленный ОЗХО за эти годы, является залогом дальнейшего поступательного совершенствования ее деятельности с целью обеспечения эффективного контроля за соблюдением Конвенции и содействия развитию принципиально новых методов мониторинга за использованием высоких технологий в целях создания химического оружия.

Для преодоления трудностей, связанных с организацией контроля за использованием высоких технологий в целях создания химического оружия, представляется целесообразным российской делегации на очередной Конференции государств-участников в соответствии с п. 21h ст. VIII Конвенции включить вопрос о рассмотрении научно-технических достижений высоких технологий, которые могли бы сказаться на действии настоящей Конвенции. Одновременно представляется целесообразным рекомендовать Генеральному директору ОЗХО учредить Научно-консультативный совет, состоящий из независимых экспертов, который бы мог подготовить квалифицированные предложения по созданию международной системы контроля за использованием высоких технологий в целях создания химического оружия. Эти предложения должны быть направлены на решение трех основных проблем:

- формирование достоверного режима контроля и учета всех имеющихся в мире лабораторий, в которых могут вестись работы по созданию особо опасных химических веществ нового поколения;
- обеспечение необходимого уровня физической защиты объектов, на которых производятся работы по созданию средств защиты от особо опасных химических веществ нового поколения;
- создание условий для эффективного экспортного контроля за перемещением продукции высоких технологий, пригодных для производства опасных химических веществ.

Необходимо также оценить защитные характеристики существующих СИЗ от нового поколения отравляющих веществ, включая наночастицы различного характера. Исследования по определению защитных свойств современных СИЗ целесообразно провести от всех возможных видов новых отравляющих веществ.

Необходимо отметить, что в условиях террористических актов реально обеспечить защиту человека в момент внезапно возникшей опасности может только средство защиты, которое находится в пределах его досягаемости. Любое защитное устройство, недоступное пользователю в момент ЧС, является практически бесполезным. Таким образом, важным требованием, предъявляемым к данному типу СИЗ, является **требование портативности.**

Создание высокоэффективных СИЗ, отвечающих современным требованиям, невозможно без использования современных материалов и оборудования, а также инновационных технологий. Имеющиеся отечественные серийные сорбенты и катализаторы для средств защиты по своим поглотительным способностям уступают лучшим импортным образцам. В результате существенное снижение массогабаритных характеристик СИЗ весьма затруднительно. На ряде предприятий России имеются перспективные научные разработки по высокоэффективным фильтрующим материалам, адсорбентам, катализаторам и поглотителям, принципиально новым конструктивным и технологическим решениям [14].

Наряду с этим необходимо также предусмотреть выполнение научно-исследовательских работ, направленных на создание:

- эффективных средств защиты от нетрадиционных отравляющих веществ;
- достоверных средств химико-аналитического контроля, обеспечивающих экспресс-обнаружение химических агентов нового поколения;
- высокопроизводительных технологий дегазации объектов, подвергшихся атаке с помощью новых видов химического оружия.

Заключение

Приведенные в настоящей статье материалы позволяют сделать вывод о том, что многие современные технологии могут быть использованы для создания новых видов химического оружия. Полученные знания от развития таких высоких технологий, как

биотехнологии и нанотехнологии, могут предложить принципиально новые направления поиска высокотоксичных отравляющих веществ, характеристики которых очень трудно предсказать. Это необходимо учитывать при планировании деятельности по дальнейшему совершенствованию форм и способов защиты населения от новых видов угроз химического характера.

Во-первых, необходимо на уровне Организации по запрещению химического оружия инициировать предложение по созданию международной системы контроля за использованием высоких технологий в целях получения высокотоксичных веществ.

Во-вторых, необходимо продолжить работы по созданию более совершенных и универсальных средств индивидуальной защиты от всех возможных видов химического оружия. На ряде предприятий России имеются перспективные научные разработки по созданию высокоэффективных средств защиты по принципиально новым конструктивным и технологическим решениям. Однако эти работы не доходят до стадии промышленного производства. Основная причина — отсутствие эффективной научно-технической политики при распределении финансовых средств на наиболее перспективные разработки. При осуществлении заказов на разработку перспективных средств защиты необходимо обеспечить тесное межведомственное взаимодействие федеральных органов исполнительной власти и привлечение к формированию заказов экспертного сообщества, включая ученых РАН. Целесообразно также направить усилия на создание интегрированных научно-производственных структур, объединяющих разработчиков и производителей средств защиты населения от воздействия опасных химических веществ любого характера с целью концентрации финансовых, материальных и интеллектуальных ресурсов для решения задач по созданию наиболее эффективных образцов.

Литература

1. Шкодич П.Е., Желтобрюхов В.Ф., Клаучек В.В. Эколого-гигиенические аспекты проблемы уничтожения оружия. Волгоград: ВолГУ, 2004.
2. Антонов Н.С. Химическое оружие на рубеже двух столетий. М.: Прогресс, 1994.
3. Малышев В.П. Трансгенные продукты: возможные риски и пути их снижения // Проблемы анализа риска. 2006, Т. 3, № 3.
4. Clive James. Global Status of Commerzialized Biotech/GM Crops, 2004, Report JSAAA. 2004.
5. Lang D.G., Hollman U.K. Rish Analysis, N 25 No 4, 2005.
6. Материалы Воронежской конференции по нанотехнологиям. 2014.
7. Тутельян В.А. и др. Отчет Института питания РАМН. М., 1998.
8. Кузнецов В.В., Куликов А.М. Российский химический журнал. 2005, Т. XLIX, № 4.
9. Global Treaty Adopted on Genetically Modified Organisms. UNEP, Nairobi. 2000.
10. Артюхов И.В., Кеменов В.Н., Нестеров С.Б. Биомедицинские технологии. Обзор состояния и направления работы. Материалы 9-й научно-технической конференции «Вакуумная наука и техника». М.: МИЭМ, 2012.
11. Лен Ж.-М. Супрамолекулярная химия: концепции и перспективы. Новосибирск: Наука, 1998.
12. Нестеров С.Б. Нанотехнология. Современное состояние и перспективы. Новые информационные технологии. Тезисы докладов XII Международной студенческой школы-семинара. М.: МГИЭМ, 2014.
13. Конвенция о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении. 1994.
14. Батырев В.В. Химическая защита населения в чрезвычайных ситуациях мирного и военного времени. Основные проблемы и пути их решения. Материалы VIII Научно-практической конференции по совершенствованию гражданской обороны Российской Федерации. М.: МЧС России, 2011.

Сведения об авторе

Малышев Владлен Платонович: доктор химических наук, профессор, заслуженный деятель Российской Федерации, главный научный сотрудник ФКУ ЦСИ ГЗ МЧС России

Число публикаций: 350

Область научных интересов: радиационная, химическая и биологическая безопасность

Контактная информация:

Адрес: 121352, г. Москва ул. Давыдковская, д. 7

Тел.: +7 (495) 400-99-52

E-mail: csi430@mail.ru

Издательский дом
ДЕЛОВОЙ ЭКСПРЕСС

От идеи до готового тиража

КАЛЕНДАРИ
БУКЛЕТЫ
ОТКРЫТКИ

ГОДОВЫЕ
ОТЧЕТЫ

КОРПОРАТИВНЫЕ
ЖУРНАЛЫ

АЙДЕНТИКА

В нашей работе мы много внимания уделяем развитию дизайна, как креативной, видимой, его стороне, так и процессам, которые клиенту не видны. При этом особый упор мы делаем именно на технологическую и психологическую составляющие дизайна. Продуманность, неслучайность, технологический контроль и забота о конечном потребителе дизайна, следование тенденциям и опережение мировых трендов – то, что мы предлагаем нашим клиентам в первую очередь.

125167, Москва
Тел. +7 (495) 787-52-26
4-я улица 8 Марта, д. 6А

УДК 338.24, 30.4

ISSN 1812-5220

Новые задачи и Предметный указатель в экономике

Е. Д. Соложенцев,
Институт проблем машиноведения РАН, г. Санкт-Петербург

Аннотация

В настоящей статье разработан Предметный указатель научной дисциплины «Топ-экономика. Управление социально-экономической безопасностью» и приводится список новых задач в экономике. Использована книга автора «Топ-экономика. Управление экономической безопасностью». В западных редакциях не принимают к публикации книги без предметного указателя, в российских же книгах по экономике предметный указатель обычно отсутствует. Это свидетельствует о небольшом количестве новых понятий и результатов в книгах и непонимании роли предметного указателя для структуризации и усвоения знаний.

Ключевые слова: предметный указатель, социально-экономическая безопасность, логико-вероятностные модели, риск, анализ, управление, социально-экономические системы, топ-экономика, невалидность, новые задачи, экономическая теория.

Содержание

Введение

Указатель — это справочный текст, который выглядит как список ключевых слов и страниц, где они упомянуты. Указатель помогает найти нужный фрагмент книги. Он является частью книги и входит в научный аппарат книги (Википедия). Указатель можно рассматривать как базу знаний о научной дисциплине.

О технологии, качестве и культуре публикаций за рубежом свидетельствует, например, специальный выпуск журнала International Journal of Risk assessment and management (IJ RAM) [1]. Десяток статей разных авторов имеют единый список предметных индексов, сделанный самой редакцией с помощью специальных программ.

Монография «Топ-экономика. Управление экономической безопасностью» [2] включает в себя введение, четыре главы, заключение, список литературы и предметный указатель. Рецензентами книги являются известные в России и на Западе ученые: доктор физико-математических наук, профессор, лауреат Государственной премии Польши *В. П. Одинец,* доктор физико-математических наук, профессор кафедры экономической кибернетики Санкт-Петербургского государственного университета *Н. В. Хованов* и доктор экономических наук, декан экономического факультета Санкт-Петербургского

государственного университета аэрокосмического приборостроения *А. С. Будагов.*

Монография, имеющая 272 с., количество таблиц — 46, рисунков — 44, формул — 151 и библиографический список из 88 наименований, посвящена новой научной дисциплине «Топ-экономика: управление социально-экономической безопасностью социально-экономических систем» на основе логико-вероятностных (ЛВ) моделей риска. Даны определения невалидности в экономике по аналогии с надежностью в технике. Названы особенности и рассмотрены компоненты топ-экономики: методы, модели, технологии, задачи, объекты и специальные software.

Введены новые типы булевых событий-высказываний в экономике: о неуспехе объектов и субъектов, о невалидности, концептуальные события-высказывания, индикативные события-высказывания, события-высказывания о латентности, несовместные события-высказывания и др.

Введены новые типы ЛВ-моделей риска в экономике: гибридные ЛВ-модели неуспеха в управлении социально-экономическими системами, ЛВ-модели невалидности, концептуальные ЛВ-модели прогнозирования, индикативные ЛВ-модели опасности. Все эти новые типы ЛВ-моделей могут быть использованы для одной СЭС для всестороннего анализа и управления социально-экономической безопасностью.

Объекты исследования топ-экономики — социально-экономические системы: СЭС-1 — наивысшей важности для государства, предназначенные для уменьшения потерь средств и увеличения их поступления; СЭС-2 — комплексные, зависящие от нескольких министерств и ведомств; СЭС-3 — локальные для предприятий. Рассмотрены задачи топ-экономики: построение ЛВ-моделей; ЛВ-анализ; ЛВ-прогнозирование и ЛВ-управление риском СЭС.

Примеры приложений топ-экономики: управление системой инноваций, противодействие коррупции и наркотизации населения, управление операционным риском и резервированием капитала банка по Базель, управление качеством систем и продукции по ВТО, управление процессом кредитования банка. В экономической безопасности страны решаются задачи моделирования риска, анализа и управления риском и экономическими войнами с санкциями. На примерах показано: 1) без ученых и общественного мнения проблемы СЭС страны не решаются; 2) создание СЭС первостепенной важности невозможно без реформ в образовании, науке и экономике; 3) для развития топ-экономики необходима сертификация созданных специальных software.

Книга адресована экономистам и менеджерам, занимающимся проблемами управления экономической безопасностью СЭС, студентам, аспирантам и преподавателям вузов экономических специальностей.

1. Необходимость предметного указателя

Особое внимание в работе уделено разработке предметного указателя как некоторой базы знаний научной дисциплины.

В российских книгах по экономике предметный указатель обычно отсутствует. Это свидетельствует о небольшом количестве новых понятий, результатов и непонимании значения указателя для усвоения и структуризации знаний по предмету исследования. Западные издательства не принимают к печати книги без списка индексов. В то же время такие российские книги: В. И. Рачков. Основы теории опасных систем. М.: Наука, 2015. 165 с.; Владимир Масликов. Универсум; Общая теория управления. М.: Алгоритм, 2015. 688 с. и многие другие, имеющие звучные названия и большие объемы, изданы без предметного указателя.

Проблема создания предметного указателя и редакторы текстов связаны. Экономические редакции, российские и некоторые западные, обязывают предоставлять рукописи книг для публикации, подготовленные в редакторе Word. Книги отличаются большим однообразием с изложением «рассказов» по экономике и иллюстрациями временных рядов различных показателей в экономике страны и региональной экономике, которые, по мнению авторов, позволяют принимать решения.

Для публикации книг и статей по математике, механике и другим точным наукам редакции обязывают представлять материалы, подготовленные в редакторе LaTex. Публикации в редакторе LaTex отличаются большим разнообразием используемых

средств: стилевых файлов, автоматизированного учета ссылок, формул, таблиц и рисунков, размещения и размеров таблиц и рисунков. Каждый раздел располагается на новой правой странице, что удобно для продажи электронного текста раздела отдельным клиентам. Главное же для рассматриваемой проблемы заключается в простоте создания списка предметного указателя.

Список предметного указателя названной выше монографии [2] является обширным и выразительным. Выделено 26 разделов, в которых названы 145 указателей.

2. Новые задачи в экономике и экономической теории

Экономическая наука еще далека от совершенства и нуждается в развитии. Об этом свидетельствуют неудачи компаний, неуспехи экономики стран и многие нерешенные проблемы в экономической науке.

Назовем нерешенные проблемы в экономической науке из-за отсутствия или некорректности следующих математических моделей состояния систем: связи экономики, политики, государства, науки и общества; учета событий-высказываний от деятелей государства, бизнеса, науки, общества об изменениях законов, ситуации на рынке, появлении инноваций и др.; связи разных социально-экономических систем (СЭС); перехода от любых баз данных к базам знаний для принятия решений; использования невалидности в экономике, имеющей много значений (multi-state), как отказа в технике; методики построения модели риска системы по параметрам одного ее состояния; модели невалидные, концептуальные, индикативные и гибридные для всесторонней оценки экономической системы; интеграция моделей логическими операциями *AND, OR, NOT*; учебного курса «Управление социально-экономической безопасностью» для экономических кафедр. Экономические кафедры (созданные на базе кафедр бухучета и аудита) и научные институты с названием «Экономическая безопасность» не занимаются управлением безопасностью.

Назовем нерешенные проблемы в экономической науке из-за отсутствия или некорректности следующих математических моделей управления: принятие решений в основном «по понятиям» и осуществление «ручного» управления; управление операционным риском банков и резервированием капитала по Базель; управление качеством систем и продукции по ВТО; управление процессом кредитования в банках; управление экономическими войнами на основе санкций; управление реформами в образовании, науке и экономике; управление участием общественного мнения и ученых в решении социально-экономических проблем; развитие систем как сложных объектов с движением по программной траектории и коррекцией при отклонении от нее; управление стратегией развития страны и регионов на основе корректировки моделей по информации об изменениях в экономике, политике, праве и инновациях.

Эффективность ЛВ-управления рассматривается на примере управления безопасностью СЭС страны. Управление социально-экономической безопасностью усложняют следующие особенности: управление имеет комплексный характер, так как зависит от нескольких министерств, ведомств и органов по правам; отсутствует унифицированная система моделей, методов, задач, технологий и специальных software для управления социально-экономической безопасностью. Множества и ЛВ-модели, по мнению ряда ученых, являются самыми простыми и прозрачными разделами математики. Социально-экономической безопасностью следует управлять на основе математических моделей, а не «по понятиям», которые часто бывают ошибочными.

Анализ нерешенных проблем в экономической науке показал, что необходима новая экономическая дисциплина «Управление социально-экономической безопасностью». На разработку новой научной дисциплины оказали влияние известные ученые: Дж. Буль, предложивший логическое исчисление высказываний; П. Порецкий, установивший связь логики с теорией вероятностей; И. Рябинин, создавший теорию ЛВ-анализа надежности в технике; лауреаты Нобелевской премии Дж. Бьюкенен и Дж. Хекман, исследовавшие связь экономики, политики и государства на основе теории игр и анализа статистических данных; Н. Винер и Дж. фон Нейман, считавшие, что математические методы для управления экономическими и социальными системами должны основываться на логике, теории вероятностей, множествах и комбинаторике; А. Эйн-

штейн, считавший, что никакую проблему нельзя решить на том же уровне, на котором она возникла.

В работе [2] определяется невалидность параметров и системы как отклонение от заданных значений, вводятся новые типы булевых событий-высказываний и новые типы логико-вероятностных моделей риска для управления социально-экономической безопасностью. Используется событийный подход к моделированию риска систем и решению задач анализа, прогнозирования и управления риском. Для социально-экономической системы последовательно строят сценарную, структурную, логическую и вероятностную модели риска. В технологии управления безопасностью СЭС центральное место занимают процедуры: ортогонализация логической функции риска, оценка невалидности инициирующих событий и ЛВ-анализ риска системы по вкладам событий.

Новая экономическая дисциплина влияет на развитие теории надежности и безопасности в технике: вводит для состояний элементов системы не два значения (отказ и неотказ), а несколько (multi-state) значений и динамичность ЛВ-модели риска [3, 4].

Новая экономическая дисциплина «Управление социально-экономической безопасностью» представляет собой унифицированный комплекс моделей, методов, знаний, технологий и software, базой которого служат ЛВ-модели риска и ЛВ-исчисление. Научная и практическая значимость дисциплины определяется тем, что в ней решаются названные выше нерешенные проблемы в экономической науке.

Эффективность экономики повысится, если наряду с задачами микро- и макроэкономики решать задачи управления социально-экономической безопасностью.

3. Разделы Предметного указателя

Ниже приведены разделы Предметного указателя с указанием в скобках числа указателей в каждом.

1. Анализ риска в социально-экономических системах (6 указателей).
2. Булевы события-высказывания в управлении экономикой (8).
3. Динамичность ЛВ-моделей риска (5).
4. Достоинства и особенности топ-экономики (12).
5. Классы ЛВ-моделей риска (5).
6. Компоненты топ-экономики (7).
7. Модели топ-экономики (4).
8. Мониторинг и управление процессом кредитования банка (4).
9. Невалидность (4).
10. Объекты в топ-экономике (3).
11. Операционный риск банка и резервирования капитала по Базель (3).
12. Примеры СЭС-приложений топ-экономики (10).
13. Противодействие взяткам и коррупции (4).
14. Противодействие наркотизации страны (3).
15. Процедуры технологии для классов (6).
16. СЭС-1 наивысшей важности для страны (6).
17. Свойства топ-экономики (12).
18. Синтез вероятностей событий для ЛВ-моделей риска (3).
19. Специальные software (10).
20. Состояние топ-экономики (6).
21. Технологии управления риском (4).
22. Топ-экономика (3).
23. Управление качеством систем по ВТО (2).
24. Управление риском в СЭС (4).
25. Управление риском системы инноваций страны (4).
26. Управление риском экономического состояния России (5).

4. Предметный указатель

Разделы предметного указателя и сами указатели составлены для удобства в алфавитном порядке. Предметный указатель рассматриваемой научной дисциплины следующий:

Анализ риска в социально-экономических системах (СЭС):

вклады в левом и правом «хвостах» распределения,
вклады событий на плюс и на минус,
экономические войны с санкциями,
опасные события и их комбинации,
структурная и вероятностная значимость событий,
частотный анализ событий.

Булевы события-высказывания в управлении экономикой:

индикативные события,
концептуальные события,
латентные события,
невалидные события,

Заключение

В статье приведен список новых задач в экономике и экономической науке и разработан Предметный указатель научной дисциплины «Топ-экономика. Управление социально-экономической безопасностью».

Топ-экономика имеет унифицированную систему моделей, методов, технологий и software для управления социально-экономической безопасностью СЭС различной сложности. Для обозначения этой унифицированной системы знаний и методов, базой которых служат ЛВ-модели риска и ЛВ-исчисление, предлагается название «топ-экономика». Топ-экономика имеет свои методы, модели, технологии, объекты, задачи и специальные software. В ней рассмотрены задачи управления экономической безопасностью, которые не решаются в макроэкономике и микроэкономике [2, 3].

Нобелевские лауреаты Дж. Бьюкенен и Дж. Хекман исследовали связь экономики и политики в развитии государства на основе теории игр и анализа статистических данных. В развитии их работ предлагается новый подход к анализу и управлению экономической безопасностью на основе топ-экономики. Топ-экономика рассматривает связь экономики, политики, бизнеса, науки и общества в широком аспекте. Учитываются инициирующие события, зависящие от решений правительства и принятых законов, вероятности государства, бизнеса, ученых и общества решить проблему СЭС, сигнальные события об изменениях в экономике, политике, праве, инновациях, на мировом рынке для коррекции вероятностей инициирующих событий в ЛВ-модели риска.

Оглавление книги, тексты разделов, Предметный указатель и Список нерешенных проблем в экономической теории в целом дают полное представление о проблеме управления социально-экономической безопасностью социально-экономических систем и способствуют структуризации знаний и их усвоению по научной дисциплине «Топ-экономика. Управление социально-экономической безопасностью».

Литература

1. International Journal of Risk Assessment and Management. Special issue “Risk managemen technologies in structure complex systems” / Edited by E.D. Solozhentsev. 2015. T. 18. Nos 3\4.
2. Соложенцев Е.Д. Топ-экономика. Управление экономической безопасностью. 2-е изд. СПб.: Троицкий мост, 2016. 272 с.
3. Solozhentsev E.D. Risk Management Technologies with Logic and Probabilistic Models. Dordrecht, Heidelberg, New York, London: Springer, 2012. 328 p.
4. Соложенцев Е.Д. Невалидность и события-высказывания в логико-вероятностных моделях для управления риском в социально-экономических системах // Проблемы анализа риска. 2015. Т. 12. № 6. С. 30—43.

Сведения об авторе

Соложенцев Евгений Дмитриевич: заслуженный деятель науки РФ, доктор технических наук, заведующий лабораторией Интегрированных систем автоматизированного проектирования (ИСАПР) Института проблем машиноведения Российской академии наук (ИПМаш РАН), профессор кафедры «Бизнес-информатика» Государственного университета аэрокосмического приборостроения (ГУАП), Председатель Организационного и Программного комитетов Международных научных школ «Моделирование и анализ безопасности и риска в сложных системах» (2001—2016, Санкт-Петербург), приглашенный редактор специальных выпусков журналов «Проблемы анализа риска» и “International Journal of Risk and Analysis Management”.
Количество публикаций: более 300, из них 5 книг на русском и 3 книги на английском языке
Область научных интересов: моделирование, анализ и управление риском и эффективностью на стадиях проектирования, испытаний и эксплуатации социально-экономических и технических систем
Контактная информация:
Адрес: 199178, г. Санкт-Петербург, Большой пр., д. 61, В. О.
Тел.: +7 (812) 321-47-66
E-mail: esokar@gmail.com

Аннотации статей на английском языке

A NEW TYPE OF RISKS: CYBER RISKS

Yu. I. Sokolov, VNII GOCHS Emercom of Russia, Scientific Research Center 6, Moscow

Annotation. The article discusses the risks of using cyberspace when automating control of industrial facilities, critical facilities, in the work of management and governance bodies, and the issues of ciber security.

Keywords: the Internet, cyberspace, the automated control systems of technological process, information and communication technologies, key systems of information infrastructure, computer viruses, hacker, cyber threats, cyber attacks, cyberwar, cybersecurity.

RISKS OF BREXIT

O. V. Khmyz, Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation

Annotation. The paper analyzes already arrived and potential consequences of the historic decision to exit Britain from the European Union, leading to the emergence and escalation of national, regional and global risks.

Keywords: risk, Brexit, United Kingdom, European Union, Germany, London, Frankfurt, financial risk, currency risk, interest rate risk, capital markets, exchange rates, financial markets, budget, pound, dollar, euro

INDEX-BASED APPROACH TO COUNTRY RISK ASSESMENT FOR INVESTMENTS

I. V. Demkin, D. A. Vlasov, A. O. Gabrielov, V. D. Barkhatov, NIIgazeconomika plc., Moscow,

N. V. Lukyanovich, Financial University under the Government of the Russian Federation, Moscow

Annotation. Globalization of the world economy is forcing companies to enter international markets by implementing investment projects and competing for scarce resources and markets in foreign countries. Companies are faced with the need to assess country risk in order to select attractive countries for investment with an acceptable level of risk. This work is devoted to development approach to the qualitative assessment of country risk.

Keywords: risk assessment, country risk, country development indices, credit ratings.

RISK MANAGEMENT INFORMATION DISCLOSURE IN NON-FINANCIAL ANNUAL REPORTS OF RUSSIAN OIL AND GAS COMPANIES THAT HAVE PROJECTS IN THE ARCTIC

S. N. Bobylev, S. M. Niconorov, A. V. Kornilova, Lomonosov Moscow State University

Annotation. The subject of this research is the system of risk management of Russian oil and gas companies that have resource exploration projects in the Russian Arctic. The study analyses risk management practices of such companies as Gazprom Neft, Lukoil, Rosneft, Zarubezhneft, Surgutneftegaz and Novatek. The main aim of this research is analyzing the risk management system, that includes environmental and social risk management, based on the information that is disclosed in the annual non-financial reports. Comparative analysis of the reported information is based on the authors' methodology for assessing the quality of the information disclosure within the limits of key risk management information indicators identified by the authors. This study examines the information provided by companies in their 2014 annual reports. The main results of the research are presented by determination of the leaders in the field of risk management among the surveyed companies. The practical significance of the study is determined by the ability to use the established methodology for assessing the risk management information disclosed in the annual reports of companies from other sectors of the economy and companies from other countries. This study is part of a larger research that is aimed at analyzing the system of environmental and social responsibility of Russian oil and gas companies that have their projects in the Arctic.

Keywords: risk management, social risks, environmental risks, Arctic, non-financial reporting

RISKS IDENTIFICATION IN INTERNATIONAL FREIGHT FORWARDING ACTIVITY

E.V. Zenina, Plekhanov Russian University of Economics, Moscow

T.T. Zenina, Saint-Petersburg State University of Economics

Annotation. The article discusses main risks of freight forwarding activities. A failure in one of the links of the logistics chain automatically increases the likelihood of the risk occurrence throughout the chain, so there is a need to build a supply chain based on the assessment of the sustainability of each link, understanding the probability of occurrence of risks in different operations.

Keywords: forwarding company, forwarding services, risk management.

POSSIBLE PROSPECTS OF NEW FORMS OF CHEMICAL WEAPON CREATION AND MEASURES TO REDUCE HAZARDS OF THEIR APPLICATION

V. P. Malyshev, FKU CSI GZ MChS of Russia, Moscow

Annotation. The article considers possible prospects of new forms of chemical weapon creation and proposes the activity directions allowing to reduce hazards of their application. To create new forms of chemical weapon might be used achievements in the field of biotechnology and nanotechnology.

Keywords: chemical weapons, toxic agents, biotechnology, nanotechnology, international control, means and protection methods from chemical weapon.

NEW PROBLEMS AND SUBJECT INDEX IN ECONOMICS

E D. Solozhentsev, Institute of Problems of Mechanical Engineering of RAS, Intelligent Integrated Systems of Automated Designing Laboratory, Saint Petersburg

Annotation. In this paper we develop and describe the Subject index and new problems of the discipline "Top economics. Management of socioeconomic safety" and List of unsolved problems in the theory of economy. We used the author's book "Top-economy. Economic Safety Management». Western publishing houses do not accept books for publishing without subject index. Russian books on Economics have not usually subject index. This shows about a small amount of new concepts and the results in books and the lack of understanding of the role of the index for structuring and learning of knowledge.

Keywords: index, socioeconomic safety, logical and probabilistic models, risk, analysis, management, socioeconomic system, the top-economics, invalidity, new problems, economic theory.

Инструкция для авторов

1. Общие требования к представлению статьи. Журнал «Проблемы анализа риска» публикует междисциплинарные научные и прикладные материалы, посвященные анализу рисков различного происхождения и характера: техногенного, природного, социально-экономического, финансового, экологического и др.

Представляемая в редакцию статья должна соответствовать тематике журнала, быть написана на русском языке (титульный лист представляется на русском и английском языке), быть оригинальной, ранее не опубликованной и не представленной к публикации в другом издании.

Авторы несут ответственность за достоверность приведенных сведений, отсутствие данных, не подлежащих открытой публикации, и точность информации по цитируемой литературе.

Все представленные в редакцию журнала рукописи авторам не возвращаются.

2. Порядок представления рукописи. Первоначальное представление статьи в редакцию журнала осуществляется в электронном виде одним из следующих способов: с помощью электронной почты на e-mail journal@dex.ru; на CD-диске по почте; непосредственно в редакцию журнала на любом электронном носителе.

В наименовании электронного файла должны быть указаны: первый автор статьи, сокращенное название статьи, дата представления (например, «Иванов_Стандарты финансового РМ_120111»). На обложке CD-диска или в теме сообщения, посланного на электронный ящик редакции, должно быть указано наименование файла статьи.

Статья будет направлена на рецензирование одному или двум экспертам. Возможно, потребуется доработка или переработка статьи по результатам рецензирования до принятия решения о ее опубликовании.

После принятия решения об опубликовании статьи авторы должны представить в редакцию окончательный подписанный вариант рукописи, на бумажном носителе, а также электронную версию статьи и свою фотографию, приложив их к рукописи на CD-диске или передав на электронный почтовый ящик редакции (par@dex.ru, journal@dex.ru). Редакция оставляет за собой право дальнейшей редакционной и корректорской правки статьи. Корректура автору в обязательном порядке не высылается, с ней можно ознакомиться в редакции.

Если статья не принимается к печати, автору высылается отказ по электронной почте.

3. Лицензионный договор. Если принято решение об опубликовании статьи, в соответствии с требованиями Гражданского кодекса РФ между авторами и журналом заключается лицензионный договор с приложением к нему акта приема-передачи произведения. С лицензионным договором и актом приема-передачи произведения можно ознакомиться на сайте www.dex.ru в разделе «Инструкция для авторов». Данные документы, подписанные со стороны авторов, должны быть переданы в редакцию вместе с окончательным подписанным вариантом рукописи.

4. Общие требования к рукописи. Электронный файл рукописи должен быть сформирован с использованием стандартных пакетов редакторских программ (например, MS Word, WordPad).

Формат страниц: А4, рекомендуемые отступы от краев листа: сверху и снизу — 3 см, слева и справа — 2 см, рекомендуемый шрифт Times New Roman, 12 пт, междустрочный интервал — одинарный или полуторный. Страницы должны быть пронумерованы.

Файл со статьей должен содержать:

1) титульный лист (на русском и английском языке),

2) текст статьи (введение, структурированные разделы статьи, заключение),

3) литературу (последовательный перечень цитируемой литературы),

4) сведения об авторах.

5. Титульный лист. Представляется на русском и английском языках и должен включать: УДК, краткое информативно-смысловое название, инициалы, фамилию, краткое (по возможности) наименование организации (при указании организации не допускается приводить только аббревиатуру). Располагается после фамилии автора, город, аннотацию: должна быть краткой (не более 200 слов), информативной и отражать основные положения и выводы представляемой к публикации статьи, ключевые слова (не более 15) должны способствовать индексации и классификации, содержание: включает заголовки первого уровня разделов, использование ссылок и указание страниц не допускается.

6. Текст статьи. Основной текст статьи должен содержать: введение, структурированные, пронумерованные разделы статьи, заключение, литература.

Введение должно содержать четкое обозначение целей и задач работы. В нем могут даваться ссылки на ключевые работы в области исследования, но введение не должно быть литературным или историческим обзором.

Структурированные разделы статьи должны содержать четкое и последовательное изложение материала работы. Заголовки разделов основной части должны иметь нумерацию (1, 2, 3 и т. д.), эта же нумерация должна быть отражена в содержании (разделы введение, заключение, литература, сведения об авторах не нумеруются). Допускается в каждом разделе создавать подзаголовки разделов.

Заключение должно включать основные выводы, обсуждение спорных моментов, значимость теоретических положений, их ограничения; место и роль в разрезе предыдущих исследований, возможностей практических приложений.

7. Требования к таблицам, рисункам и формулам

Таблицы и рисунки рекомендуется располагать внутри текста после первого указания на них. Размер таблиц и рисунков не должен выходить за рамки формата текста. Все таблицы и рисунки должны быть последовательно пронумерованы и иметь краткое название (название таблиц дается над таблицей, рисунков — под ними).

Таблицы и рисунки должны быть понятными безотносительно к объяснению в тексте. Пояснения к таблицам и рисункам должны быть краткими. Пояснения к таблицам должны располагаться внизу таблицы и иметь указатели с использованием надстрочной буквенной или цифровой индексации (меньшего размера относительно текста). Пояснения к рисункам должны располагаться под названием рисунков с использованием шрифта меньшего размера относительно текста названия рисунков.

Таблицы представляются в стандартном редакторе MS Office, например MS Word или MS Excel.

Рисунки должны быть высокого качества. Графики должны предоставляться преимущественно в формате MS Excel. Схемы и карты предоставляются в векторных форматах EPS, CDR. Фотографии и другие иллюстративные материалы, предоставляемые в виде растровых изображений, должны иметь разрешение 300 dpi (при размере на формат издания) и быть в форматах TIFF или JPEG (без сжатия). На растровых рисунках должны хорошо прочитываться текст и все значимые элементы.

Формулы отдельно стоящие формулы должны быть набраны с использованием стандартных средств MathType или Equation.

Переменные величины и элементы формул, располагаемые внутри текста, набираются по возможности с использованием текстовых выделений (нижний, верхний регистры, курсив, греческие буквы и т. д.)

Формулы и буквенные обозначения должны быть тщательно выверены автором, который несет за них полную ответственность.

8. Литература. Библиографические ссылки в статье рекомендуется осуществлять как затекстовые ссылки и обозначать номерами в порядке цитирования в квадратных скобках, например [1] или [2—5], при необходимости с указанием страниц. Ссылки на неопубликованные работы недопустимы. Список литературы должен размещаться в конце статьи и составляется в соответствии с ГОСТ Р 7.0.5-2008 «Библиографическая ссылка».

Порядок составления списка следующий: для книг: фамилия и инициалы автора (авторов), полное название, место и год издания, издательство, общее количество страниц; для глав в книгах и статей в сборниках: фамилия и инициалы автора (авторов), полное название статьи, полное название книги, фамилия и инициалы редактора (редакторов), место и год издания, издательство, номера первой и последней страниц; для журнальных статей: фамилия и инициалы автора (авторов), полное название статьи, название журнала, том издания, номер, номера первой и последней страниц. Если число авторов больше трех, вначале пишется название статьи, затем все авторы и далее название журнала, том издания, номер, номера первой и последней страниц; для диссертаций: фамилия и инициалы автора, докторская или кандидатская, полное название работы, год и место издания.

Ссылки на литературу в статьях, представленных для публикации зарубежными авторами, могут производиться с использованием международного стандарта.

Авторы самостоятельно несут ответственность за точность информации по цитируемой литературе.

9. Сведения об авторах. Сведения об авторах должны включать: фамилию, имя и отчество (полностью), степень, звание и занимаемую должность, полное и краткое наименование организации, число публикаций, в том числе монографий, учебных изданий, область научных интересов, контактную информацию: почтовый адрес, телефон, факс, e-mail.

Учредители:
- Общероссийская общественная организация «Российское научное общество анализа риска»
- ФГБУ «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (ФЦ)
- Финансовый издательский дом «Деловой экспресс»

Журнал внесен в перечень ведущих рецензируемых научных журналов и изданий, рекомендованных Высшей аттестационной комиссией Минобрнауки России (ВАК) для опубликования основных научных результатов диссертаций на соискание ученых степеней доктора и кандидата наук

Плата с аспирантов за публикацию рукописей не взимается

Присланные в редакцию материалы рецензируются и не возвращаются

Статьи, не оформленные в соответствии с Инструкцией для авторов, к рассмотрению не принимаются

Ответственность за достоверность фактов, изложенных в материалах номера, несут их авторы

Мнение членов редколлегии и редсовета может не совпадать с точкой зрения авторов

Редакция не имеет возможности вести переписку с читателями (не считая ответов в виде журнальных публикаций)

Журнал издается с 2004 года. Периодичность: 1 раз в 2 месяца

Свидетельство о регистрации средства массовой информации ПИ № ФС 77-61704 от 25.05.2015

Формат 60 × 84 1/8. Объем 12 печ. л. Печать офсетная.
Тираж 1000 экз. Подписано в печать 22.12.2016.

Редакция:
Главный редактор
Быков Андрей Александрович
E-mail: journal@dex.ru, par@dex.ru

Ответственный секретарь
Виноградова Лилия Владимировна
E-mail: journal@dex.ru

Отдел подписки
Тел.: +7 (495) 787-52-26
E-mail: journal@dex.ru

Верстка:
Луговой Александр Вячеславович,
Лебедева Наталья Сергеевна,
Столбова Марина Сергеевна

Корректура:
Легостаева Инна Леонидовна,
Таборская Людмила Вильгельмовна,
Шольчева Янина Геннадьевна

Дизайн: АО ФИД «Деловой экспресс»

Адрес редакции:
125167, г. Москва, ул. Восьмого Марта 4-я, д. 6А
АО ФИД «Деловой экспресс»
Тел.: +7 (495) 787-52-26

Издание, распространение и реклама —
АО ФИД «Деловой экспресс»,
125167, Москва, ул. Восьмого Марта 4-я, д. 6А
Тел.: +7 (495) 787-52-26
E-mail: journal@dex.ru

http://www.dex.ru