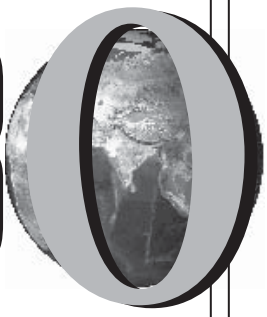
Научно-практический журнал

Non multa, sed multum

Выходит четыре раза в год

ИНДЕКС БЕЗОПАСНОСТИ



№ 4 (115), Том 21
Зима 2015

Российский журнал о международной безопасности

SECURITY INDEX

Издается с ноября 1994 г. (с 1994 по 2006 г. выходил под названием «Ядерный Контроль»)

ISSN 1992-9242

PIRPRESS

ИНДЕКС БЕЗОПАСНОСТИ

Издается с ноября 1994 г. В период с 1994 до 2006 г. выходил под названием *Ядерный Контроль*.
Выходит четыре раза в год.
Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Свидетельство о регистрации ПИ № ФС 77-60198 от 17.12.2014 г.
16 +. Для лиц старше 16 лет.

Учредитель
Общество с ограниченной ответственностью «ПИР-ПРЕСС»

№ 4 (115), Том 21
Зима 2015

Дата выхода номера

Редакция
Мостинская О.С., главный редактор
[mostinskaya@pircenter.org]
Трухтанова Е.А., технический редактор
Макеева Е.И., корректор

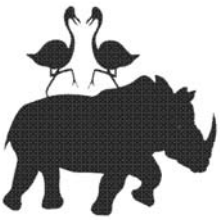
Адрес редакции и издателя
123242, г. Москва, ул. Дружинниковская, д. 30, стр. 1

Интернет-представительство:
http://si.pircenter.org

Тираж (российское и глобальное издания) 1000 экз.

Свободная цена

Отпечатано в ООО «Центр полиграфических услуг «Радуга», 115280, Москва, ул. Автозаводская, д. 25



Еще пару десятилетий назад взлом электронной почты требовал серьезных навыков программирования. Сегодня реальностью становятся молниеносные и анонимные атаки на банковские системы, подключенную к интернету бытовую технику и медицинское оборудование. Все чаще звучит термин *кибервойна*. Провозвестником новой эры стал вирус *Stuxnet*, в 2010 г. поразивший иранские центрифуги для обогащения урана и отбросивший ядерную программу страны на пару лет назад. Из проблем *второго эшелона* вопросы кибербезопасности переходят в категорию ПОВТОРНО, СРОЧНО.

О защите критической энергетической инфраструктуры от киберугроз, существующих пробелах в законодательстве и планах по их ликвидации главному редактору *Индекса Безопасности* О. Мостинской рассказал заместитель министра энергетики Российской Федерации Ю. Сентюрин.

Юрий Сентюрин:

«МЫ НЕ МОЖЕМ НЕ ВОСПРИНИМАТЬ ВСЕРЬЕЗ УТВЕРЖДЕНИЯ КОЛЛЕГ, КОТОРЫЕ ГОВОРЯТ О ПРИЗНАКАХ БОЕВЫХ ДЕЙСТВИЙ В КИБЕРПРОСТРАНСТВЕ»

— Уровень информатизации объектов ТЭК очень высок и постоянно растет. Возможны ли киберинциденты на объектах критической энергетической инфраструктуры, которые бы привели к серьезным авариям, аналогичным по масштабу аварии на Саяно-Шушенской ГЭС, — внеплановым сбросам воды или серьезным перебоям с энергоснабжением? Случались ли уже такие инциденты?

— По моему личному мнению, такого рода воздействия на работающую ТЭКовскую систему возможны. В этих вопросах министерство ориентируется на информацию и установки, которые мы получаем от профильных ведомств и организаций.

Очевидно, что реальная опасность в киберпространстве существует и нарастает. Безусловно, это является предметом обсуждения на специальных площадках. К слову, помимо отечественных экспертов такими же проблемами занимаются наши зарубежные партнеры. И мы не можем не воспринимать всерьез утверждения коллег, которые говорят о признаках *боевых действий* в киберпространстве. Это, безусловно, алармистская терминология, но не учитывать эти мнения, сбрасывать их со счетов нельзя.

Возможно ли эти вещи увидеть на конкретных примерах? К сожалению, да. Потому как управление производственным процессом на объектах критической топливно-энергетической инфраструктуры обеспечивается с помощью информационно-коммуникационных систем. Хотя в большинстве своем они работают в автономном режиме, без соприкосновения с глобальным киберпространством не обойтись. Есть примеры, когда пуски и остановы энергоблоков — а это ключевой элемент энергетического комплекса — имели место не с пульта оператора, размещающегося на энергообъекте, а из удаленных центров доступа. Понятно, что на этих коммуникационных линиях возможны разного рода несанкционированные действия.

С учетом нынешней ситуации в мире целесообразно действовать в режиме перестраховки. Такой подход позволяет чувствовать себя безопаснее, надежнее обеспечивать потребителей — промышленность, домохозяйства. Нельзя пренебрегать необходимостью повышать защищенность наших информационно-телекоммуникационных систем и информационных массивов от разного рода недружественных системных воздействий. Мы это понимаем и соответствующие действия предпринимаем.

Отмечу, что в киберпространстве имеют место и проявления киберхулиганства. Вреда от них не меньше. Армия профессиональных взломщиков, хакеров, которые орудуют в киберпространстве, далеко не всегда руководствуясь чистыми и благородными целями, разрастается. Информация об этом идет из самых разных источников, в том числе от известной *Лаборатории Касперского*. Свою задачу мы видим в том, чтобы обеспечить глобальную защиту, особенно в свете усложняющихся межгосударственных отношений.

Мы видим, какие угрозы и вызовы стоят перед нами. Вопрос в том, как на эти вызовы реагировать, какими силами и средствами. Энергетики понимают, что объекты ТЭК являются приоритетными, критически значимыми, обеспечивающими основы жизнедеятельности современной цивилизации. Логично, что эти объекты и их информационно-коммуникационные системы нуждаются в защите. Поэтому в законе, направленном на обеспечение безопасности объектов ТЭК, есть специальная статья по безопасности информационных систем. Статья — это акцент на проблеме. Задача соответствующих министерств и ведомств — подкрепить этот акцент практическими действиями.

— Вы упомянули 256-й закон и его статью 11. В ней действительно говорится об обеспечении безопасности информационных систем объектов ТЭК, но не содержится никаких конкретных требований. При этом, насколько я знаю, еще в 2013 г. был подготовлен проект закона о безопасности критической информационной инфраструктуры, который получил неплохую оценку со стороны экспертного сообщества. В нем есть ряд весомых досто-

инств: прописаны основные определения, зоны ответственности. Однако он до сих пор не принят. Почему и какие у него перспективы?

— Этот законопроект готовился не по линии Минэнерго России. У каждого ведомства своя зона ответственности. Есть государственные органы, которые по своему профилю отвечают за это направление работы. Мы были причастны к этому документу как соисполнители и последовательно выступали в его поддержку. Параллельно с разработкой этого концептуального документа мы в рамках ведомственных полномочий работали над обеспечением информационной безопасности наших объектов.

В 2013 г. мы вышли с предложением внести изменения в ФЗ 256 *О безопасности объектов ТЭК*. Этот закон был принят в середине 2011 г., начал применяться в полном объеме с 1 января 2012 г. Концептуально ответственность за обеспечение безопасности закон возлагает на собственников объектов ТЭК при том понимании, что ответственность государства состоит в противодействии экстремизму, терроризму, обеспечении глобальной безопасности. Возлагая ответственность на корпоративный сектор, государство устанавливает требования, стандарты, ниже которых нельзя *опускаться* в выстраивании систем защиты.

Таков общий подход. Однако если по направлениями физической защиты, по вопросам привлечения персонала, который отвечает за обеспечение безопасности, правила и требования были подробно прописаны, то в сфере защиты информационно-коммуникационных систем был просто сделан акцент и было обозначено, что ответственность лежит на бизнесе. *Централизованных* правил и требований, устанавливаемых государством, предложено не было. Поэтому в 2013 г. мы предложили внести изменения в ФЗ 256, чтобы собственники, несущие всю полноту ответственности за обеспечение безопасности, имели ориентиры для практической работы.

Этот замысел не был реализован в полном объеме, в том числе из-за опасений наших партнеров из корпоративного сектора по поводу *завышения* требований, что могло, по их мнению, привести к существенному возрастанию затрат, *перестройке* технической части, поскольку сегодня всем очевидно, что в этой работе нужно ориентироваться на отечественные разработки, элементную базу и технику.

Вместе с тем, весьма непросто, оказавшись перед столь широкой гаммой вызовов, как снижающаяся стоимость энергоресурсов на мировом рынке, односторонние санкции, ограничение доступа к передовым технологиям, пойти на серьезные затраты в целях решения вопросов, которые еще недавно воспринимались как задачи сопутствующего характера. Поэтому вопрос разумного баланса, золотой середины является принципиально важным.

Поясню на примере: в сентябре 2015 г. вышло постановление правительства России, устанавливающее правила обеспечения безопасности линейных объектов ТЭК. Этот документ готовился довольно долго как раз по тем причинам, о которых я говорил: страна очень большая, миллионы километров электрических воздушных линий и десятки тысяч километров трубопроводов. Их надежная защита безусловно требует больших расходов. Поэтому выходу документа предшествовала

интенсивная дискуссия, позволившая найти взвешенный компромисс. Государство понимает, что сегодня ввести *сверхзатратные* требования, конечно, нельзя.

Аналогичный подход принят за основу в работе по защите от киберопасности. Есть понимание, что угроза реальна, и именно государство должно сформулировать универсальные подходы к обеспечению безопасности на уровне отдельных компаний.

Пока не приняты изменения в ст. 11 ФЗ 256, мы работаем на уровне ведомственных нормативных актов. Функционирует созданная приказом министерства рабочая группа по противодействию терроризму в ТЭК. Это межведомственный орган, в состав которого помимо министерских работников и руководителей службы безопасности компаний ТЭК входят представители МВД, ФСБ, Национального антитеррористического комитета, министерства юстиции, МЧС — в общем, все профильные специалисты. На этой площадке мы и прорабатываем такого рода вопросы.

В частности, изучены специфика организации защиты информационных систем в компаниях — лидерах рынка. Это компании электроэнергетического, нефтегазового, угольного профиля. Проведен обмен мнениями и опытом, мы посмотрели, как степень защищенности оценивается специалистами эксплуатирующих организаций. Отмечу, что универсальных подходов нет. В итоге специалисты, изучив весь этот материал, пришли к выводу о необходимости унификации требований, в т. ч. в связи с запуском механизма государственного контроля (надзора) за обеспечением безопасности объектов ТЭК. Эта функция закреплена за МВД России. Предусмотрена система плановых и внеплановых проверок. Возникает вопрос: чем проверяющая инстанция будет руководствоваться, *тестируя* систему защиты информационно-коммуникационного блока? Естественно, пока придерживаемся требований приказа ФСТЭК № 31, притом что, по мнению специалистов, в этом документе, несмотря на его универсальность, в полном объеме специфика ТЭКовских объектов не учтена.

— Есть еще одна проблема: приказ ФСТЭК не опирается ни на один федеральный закон, поэтому его юридическая сила не очевидна.

— Именно поэтому считаем, что ст. 11 должна быть дополнена полномочиями правительства Российской Федерации устанавливать подобного рода правила и требования.

При этом важно учесть передовой опыт и все имеющиеся наработки, не забывая о необходимости сбалансированного подхода, чтобы, заботясь о защите информационных систем, мы не набросили удавку на бизнес в виде чрезмерных расходов. Простого решения тут быть не может. Безусловно, потребуется переходный период, время на адаптацию, время на то, чтобы развернуть производство соответствующих мировым стандартам отечественных аналогов.

В этом направлении мы сейчас планово движемся. Работаем через механизм специально созданной при вышеупомянутой рабочей группе министерства секции, в состав которой вошли представители ключевых компаний ТЭК, коллеги из ФСТЭК и других специализированных организаций, как государственных, так

и частных. Мы рассчитываем к концу первого квартала 2016 г. получить базовый материал, который вынесем на широкое общественное обсуждение.

— Работа предстоит довольно масштабная. При этом есть опыт других стран, других отраслей. Ведется ли международное, межведомственное сотрудничество? Большой опыт обеспечения кибербезопасности есть у атомной отрасли, у* Росатома*, МАГАТЭ, которое выпустило уже немало регламентов по кибербезопасности. В этом году состоялась первая* Конференция МАГАТЭ по компьютерной безопасности в ядерном мире*. Есть ли планы использовать опыт коллег?

— Безусловно, несмотря на специфику производственных процессов в ТЭКе, информационно-коммуникационные системы, используемые в отрасли, достаточно универсальны. В основе нашей работы — изучение опыта передовых компаний, в том числе работающих в атомной отрасли. Что касается международного опыта — секции поставлена задача изучить все тематические публикации, в том числе документы МАГАТЭ.

Естественно, не вся информация находится в режиме свободного доступа, такова специфика темы. Однако изобретать велосипед не собираемся, будем опираться на передовой опыт.

— Сегодня за промышленную и информационную безопасность отвечают разные ведомства. Что, если произойдет киберинцидент с серьезными последствиями? В их ликвидации будут задействованы и ФСТЭК, и ФСБ, и МВД, и Минэнерго. Как будет делиться ответственность? Существуют ли механизмы координации?

— Затронут очень важный вопрос. Мы работаем параллельно — я упоминал это, когда рассказывал о проекте закона, который разрабатывают коллеги из соседних структур. Мы пытаемся решить проблему через механизм межведомственной рабочей группы, привлекая туда всех, кто причастен к этой работе, чтобы избежать дублирования норм и требований.

Наша задача — безусловно, привести все к единому знаменателю. Упомянутая секция столкнулась с проблемой стыковки норм промышленной, информационной и прочих видов безопасности. В этой работе нам очень помогает, к примеру, помимо упомянутых структур, Межведомственная рабочая группа Совета Безопасности России по информационной безопасности. На этой площадке мы получаем материал установочного характера, пытаемся потом к нему пристыковать отраслевую специфику и вносим предложения, которые не противоречат общим установкам.

— Есть ли планы по проведению учений для отработки координации действий различных ведомств в случае чрезвычайных ситуаций, вызванных киберинцидентами?

— Такие задумки есть. Подобного рода учения — требования жизни. Приведу пример: в начале ноября текущего года после террористических атак во Франции мы провели всероссийское селекторное совещание, поставили задачу организовать тренировки корпоративного уровня, проверить надежность работы всех наших

коммуникационных систем и связи. При возникновении сложной ситуации — будь то ЧС, техногенная авария или противоправное вмешательство в деятельность отраслевого субъекта — необходима система коллективных контрмер. Поэтому все системы взаимодействия находятся в повышенной готовности. Специального акцента на том сценарии учений, о котором вы говорите, мы не делаем. Одна из причин — подобного рода тренировки проводятся по инициативе профильных организаций, комплексно отвечающих за вопросы противодействия экстремизму в силу специального закона. По нашей информации, такие планы есть.

Вопросы киберопасности обсуждаются все шире. Серьезный анализ проводился во время подготовки и проведения Олимпийских и Паралимпийских игр в Сочи. Тогда была развернута целая система контроля за киберпространством, фиксировались киберпосягательства, приняты своевременные меры. Эти события дали толчок к активизации наших усилий по совершенствованию 11-й статьи и по созданию специальной секции министерской рабочей группы по противодействию терроризму. Процесс пошел. 

Андрей Малов

ЧТО СТОИТ НА ПУТИ К ДОГОВОРУ О ПРЕДОТВРАЩЕНИИ РАЗМЕЩЕНИЯ ОРУЖИЯ В КОСМОСЕ

В настоящее время мы являемся свидетелями резко возросшего интереса международного сообщества к решению практических вопросов обеспечения безопасности космической деятельности (БКД). В экспертных кругах сложилось общее понимание, что БКД — сложное многокомпонентное понятие, а ее обеспечение требует широкого спектра мер, нацеленных на решение проблем оружейного, техногенного и международно-правового характера.

При этом следует констатировать, что космическая деятельность традиционно несет значительную оборонную нагрузку, а обеспечение сохранности и устойчивости функционирования космических аппаратов является одним из основных условий поддержания стратегической стабильности и военно-политической предсказуемости в глобальном масштабе.

Характерно, что ряд областей военной деятельности в космосе с международно-правовой точки зрения ничем не ограничен. Вряд ли кто-либо из серьезных экспертов поставит под сомнение легитимность использования таких средств военно-космического обеспечения, как геодезия, метеопрогнозирование, связь, навигация, разведка, слежение и нацеливание. Вместе с тем существующая нормативная база в области международного космического права регулирует лишь отдельные аспекты использования космоса в военных целях и недостаточна для предотвращения размещения там оружия. Договор по космосу 1967 г. запрещает выведение в космическое пространство только оружия массового уничтожения (ОМУ), запрет же на размещение в космосе иных видов оружия не установлен.

При этом по ряду направлений военной космической деятельности нет никаких запретительных или ограничительных норм. Это касается как создания и использования отмеченных нами выше военных космических систем обеспечения — *support space systems*, так и создания и возможного размещения в космосе оружейных ударных космических систем, не относящихся к ядерным или любым другим видам ОМУ — *weapon space systems*.

Не секрет, что на протяжении последних десятилетий — и об этом неоднократно сообщалось в открытых источниках — в ряде технологически развитых стран проводятся интенсивные НИОКР в области достаточно широкого спектра оружия космического базирования, отличного от ОМУ.

В чем причины настороженного отношения к перспективам вывода оружия в космос?

Полагаем, что в целом такие ударные космические системы следовало бы отнести к новому виду *стратегического оружия* в силу их характеристик. Прежде всего потому, что такое оружие имело бы глобальную зону действия, высокую готовность к применению, возможность внезапного и скрытного воздействия на поражаемые объекты. В отличие от ОМУ оно стало бы не инструментом сдерживания, а *оружием реального применения*.

Формируя *потенциал первого удара*, многократно усиливая значение фактора внезапности, оружие космического базирования явилось бы дестабилизирующим по своей сути, оказало бы глубокое и во многом непредсказуемое влияние на стратегический паритет, вызвало бы подозрительность и напряженность в межгосударственных отношениях. Климат взаимного доверия и сотрудничества в освоении космоса был бы разрушен. Государства были бы поставлены перед необходимостью принимать ответные меры, что провоцировало бы качественно новый этап гонки вооружений. Кроме того, воздействие космического оружия на ионосферу Земли имело бы пагубные последствия.

Важно учитывать также принципиально новые информационно-технологические возможности, которые предоставляет грядущий, шестой, научно-технический и, следовательно, экономический уклад, в который неуклонно *входит* человечество. Как следствие, бурный процесс миниатюризации космических аппаратов (КА), повышение уровня их управляемости и мобильности, возможностей скрытно влиять на функционирование *чужих* КА, переподчинять их своей воле.

Можно ли обеспечить безопасность космической деятельности без установления надежной преграды для возможного размещения оружия в космосе? На наш взгляд, нельзя. И такое понимание медленно, но неуклонно пробивает себе дорогу во все большем числе государств.

Ведь в случае размещения оружия в космосе нереально будет говорить о сохранности дорогостоящей и стратегически, экономически, научно важной космической собственности. Значительный ущерб мог бы быть нанесен не только военной компоненте космической группировки. С учетом значительной интеграции в использовании космических активов, как военных, так и гражданских, а по отдельным космическим программам — участия большого количества государств и международных организаций, вывод из строя таких средств негативно сказался бы на экономическом и научном потенциале всего международного сообщества. Кроме того, в стратегическом плане вопрос об оружии в космосе однозначно связан с возможностью доминирования в нем, что вплотную подводит нас к попыткам военно-политического доминирования на Земле.

Совокупностью этих причин и задачей обеспечения устойчивости и предсказуемости международной безопасности, поддержания стратегической стабильности, особенно в период продолжающегося накопления конфликтного потенциала в мире, и определяется убежденность России в необходимости заключения всеобъемлющей юридически обязывающей международно-правовой договоренности о предотвращении размещения в космосе оружия любого вида.

Ключевые положения международного космического права:

- *государства исследуют и используют космическое пространство в соответствии с международным правом, включая Устав ООН;*
- *космическое пространство открыто для исследования и использования всеми государствами без какой-либо дискриминации на основе принципов равенства и свободы доступа;*
- *космическое пространство не подлежит национальному присвоению ни путем провозглашения на него суверенитета, ни путем использования или оккупации, ни любыми другими средствами;*
- *государства обязались запретить, предотвратить и не производить любые испытательные взрывы ядерного оружия и любые другие ядерные взрывы в космическом пространстве;*
- *государства обязались запретить военное или иное враждебное использование средств воздействия на природную среду, в том числе и на космическое пространство;*
- *государства обязались не выводить на орбиту вокруг Земли любые объекты с ядерным оружием или любыми другими видами ОМУ, не устанавливать такое оружие в космическом пространстве каким-либо иным образом. Запрещается создание на небесных телах военных баз, сооружений и укреплений, испытание любых типов оружия и проведение военных маневров.*

ЛИСТАЯ СТАРЫЕ СТРАНИЦЫ

ВАСИЛИЙ ЛАТА, ВЛАДИМИР МАЛЬЦЕВ

Статистика показывает, что в годы Второй мировой войны для уничтожения такой типовой цели, как крупный железнодорожный мост через широкую реку, требовалось совершить 4,5 тыс. самолетовылетов и сбросить около 9 тыс. авиабомб. В то же время за счет повышения точности поражения в войне во Вьетнаме подобная цель уничтожалась 190 авиабомбами, сброшенными 95 самолетами. В войне в Югославии эту же боевую задачу решали 1–3 высокоточные крылатые ракеты, запущенные с подводной лодки, находящейся в Средиземном море. Такое повышение точности возможно лишь при сопряжении ударных средств с космическими. Это сопряжение, безусловно, дает глобальное одностороннее преимущество стороне, которая обладает такими средствами поражения.

Усилия ООН, других международных организаций в области международно-правового регулирования космической деятельности необходимо сосредоточить на создание такой нормативно-правовой базы, которая накладывала бы ограничения на количественные и качественные характеристики существующих и разрабатываемых космических систем военного и двойного назначения, способных быть включенными в контур боевого управления системами оружия.

Таким образом, можно сделать вывод о том, что распространение гонки вооружений на космос не может укрепить чью-либо безопасность. Создание систем оружия на основе широкого использования в их составе космических средств может привести к увеличению масштабов и числа участников военных конфликтов, так как космос является умножителем возможностей вооруженных сил государств мира. При этом государства, имеющие значительный космический потенциал, будут обладать серьезными стратегическими преимуществами. Для решения этих проблем необходимо плодотворное конструктивное сотрудничество всего мирового сообщества под эгидой ООН.

Система систем: информационно-ударное оружие.
***Индекс Безопасности*. 2007. Т. 13, № 3 (83).**

НЕМНОГО ИСТОРИИ

В 1980-х гг. Россия выступила в ООН с предложением выработать соглашения о неприменении силы из космоса в отношении Земли и с Земли в отношении космических объектов. Предложения натолкнулись на неприятие со стороны США и дальнейшего развития не получили. Затем, уже на новом витке истории, по предложению президента России, которое было озвучено на Саммите тысячелетия в Нью-Йорке в сентябре 2000 г., в Москве в апреле 2001 г. состоялась международная конференция *Космос без оружия — арена мирного сотрудничества в XXI веке*. В ходе конференции впервые были четко сформулированы и озвучены идеи о разработке договоренности по предотвращению размещения оружия в космосе (ПРОК), неприменению силы или угрозы силой в отношении космических объектов. Была также озвучена идея ввести мораторий на размещение в космосе боевых средств.

Свое официальное оформление эта инициатива получила на 56-й сессии ГА ООН (сентябрь 2001 г.), когда министр иностранных дел России предложил начать работу над соответствующими договоренностями. Конкретные предложения включали выработку договоренности по ПРОК, а также введение моратория на размещение в космосе боевых средств. В тот период инициатива воплотилась в российско-китайском документе о возможных элементах будущей договоренности по ПРОК, который был представлен в июне 2002 г. на Конференции по разоружению (КР). На 59-й сессии ГА ООН в 2004 г. Россия заявила, что не будет первой размещать в космосе оружие любого вида и призвала все государства, обладающие космическим потенциалом, последовать ее примеру. В 2005 г. к инициативе присоединились государства ОДКБ. В настоящее время участниками инициативы также стали Шри-Ланка, Бразилия, Индонезия, Аргентина и Куба.

Российско-китайский проект договора по ПРОК (ДПРОК) был официально внесен Министром иностранных дел России на Конференцию по разоружению (КР) 12 февраля 2008 г. За период после внесения проекта ДПРОК прошли интенсивные дискуссии по его различным аспектам, были представлены замечания и предложения. Для продвижения проекта, разъяснения сути его ключевых положений использовались официальные и неофициальные заседания КР, ежегодные международные конференции по безопасности космической деятельности, проводимые Институтом ООН по исследованию проблем разоружения (ЮНИДИР).

В июне 2014 г. Россия и Китай внесли на КР обновленную версию проекта ДПРОК[1], составленную с учетом внесенных замечаний. Таким образом, документ перестал быть продуктом двусторонних усилий, став, по сути, результатом коллективного труда и приобретя тем самым многосторонний характер.

В ЧЕМ СУТЬ ДПРОК?

По своему характеру ДПРОК представляет собой международный юридически обязывающий инструмент превентивного действия, устанавливающий барьер на пути возникновения качественно новой сферы вооруженного противостояния. К ключевым обязательствам по ДПРОК как в его изначальной, так и в доработанной версии следует, на наш взгляд, прежде всего отнести следующие обязательства: не размещать в космическом пространстве оружие любого вида; не при-

бегать к применению силы или угрозы силой в отношении космических объектов государств-участников. При этом проект ДПРОК изначально не задумывался как документ, нацеленный на запрещение конкретного вида вооружений. Совокупность этих элементов, составляющих сферу охвата договора, и должна, по замыслу разработчиков, сделать, как минимум, нецелесообразным разработку и испытание таких видов вооружений. Ценность договора, на наш взгляд, заключается в том, что он прежде всего нацелен на создание условий для минимизации стимулов для создания такого оружия.

Запрет на проведение исследований, разработку, производство и даже наземное хранение оружия или его элементов, предназначенных для космического базирования, лишен смысла по одной простой причине — практической невозможности все это проконтролировать. По этой же причине не вводятся запреты на проведение испытаний в этой области.

Российские представители на разных уровнях и с трибун различных форумов отмечали, что обновленный проект ДПРОК — это не документ, *вырезанный из камня*, и что дальнейшая его доработка и улучшение являются естественным и во многом необходимым условием подготовки к его принятию в рамках переговорного процесса. При этом — и, на наш взгляд, вполне обоснованно — подчеркивалось, что документ созрел для полноценной переговорной работы, естественной площадкой которой явилась бы Конференция по разоружению. Уместно подчеркнуть, что идея перевода обсуждений проблематики предотвращения гонки вооружений в космическом пространстве (ПГВК) в русло переговорных усилий по выработке ДПРОК поддерживается значительным числом государств, включая наших союзников по ОДКБ и партнеров по БРИКС. Вместе с тем идея международно-правового *барьера* на пути размещения ударного оружия в космосе с самого начала натолкнулась на значительное противодействие со стороны такого космического *тяжеловеса*, как США.

Весьма показательно, что традиционная ежегодная резолюция, вносимая поочередно Египтом и Шри-Ланкой на сессиях Генеральной Ассамблеи ООН, — *Предотвращение гонки космических вооружений в космическом пространстве*[2] — получает почти универсальное одобрение за исключением двух голосов воздержавшихся — США и Израиля. Сам факт, что против резолюции никто не голосует, наглядно подтверждает исключительную актуальность проблемы ПГВК и признание международным сообществом необходимости ее скорейшего решения.

Справедливости ради, надо признать поддержку, которую оказывают американцы резолюции по мерам транспарентности и доверия в космической деятельности (МТДК), выработанную по итогам работы профильной Группы правительственных экспертов (ГПЭ). США даже вошли в число соавторов этой резолюции, создав во многом беспрецедентный *триумвират* в лице России, Китая и США, тем самым фактически дав понять, что они являются сторонниками преимущественно рекомендательных подходов к поиску наиболее адекватных методов и форм обеспечения безопасности космической деятельности и выступают за выработку скорее свода правил поведения, чем обязывающих норм. Уместно при этом отметить различные интерпретации МТДК, которые все чаще озвучиваются в ходе попыток нащупать конкретные формы и способы их осуществления и продвижения. Уже на этапе выработки и согласования итогового доклада ГПЭ по МТДК российскими

экспертами подчеркивалось, что эти меры могут иметь как добровольно-рекомендательный характер, так и включать в себя юридически обязывающие договоренности, тогда как американскими экспертами делался акцент на преимущественно добровольном характере этих мер.

Так что же мешает активно поддержать идею выработки ДПРОК? Официально озвучиваются следующие основные аргументы, которые используются американскими представителями на различных международных площадках с целью обосновать непринятие не просто обновленного ДПРОК, но и самой идеи выработки юридически обязывающего инструмента в этой области. В концептуальном плане американские представители, включая профильных экспертов, подтверждают важность сохранения норм международного космического права и заявляют о готовности рассматривать предложения по новым юридически обязывающим договоренностям, если таковые будут отвечать трем критериям: объективности, проверяемости и соответствию интересам укрепления национальной безопасности США и их союзников. При этом в отношении как изначального, так и обновленного проектов российско-китайского ДПРОК американцы продолжают утверждать, что он не соответствует данным критериям.

С точки зрения критерия *объективности* американские коллеги заявляют, что оружия в космосе сейчас нет, когда оно там появится, неизвестно, а потому, по их мнению, ни о какой гонке вооружений в космическом пространстве пока говорить не приходится. Американцы настаивают, что сосредотачиваться надо на таких более конкретных вызовах, как опасные сближения космических аппаратов, космический мусор и т. п. Другой аргумент, традиционно выдвигаемый американцами, касается критерия *проверяемости*. Проект ДПРОК подвергается устойчивой критике за отсутствие в нем механизма проверки. Здесь уместно напомнить, что, работая вместе в ГПЭ по МТДК, американцы последовательно отстаивали их сугубо добровольный характер. При этом наши эксперты не исключали возможность выработки государствами не только добровольных, но и политически и юридически обязывающих договоренностей. Предлагали рассматривать массив обсуждаемых МТДК в качестве составной части проекта ДПРОК как каркас возможного будущего инструмента проверки соблюдения договора. Одновременно мы подчеркивали и подчеркиваем, что проект обновленного ДПРОК — это приглашение к предметной работе над текстом договора, который остается открытым для различных новаций и предложений, включая те из них, которые имеют отношение к проверочному механизму инструмента.

В более широком плане нами неоднократно отмечалось, что далеко не все действующие договоры имеют механизм проверки. Пример — Договор по космосу 1967 г.[3] и прописанное в нем обязательство *не выводить на орбиту вокруг Земли любые объекты с ядерным оружием или любыми другими видами оружия массового уничтожения*. При этом стоит обратить внимание на Статью IX Договора, в которой говорится: «Государство — участник Договора, имеющее основание полагать, что деятельность или эксперимент, запланированные другим государством — участником Договора в космическом пространстве… создадут потенциально вредные помехи в деле мирного исследования и использования космического пространства… может запросить проведение консультаций относительно такой деятельности или эксперимента». Прежде всего хотели бы подчеркнуть, что соответствующее положение о проведении консультаций включено и в обновлен-

ный текст проекта ДПРОК — статья VII. Исходим также из того, что с развитием технологий наблюдения и контроля упомянутые в тексте статьи Договора *основания полагать* во все большей степени будут подкрепляться техническими возможностями. Существуют и другие опции — например, система коллективного обмена данными и анализа ситуации. Кроме того, государства — участники ДПРОК могут делать ежегодные заявления в отношении своей космической политики и стратегии. Что касается государств — не членов ДПРОК, они могут использовать национальные средства контроля и отдельные механизмы договора.

Итак, вариантов немало, дело за политической волей. В общем политическом плане соблюдение запретительного режима могло бы стимулироваться и тем пониманием, что в случае обнаружения его нарушения международные последствия для государства-нарушителя могут оказаться несоизмеримыми с кажущейся выгодой от этого нарушения. Кроме того, в целом предлагаемый запрет на размещение и применение оружия в космосе, а также на применение средств с целью нанесения ущерба космическим объектам других государств делают разработку, тестирование и производство таких вооружений нецелесообразными в силу их дороговизны. Особняком в наборе аргументов против ДПРОК стоит фактор применения силы в космосе как неразрывный элемент права на самооборону. Американские эксперты склонны утверждать, что п. 4 Статьи II Устава ООН[4] уже запрещает применение силы или угрозу силой в отношении космических объектов другого государства.

В этом контексте хотели бы привлечь внимание к весьма абстрактной формулировке, которая предлагает воздерживаться от применения силы или угрозы силой *каким-либо другим образом, не совместимым с целями Объединенных наций*. При этом уместно подчеркнуть, что Устав ООН, при всей его абсолютной значимости, писался в докосмическую и доинформационную эпоху, и многие формулировки требуют выработки дополнительных критериев, нацеленных на согласованную и универсально понимаемую их интерпретацию. Многие эксперты признают, что в правовом отношении право на самооборону и на применение силы до конца не проработано. Достаточно сказать, что реализация права на самооборону необходима с соблюдением принципов пропорциональности и соразмерности, границы которых при нападении на космические объекты определить может быть весьма затруднительно.

Правовая дискуссия может быть также отягощена фактором так называемых *устаревших* со времени принятия Устава ООН формулировок. Статья 51 описывает нападение как *armed attack*, что в эпоху информационных и других новейших технологий не всегда соответствует буквальному значению методов ведения боевых действий с использованием обычных сил и средств. В этом контексте конкретизация существующих норм международного права в отношении космического пространства, и в частности, концепции *применения силы* или *угрозы силой* и является одним из условий обеспечения безопасности в космосе. Российско-китайский проект ДПРОК как раз и мог бы внести свой конкретный практический вклад в решение этой проблемы.

С темой обоснованного права за защиту тесно связано и положение о праве на самооборону в соответствии со Статьей 51 Устава ООН, которое в формулировочном плане дано в обновленном варианте проекта договора в максимально прибли-

женном к оригиналу виде. Аргументы некоторых критиков ДПРОК, что зафиксированное в тексте право на самооборону якобы противоречит самой цели ДПРОК, этой самой критики не выдерживают. К числу других традиционных аргументов против ДПРОК относится довод о том, что проект не предусматривает полного запрета на противоспутниковые средства (ПСС).

Полагаем, что этот вопрос нельзя вырывать из стратегического контекста. Понимание опасности возможного практического размещения оружия в космосе и является главной побудительной причиной создания ПСС. При этом ПСС рассматриваются в качестве асимметричных мер, прежде всего против потенциальных ударных космических систем.

В этом контексте, запрещая размещение оружия в космосе, необходимо учитывать возможность вступления в международные договоренности не всех государств, а также право выхода из нее любого государства. Поэтому потенциал создания оружия космического базирования будет сохраняться, а государства-участники вправе иметь в такой ситуации ответные возможности, в качестве которых и рассматриваются ПСС. Именно по этой причине обновленный проект ДПРОК, запрещая размещение в космосе оружия любого вида и вводя обязательство не прибегать к применению силы или угрозе силой, *намеренно* не вводит запрет на создание и испытание по собственным мишеням ПСС наземного, морского и воздушного базирования.

Таковы *внешние* аргументы, которые приводятся для того, чтобы подвергнуть сомнению целесообразность предметной работы по выработке и принятию ДПРОК.

ЧТО В РЕАЛЬНОСТИ МЕШАЕТ ПРИНЯТЬ ИДЕЮ ДПРОК?

Прежде чем ответить на этот вопрос, обратимся к не столь отдаленной истории.

Последние 10–15 лет Администрации США, что при Дж. Буше, что при Б. Обаме, проводят интенсивную программу исследований и разработок, нацеленную на создание перспективных боевых систем и конкретных космических платформ, обладающих способностью не только уничтожать объекты, находящиеся в космосе, но и наземную стратегическую инфраструктуру. Наглядным примером таких приготовлений служит серия проведенных испытаний космической платформы многоразового пользования Х-37В, размещение на орбите способных автономно маневрировать мини-спутников весом по несколько килограммов, эксперименты по электронному противодействию и радиоэлектронной борьбе (РЭБ) в космосе.

Следует, впрочем, отметить, что научно-технологические заделы качественно нового этапа подготовки боевого ударного космического потенциала, осуществляемого в наши дни, создавались еще на более раннем этапе освоения космоса. В период холодной войны как в СССР, так и в США были проведены широкие исследования областей возможного применения космической техники в военных целях, принят на вооружение ряд космических систем военного назначения, которые в ту пору получили общее наименование *космических средств обеспечения вооруженных сил*. К их числу относили космические системы видовой разведки, радио- и радиоэлектронной разведки, обнаружения стартов ракет и предупреждения о ракетном нападении, обнаружения ядерных взрывов в различных средах, боевого управления и связи (Command Control Communication and Intelligence —

си-кьюб-ай), метеорологического, навигационного, топогеодезического и картографического обеспечения вооруженных сил. Как мы уже отмечали выше, космические системы такого назначения существенно повысили эффективность систем оружия и вооруженных сил и надолго укоренились как важный элемент структуры вооружений космических держав.

К тому же периоду относятся практические попытки разместить в космосе оружие для поражения наземных, морских и воздушных целей. Следует подчеркнуть, что известные результаты зарубежных исследований не показали в ту пору превосходства космических систем оружия перед иными, и в силу этого они не получили заметного развития.

Вместе с тем уже на том, весьма ограниченном в плане информационного обеспечения этапе, удалось создать реально функционирующие ударные системы с частичным полетом их поражающих элементов — так называемые глобальные ракеты, или fractional orbital bombardment systems (FOBS). В ходе проводившихся исследований значительное внимание уделялось изучению возможностей создания космических систем борьбы с баллистическими ракетами — систем ПРО. В США такие работы были объединены в запущенную еще в 1983 г. и получившую широкую огласку программу *Стратегической оборонной инициативы* (СОИ).

В качестве возможных средств поражения для оснащения космических систем ПРО рассматривалось кинетическое, лазерное, пучковое, электромагнитное оружие.

В этом контексте весьма показательно то, что, несмотря на стоящий на пути этих приготовлений Договор по ПРО 1972 г., американская Администрация тех лет была готова к обсуждению внесения в него поправок, развязывающих руки для претворения в жизнь этих планов. Однако ввиду явных технических и организационных трудностей все эти глобальные планы в полной мере реализовать не удалось, и вопрос о внесении поправок был снят с повестки дня.

Широкие исследования были проведены в то время и в сфере создания и практического развертывания противоспутниковых систем. Как представляется, причины интереса космических держав к ПСС были связаны со следующими факторами. Многочисленные КА и системы различного целевого назначения являлись собственностью конкретных государств, различных международных и деловых структур. В силу экстерриториальности космического пространства, то есть его непринадлежности государству или группе государств и, как следствие, универсальной доступности космоса, вставал вопрос о сохранении и защите космической собственности. Кроме того, уже тогда возник соблазн обеспечения военно-политического доминирования через доминирование в космосе. В результате появились практические наработки в создании этих систем.

В США сначала была создана ПСС на основе ракеты-перехватчика наземного стационарного базирования, а затем в 1980-е гг. ПСС *ASAT* самолетного базирования, успешно, кстати, испытанная по реальной цели в космосе, но так и не развернутая и не поступившая на вооружение. С другой стороны, в СССР в 1970-х гг. был развернут наземный комплекс противокосмической обороны *ИС*, который находился в эксплуатации до апреля 1993 г., хотя начиная с 1983 г. испытательные пуски спутников-перехватчиков не проводились.

Кроме того, после выхода США в 2002 г. из Договора по ПРО прекратило существование и обязательство не создавать, не испытывать и не развертывать системы и компоненты ПРО космического базирования. Следует подчеркнуть, что это не только открыло путь к созданию космического оружия для целей ПРО, но и дало возможность создавать и испытывать противоспутниковое оружие (ПСО) космического базирования в силу близости соответствующих технологий. Таким образом, уже в то время закладывалась определенная основа для создания потенциала ударных боевых космических систем.

Понимая это, Советский Союз принял на себя в 1983 г. обязательство не выводить первым в космос какие-либо виды ПСО на все то время, пока другие государства будут воздерживаться от вывода в космос ПСО любого вида. Кстати сказать, этот мораторий охватывал и испытательные запуски ПСС. Весьма показательно, что условия этого моратория были Соединенными Штатами нарушены, когда в 1985 г. был осуществлен перехват противоспутниковой системой *ASAT* реального американского космического объекта — ИСЗ *Солуинд*. СССР заявил, что считает себя с этого момента свободным от одностороннего обязательства. Вместе с тем, Советский Союз продолжал воздерживаться от вывода в космос противоспутникового оружия.

Уже в *новое время* в 1992 г. президентом России была подтверждена готовность на основе взаимности с США ликвидировать существующие ПСС и выработать договоренность о полном запрете вооружений, специально создаваемых для поражения спутников. Однако и это наше предложение не нашло позитивного отклика у США. А в 1993 г. советская противоспутниковая система *ИС* была снята с эксплуатации.

Что касается нынешнего этапа космических приготовлений, то многое становится яснее при анализе ключевых положений двух базовых документов, которые закладывают основы подходов США к БКД и к проблематике военного космоса: *Национальной стратегии космической безопасности*[5] 2011 г. и *Космической политики*[6], последняя редакция которой вступила в силу 18 октября 2012 г., заменив аналогичный документ от 9 июля 1999 г.

В *Национальной стратегии*, по сути, продекларировано стремление США к превосходству в космосе, которое, впрочем, по задумкам разработчиков, должно обеспечиваться активными действиями преимущественно мирного характера. В то же время отдельные положения стратегии допускают создание и отработку орбитальных средств, предназначенных для выполнения военных операций в космосе и из космоса.

В документе, в частности, провозглашается лидерство США в космической деятельности, обеспечивающее США преимущества в ведении военных действий и решении задач национальной безопасности в глобальном масштабе и возможность контроля событий, происходящих во всем мире, что является одним из основных принципов обеспечения национальной безопасности.

Национальная стратегия предусматривает не только контроль создания космических средств в других государствах, но и активное участие в их создании, а также использование этих средств в своих интересах.

Серьезное внимание уделяется работам в Китае, особенно в части создания средств поражения объектов в космическом пространстве. Это вызывает беспокойство США, так как может, по американским оценкам, при определенном развитии событий ограничить возможности использования космического пространства.

Для контроля состояния космических исследований и работ по созданию перспективных космических средств в других государствах, в том числе и сдерживания этих работ, предлагается использовать в полной мере методы экспортного контроля.

Каким же образом США предполагают обеспечить свое лидерство в космической деятельности? В целях нашего исследования считаем целесообразным отметить следующее:

- формирование потребностей в создании космических средств исходя из *стратегических политических целей* и организация государственных заказов по разработке космических средств с учетом этих целей;
- поощрение партнерства в космической сфере с ответственными государствами, международными организациями и коммерческими компаниями *с учетом политических интересов США*, обеспечение конкурентоспособности космической промышленности;
- разработка совместно с союзниками космической доктрины, предусматривающей, в частности, использование совместного космического потенциала в кризисных и конфликтных ситуациях;
- контроль и руководство работами в области гражданской космонавтики со стороны Министерства обороны и разведывательного сообщества США.

Таким образом, основными заявленными целями Национальной стратегии космической безопасности США является сохранение существующей стабильности, а также обеспечение безопасности своих действий в космосе. При этом — и это важно для ответа на наш вопрос о ДПРОК — космические приготовления как в ее гражданской, так и в военной составляющей, очевидно, ставятся в прямую зависимость от политических и стратегических глобальных установок американского военно-политического руководства.

Кроме того, стратегия предполагает наращивание возможностей по определению источников враждебных действий, а также по парированию этих действий. Сохраняется право наносить *ответные удары* в целях самообороны и в случае, если политика сдерживания в космической области потерпит неудачу.

Для понимания причин, мягко говоря, сдержанного отношения США к идее постановки правового барьера на пути вывода ударных боевых средств в космос любопытна и директива минобороны США по космической политике от 2012 г., обнародованная за подписью на тот момент замминистра обороны Э. Картера. В правовом смысле документ, рассчитанный на десять лет, вводит в действие положения Национальной космической политики США от 2010 г. и упомянутой выше Стратегии безопасности в космосе от 2011 г., в соответствии с которыми Вашингтон относит устойчивое и свободное использование космического пространства к сфере своих важнейших интересов.

Новые установки Пентагона имеют характер активного сдерживания. Любое целенаправленное вмешательство в деятельность американских космических систем, включая наземную инфраструктуру, будет рассматриваться как прямое нарушение прав США. Вторжение в мирное время будет трактоваться как *безответственный поступок*, попытки вмешательства же в период кризисов могут привести, по образному выражению, к *эскалации*, которая потребует решительных *ответных действий*. При этом американские военные объясняют, что угроза американским средствам в космосе вполне реальна. Утверждается, что ряд государств разрабатывает ПСО, наземные лазеры, системы электронного подавления и т. п. В соответствии с задумками разработчиков, именно для купирования этих рисков в будущем и предназначен новый документ.

Под общую стратегическую задачу подверстывается и соответствующая подробная программа действий. Во-первых, американцы берут курс на поддержку развития международных норм ответственного поведения с целью поддержания *защищенного, стабильного* и *безопасного* космического пространства. Имеется в виду выработка приемлемого для Вашингтона *свода правил* или *кодекса поведения* в космическом пространстве. Возможно, поэтому Вашингтон в январе 2012 г. присоединился к активной поддержке Кодекса поведения в космосе (КПК), продвигаемого Европейским Союзом с 2007 г. в ответ на российскую резолюцию ГА ООН по МТДК 61/75. В результате этого *присоединения* в проекте документа появились положения, явно диссонирующие с его заявленным политико-декларативным характером. Имеется в виду, прежде всего, статья 4.2 Кодекса, в которой, по сути, легитимизируются силовые действия одних государств в отношении космических объектов других государств под предлогом *угрозы жизни людей* или *увеличения космического мусора*. Таким образом, документ рекомендательного характера содержит положения, допускающие односторонние несогласованные действия одних государств в отношении космической собственности других под предлогом самообороны.

Во-вторых, американцы намерены активно продвигать планы по созданию коалиций для обеспечения коллективной безопасности, а также поддержания возможностей для *асимметричного* ответа на нападения в отношении космических средств США и союзников с применением всех элементов национальной мощи. Иными словами, речь может идти о создании в перспективе *космического НАТО*, в рамках которого нападение на одного из участников альянса будет считаться нападением на всех его членов.

И, наконец, в-третьих, в директиве прописана необходимость уменьшения деструктивного воздействия подобных атак за счет повышения *устойчивости, живучести* спутниковых группировок и в целом космических систем даже в случае частичного выведения их из строя.

К слову, в развитие этих установок в конце августа 2013 г. Минобороны США представило программный документ, касающийся выживаемости космических средств военного назначения. В подготовленной ВВС *Белой книге*[7] намечены принципы построения новой спутниковой архитектуры и обосновываются ее преимущества. В Пентагоне, видимо, исходят из того, что на сегодняшний день существует реальная угроза их космическим аппаратам. Это касается как космического мусора, так и противоспутниковых средств.

В документе речь идет о так называемой *стратегии разукрупнения* (disaggregation), призванной сделать пентагоновскую орбитальную группировку более устойчивой к внешнему воздействию. Под этим понимается рассредоточение задач, функций или оборудования между многими системами, находящимися на одной или нескольких орбитах, платформах, аппаратах или в различных средах. Констатируется необходимость качественных перемен для сохранения оперативного преимущества в космосе. Отмечается, что при существующей конфигурации космические силы морально устаревают, поскольку создавались под задачи холодной войны и выполняли прежде всего функции связи, навигации и предупреждения на случай ядерной войны. Резюмируется, что в нынешнем виде космическая группировка весьма уязвима, так как она неповоротлива и слишком зависима от потери даже одного спутника. Предлагается выйти на более гибкую и дешевую группировку космических аппаратов, способную обеспечить нужды военных несмотря на действия неприятеля, воздействие окружающей среды или системные сбои.

Интересен набор практических мер, которые могли бы обеспечить выполнение поставленных задач. Это физическое разделение различных элементов одной космической системы между несколькими КА, способными взаимодействовать друг с другом. Возможно и функциональное распределение, то есть выполнение одной задачи несколькими скоординированными КА. Кроме того, взят курс на размещение американской военной аппаратуры на коммерческих спутниках и КА союзников. Наконец, планируется *разбросать* космические средства по нескольким орбитам, а их задачи дублировать и в других средах, в частности в киберпространстве и на Земле. В Пентагоне, видимо, надеются добиться сразу нескольких целей — упростить космические боевые системы, облегчить их обслуживание, снизить стоимость, усилить инновационный потенциал за счет сопряжения потенциалов гражданского и военного секторов.

На наш взгляд, при этом решается ряд стратегических задач. В их числе следует, прежде всего, отметить сдерживание противника от нападения, так как за счет рассредоточения функций и оборудования между множеством КА должна возникнуть неопределенность в выборе целей. Кроме того, в Пентагоне рассчитывают снизить ущерб для функционирования всей интегральной системы в случае выведения из строя одного или даже нескольких аппаратов.

Таким образом, есть основание говорить о перспективах создания в США *сетевых ударных систем* применительно к военному космическому потенциалу.

Создание внешне разбросанных элементов единой интегрированной системы, которые могут функционировать одновременно в трех плоскостях или пространствах — наземном, космическом и кибернетическом — повышает уровень ее оперативной управляемости в режиме реального времени.

К недавним практическим шагам в этой области следует отнести курс, взятый Пентагоном на создание в течение ближайшего времени Единого центра по обработке данных с военных и разведывательных спутников, который будет выступать фактическим дублером Центра космических операций (ЦКО) минобороны США. Тем самым создаются предпосылки для качественного улучшения координации действий Пентагона и американского разведывательного сообщества. Кроме того, в рамках стратегии *разукрупнения* предусматривается передача полномочий пен-

тагоновского ЦКО коммерческим предприятиям и гражданским структурам, а также готовится целевая комплексная программа защиты и передачи данных между КА.

Как представляется, все эти приготовления вполне укладываются в русло того, что на прошедшем в этом году в США симпозиуме по проблематике геопространственной разведки (geospatial intelligence) американский замминистра обороны Р. Уорк весьма образно охарактеризовал как *важность космической архитектуры для проекции американской мощи и парирования вызовов от растущих российского и китайского космических потенциалов*.

Таким образом, в практическом плане реализуется те принципы, которые были заложены еще в 2001 г. комиссией под руководством Д. Рамсфельда, которая в числе своих рекомендаций американской администрации предлагала *вариант размещения оружия в космосе*[8].

На наш взгляд, это ведет не только к повышению устойчивости военной космической группировки, включая ее перспективные ударные элементы, но — и это представляется главным для целей нашего краткого исследования — создает *предпосылки к повышению потенциала практической применимости боевых космических средств*.

В политическом плане это, на наш взгляд, и представляет собой основной побудительный мотив активного нежелания США и наиболее близких их союзников открыть дорогу практической многосторонней работе по выработке ДПРОК.

Примечания

1 Проект — Договор о предотвращении размещения оружия в космическом пространстве, применения силы или угрозы силой в отношении космических объектов [Электронный ресурс] // Организация Объединенных Наций [офиц. сайт]. URL: http://www.un.org/ru/documents/ods.asp?m=CD/1985.

2 Резолюция Генеральной Ассамблеи ООН A/RES/69/31 *Предотвращение гонки космических вооружений в космическом пространстве* [электронный ресурс] // Организация Объединенных Наций [офиц. сайт]. URL: http://www.un.org/ru/documents/ods.asp?m=A/RES/69/31.

3 Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела [Электронный ресурс] // Организация Объединенных Наций [Офиц. сайт]. URL: http://www.un.org/ru/documents/decl_conv/conventions/outer_space_governing.shtml.

4 Устав ООН [электронный ресурс] // Организация Объединенных Наций [офиц. сайт]. URL: http://www.un.org/ru/documents/charter.

5 2011 National Security Space Strategy (NSSS) [электронный ресурс] // Defense Technical Information Center [офиц. сайт]. URL: http://www.dtic.mil/dtic/tr/fulltext/u2/a536546.pdf.

6 Directive of the United States Department of Defense on Space Policy № 3100.10, October 18, 2012 (Space Directive) [электронный ресурс] // Defense Technical Information Center [офиц. сайт]. URL: http://www.dtic.mil/whs/directives/corres/pdf/310010p.pdf.

7 Resiliency and Disaggregated Space Architectures, White Paper [электронный ресурс] // Air Force Space Command [офиц. сайт]. URL: http://www.afspc.af.mil/shared/media/document/AFD-130821-034.pdf.

8 CRS Report for Congress “Military Space Activities: Highlights of the Rumsfeld Commission Report and Key Organization and Management Issues”, February 21, 2001 [электронный ресурс] // URL: http://www.assets.opencrs.com/rpts/RS2082420010221.pdf.

Андрей Колесников

КРАСНАЯ КНОПКА ИНТЕРНЕТА

«Сегодня телекоммуникации и интернет являются критическими средствами управления государством, фундаментом бизнеса и средством коммуникации между людьми. Важность интернета сложно переоценить», — этой мантрой интернет-бюрократы и чиновники традиционно начинают каждое свое выступление. В этой статье я постараюсь дать простое определение сложных узлов критической инфраструктуры интернета и описать необходимые технические и организационные меры для снижения угроз интернет-инфраструктуре.

ДЕНЬ, КОГДА ГОСУДАРСТВО ОБРАТИЛО ВНИМАНИЕ НА КРИТИЧЕСКУЮ ИНФРАСТРУКТУРУ ИНТЕРНЕТА

Первое серьезное обсуждение критической инфраструктуры интернета на уровне лиц, ответственных за принятие решений, произошло в начале 2009 г. в кабинете заместителя министра связи А. Солдатова. Немногим ранее возросшим влиянием интернета на безопасность озаботился Совет Безопасности России. Мне, как директору *Координационного центра национального домена сети интернет*, вместе с А. Солдатовым, А. Платоновым[1] и рядом других экспертов[2] было поручено определить перечень критических элементов инфраструктуры интернета. Из солидного первоначального списка мы оставили три: DNS-серверы доменной адресации, обслуживающие миллиарды запросов в день, каналы связи и маршрутизация IP-сетей — ключевые составляющие этой основанной на доверии экосистемы[3]. Тогда же, в 2009 г., в контексте обсуждения интернета впервые прозвучало слово *учения*.

В то время в России не было четкого понимания принципов функционирования критической инфраструктуры интернета. Об этом наглядно свидетельствует то, как в 2000-х гг. описывались угрозы. Например, в *Доктрине информационной безопасности Российской Федерации* от 2000 г.[4] технической инфраструктуре, подходящей под определение *интернет,* отводился один абзац: «угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России». В последующем описании этой угрозы всего один пункт имеет отношение к фактически подтвержденным угрозам критической инфраструктуре интернета: «уничтожение, повреждение, радиоэлек-

тронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи». Остальные перечисленные угрозы, такие как «воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации, компрометация ключей и средств криптографической защиты информации», «внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи», «перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации» или даже «использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры» не нашли фактического подтверждения в известных случаях нарушения работы адресной, маршрутной и канальной инфраструктуры интернета в России или других странах.

Вместе с тем, определения из доктрины описывают другие типы атак, направленных не на адресную инфраструктуру и средства маршрутизации, а на конкретные задачи. Например, атаку типа MITM (man in the middle, *атака посредника*)[5], когда подменяются сертификаты безопасности, которыми обмениваются пользователь и интернет-сервер, что делает возможным перехват информации. Замена оригинального сертификата сайта на операторский — довольно распространенная атака в Китае. Однако она не влечет угрозу прекращения работы сети.

За 15 лет принципиальная схема построения инфраструктуры интернета не менялась. Вероятно, не сильно изменится картина и в 2020 г. Тем не менее, сложность и ветвистость Сети возрастает вместе с ролью интернета в нашей жизни. Вероятно, именно поэтому все официальные выступления начинаются с одной и той же мантры.

ОТКЛЮЧИТЬ ИЗВНЕ ИЛИ ИЗНУТРИ?

В конце июля 2014 г. в рамках исполнения поручения Совбеза в министерстве связи и массовых коммуникаций состоялись первые учения по моделированию инфраструктурных угроз интернета. В средствах массовой информации и социальных сетях произошла нешуточная битва между пользователями, опасающимися, что Россия задумала *самоотключиться* от глобальной сети, и технически подкованными специалистами, доказывающими, что моделирование угроз (внешних или внутренних) является нормальной практикой любого ответственного государства или бизнеса[6,7].

В самом деле, планирование и ответственная эксплуатация критических узлов, подготовка регламентов для координации действий всех сторон, вовлеченных в ликвидацию последствий, необходимы вне зависимости от того, вызваны сбои в работе интернета внешними или внутренними причинами.

Для моделирования угроз, а также разработки методов скорейшего восстановления архитектуры, причины, вызвавшие кризис, не важны. Тот факт, что два элемента критической инфраструктуры — генератор файла зоны первичного DNS[8] для выгрузки на корневые серверы DNS и база данных маршрутизации (*Internet*

Routing registry, *IRR*) — размещены на территории США (*ICANN*) и Голландии (*RIPE*) соответственно, зачастую вызывает обеспокоенность у тех, кто опасается политических рисков, но помимо политических конфликтов остается, пусть и малая, вероятность катастрофического физического повреждения инфраструктуры в результате, к примеру, затопления, землетрясения или падения астероида.

Для построения модели угроз и разработки методов снижения рисков будет полезно рассмотреть подробнее критические элементы интернета и построить модели снижения угрозы.

КОРНЕВЫЕ СЕРВЕРЫ ДОМЕННЫХ ИМЕН (ROOT SERVERS)[9]

Доменная адресация построена в строгой иерархии.

В интернете все узлы имеют свой уникальный IP-адрес. Например, 194.67.1.14. Запомнить такие адреса весьма не просто[10]. Поэтому компьютерам, узлам и ресурсам в сети интернет присвоили имена, которые легко запомнить. Система имен DNS отвечает за соответствие доменного имени IP-адресу ресурса и исполняет некоторые другие функции, связанные с адресацией в интернете.

Домен первого уровня, например национальный домен России .RU, отвечает за доменную адресацию в рамках процедур и правил, определяемых национальной регистратурой АНО *Координационный центр национального домена сети интернет*. Домен .GAME принадлежит компании *Uniregistry*. Домен .ORG находится под управлением компании *Public Internet Registry* и так далее. На сегодняшний день в мире используются более тысячи доменов первого уровня, из них порядка 250 принадлежит национальным государствам. Национальные домены верхнего уровня называются ccTLD — country code Top Level Domain. Домены верхнего уровня для общего использования называются gTLD — generic Top Level Domain.

Домены второго и последующих уровней управляются их владельцами. Например, компания *Яндекс* управляет доменами YANDEX.RU, доменами третьего уровня MAPS. YANDEX.RU и MARKET. YANDEX.RU. Количество вложенных уровней не ограничено.

При обращении к интернет-ресурсу по доменному имени подключенное устройство обращается к службе доменных имен DNS и запрашивает IP-адрес, соответствующий этому имени. DNS — весьма динамичная структура. IP-адреса постоянно меняются, но при этом доменное имя остается неизменным.

Серверы DNS в день обрабатывают миллиарды запросов и представляют из себя высоко нагруженную архитектуру серверов, маршрутизаторов и каналов связи. Чтобы максимально быстро обслужить запрос на получение IP-адреса, функции сервера DNS встроены в смартфоны, персональные компьютеры и другие устройства пользователей.

Упрощенная картина архитектуры DNS выглядит так:

- верхний уровень иерархии называется корневым доменом. У него нет формального названия, иногда его обозначают точкой (.). Корневой домен управляется

в рамках исполнения функции IANA корпорацией ICANN и содержит информацию обо всех доменах верхнего уровня. Информация о доменах верхнего уровня размещена на 13 корневых DNS серверах интернета. Эта информация обновляется через *файл корневой зоны*;

- .RU — домен верхнего уровня России, запись с информацией о российских DNS-серверах размещена на корневых DNS-серверах в файле корневой зоны. Внесение изменений в запись осуществляется в рамках функции IANA по заявкам Координационного центра национального домена сети интернет;
- YANDEX.RU — домен второго уровня, таблица с информацией о DNS-серверах Яндекса размещена на серверах RIPN[11]. Внесение изменений в запись на серверах RIPN осуществляются аккредитованными регистраторами. Это российские юридические лица, аккредитованные Координационным центром для регистрации доменов в зонах .RU и .РФ. Информация обо всех доменах второго уровня .RU размещается в *файле зоны .RU.*

В таблице ниже перечислены все 13 корневых серверов, отвечающих за работу системы доменных имен верхнего уровня. Эти серверы обслуживают запросы типа *по какому адресу расположен сервер, отвечающий за функциональность домена .RU?*

Имя хоста	IP адрес	Управление
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	*VeriSign, Inc.*
b.root-servers.net	192.228.79.201, 2001:500:84::b	*University of Southern California (ISI)*
c.root-servers.net	192.33.4.12, 2001:500:2::c	*Cogent Communications*
d.root-servers.net	199.7.91.13, 2001:500:2d::d	*University of Maryland*
e.root-servers.net	192.203.230.10	*NASA (Ames Research Center)*
f.root-servers.net	192.5.5.241, 2001:500:2f::f	*Internet Systems Consortium, Inc.*
g.root-servers.net	192.112.36.4	*US Department of Defense (NIC)*
h.root-servers.net	128.63.2.53, 2001:500:1::803f:235	*US Army (Research Lab)*
i.root-servers.net	192.36.148.17, 2001:7fe::53	*Netnod*
j.root-servers.net	192.58.128.30, 2001:503: c27::2:30	*VeriSign, Inc.*
k.root-servers.net	193.0.14.129, 2001:7fd::1	*RIPE NCC*
l.root-servers.net	199.7.83.42, 2001:500:3::42	*ICANN*
m.root-servers.net	202.12.27.33, 2001: dc3::35	*WIDE Project*

Кроме вышеперечисленных 13 серверов в мире действует более 200 зеркал DNS-серверов, которые обеспечивают скорейший отклик для пользовательских DNS-запросов и обеспечивают устойчивость сети корневых серверов в различных регионах. Серверы-зеркала являются точной копией одного из 13 корневых серверов. В России размещены 7 зеркал, обслуживающих запросы пользователей Рунета: копии J, F, L в Москве, K, I в Санкт Петербурге, L в Екатеринбурге и K в Ново-

сибирске. В ответ на запрос *по какому адресу размещена информация о доменах в зоне .RU?* корневой сервер или один из серверов-зеркал ответят:

Имя хоста	IP адреса
e.dns.ripn.net	193.232.142.17 2001:678:15:0:193:232:142:17
f.dns.ripn.net	193.232.156.17 2001:678:14:0:193:232:156:17
d.dns.ripn.net	194.190.124.17 2001:678:18:0:194:190:124:17
b.dns.ripn.net	194.85.252.62 2001:678:16:0:194:85:252:62
a.dns.ripn.net	193.232.128.6 2001:678:17:0:193:232:128:6

Таким образом, узнав, по какому адресу обслуживается домен .RU, запрос клиента *по какому IP-адресу размещен сервер yandex.ru?* будет решаться на серверах доменных имен RIPN.NET, физически размещенных в АО *Центр взаимодействия компьютерных сетей MSK-IX*[12]. Схема, конечно, весьма упрощенная, потому что подавляющее большинство DNS-запросов клиента не выходит за пределы кэширующего[13] сервера местного провайдера.

УГРОЗА DNS

В файле корневой зоны размещена информация обо всех корневых доменах. Предположим, что в силу каких-либо причин выгрузка файла корневой зоны осуществилась с ошибкой в адресе серверов RIPN.NET или с полным отсутствием записи о серверах, обслуживающих корневой домен .RU. Даже при наличии сверхустойчивой архитектуры DNS нельзя исключать технический сбой при выгрузке уникального файла корневой зоны на все 13 корневых серверов. Выгрузка файла зоны осуществляется автоматически по расписанию или при внесении изменений в запись о доменах верхнего уровня (.RU, .COM, .NET и т. д.) соответствующими регистратурами[14] после многоуровневой проверки операторами в схеме работы функции IANA[15] корпорации ICANN[16].

Контроль корректности записей в файле зоны корневых серверов на постоянной основе осуществляет как минимум один российский оператор — упомянутый выше *MSK-IX*. Принцип контроля очень простой: сверяется содержимое файла корневой зоны старой и новой версии. Если в запись о национальных доменах .RU и .РФ внесены несанкционированные изменения, дежурной смене оператора, работающей в режиме 24x7x365, немедленно отправляется уведомление. Кроме того, контролируется объем изменений записей других корневых доменов. Дело в том, что изменения в файл корневой зоны вносятся не часто, и при превышении установленного параметра автоматически формируется уведомление. Схожий метод проверки достоверности выгружаемого файла зоны также используется для контроля внесенных изменений в записи о доменах второго уровня в национальных доменах России. Например, если объем внесенных изменений в файл зоны .RU, полученный от одного из аккредитованных доменных регистраторов, превышает

пороговый параметр, файл зоны не обновляется, и дежурная смена получает соответствующее уведомление.

Если гипотетически возникает ситуация несанкционированного изменения записи о домене верхнего уровня, информация очень быстро распространяется по всем 13 корневым серверам и по всем их зеркалам. Для снижения риска возникновения такой ситуации действует метод поддержки работоспособности с использованием *двойника* корневого сервера с корректной записью о доменах верхнего уровня России. Далее эффективность метода полностью зависит от координации действий ключевых интернет-операторов России. Если в течение короткого времени запись о доменах не восстановлена на корневых серверах, для восстановления работоспособности нужно направить все DNS-запросы *где информация о доменах в .RU?* всех пользователей на территории России на сервер-двойник. Это можно осуществить путем анализа DNS-трафика на сетях операторов и подмены IP-адреса *истинных корневых серверов* на IP-адрес *двойника*, и сделать это нужно по возможности быстро, чтобы информация на кэш-серверах провайдеров также обновилась.

Уже несколько лет *MSK-IX* эксплуатирует корневой сервер-двойник. Однако в случае возникновения ситуации с несанкционированной записью или ее исчезновением из файла корневой зоны DNS, вероятнее всего, во всем мире возникнут сотни *двойников* DNS-серверов, которые будут обслуживать большинство клиентских запросов пострадавшей зоны.

УГРОЗА НАРУШЕНИЯ МАРШРУТИЗАЦИИ ИЛИ ПОТЕРИ СВЯЗАННОСТИ СЕТИ

Второй угрозой, минимизация которой существенно сложнее, является нарушение маршрутизации российских сетей в глобальном интернете. Необходимо подчеркнуть самый важный аспект, из которого проистекает эта угроза. Дело в том, что маршрутизация в интернете осуществляется силами самих участников интернет-отношений. Говоря проще, в интернет-мире не существует регуляций, аналогичных, например, распределению радиочастот. Выделение блоков IP-адресов для операторов и провайдеров осуществляют региональные регистратуры. Их в мире всего пять:

- *American Registry for Internet Numbers (ARIN)* — для Северной Америки;
- *RIPE Network Coordination Centre (RIPE NCC)* — для Европы, Ближнего Востока и Центральной *Азии;*
- *Asia-Pacific Network Information Centre (APNIC)* — для Азии и Тихоокеанского региона;
- *Latin American and Caribbean Internet Addresses Registry (LACNIC)* — для Латинской Америки и *Карибского региона;*
- *African Network Information Centre (AfriNIC)* — для Африки.

Блоки IP-адресов для России выделяет *RIPE NCC,* некоммерческая организация из Нидерландов. Провайдеры и операторы связи самостоятельно обращаются в *RIPE* для получения адресов IPv4 и IPv6. Регистратура никаким образом не влияет на политики маршрутизации операторов и провайдеров. Повторю: операто-

ры и провайдеры во всем мире сами устанавливают политики маршрутизации, т. е. параметры передачи интернет-трафика между оператором А и оператором Б устанавливают эти два оператора. На глобальном уровне интернет-маршрутизация выглядит как конгломерат политик, установленных участниками интернет-отношений, которые объявляют свои политики маршрутизации во внешний мир. Усложняет эту картину мира динамически меняющийся ландшафт маршрутизации, так как в рамках проводимых работ у операторов и провайдеров в таблицы маршрутизации постоянно вносятся изменения. Они фиксируются базой данных маршрутизации (*Internet Routing Registry* — IRR), которая находится под управлением *RIPE NCC*[17]. Это справочная база данных, которой пользуются все операторы и провайдеры, в том числе для определения своих политик маршрутизации.

Существуют две угрозы, связанные с маршрутизацией. Первая — это так называемый взлом протокола динамической маршрутизации или взлом маршрута (*BGP*[18] *hijack*). Хрестоматийным примером такого взлома стал случай *Пакистан против YouTube*[19]. 22 февраля 2008 г. телекоммуникационный регулятор предписал 70 интернет-провайдерам заблокировать доступ к *YouTube* на территории Пакистана. Метод, которым была осуществлена блокировка, заключался в анонсе маршрута на сеть *YouTube* как ближайшего *сетевого соседа*[20] *Pakistan Telecom* для других провайдеров — *сетевых соседей*. Соответственно для пакистанских провайдеров вся сеть *YouTube* была отправлена *в черную дыру*[21]. При этом *Pakistan Telecom* по ошибке анонсировал этот тупиковый маршрут своему внешнему сетевому соседу *PCCW Ltd* из Гонконга. А тот, в свою очередь, являясь одним из крупнейших инфраструктурных провайдеров в мире, не проверил этот анонс и передал его своим международным пирам[22]. В результате 2/3 пользователей *YouTube* в мире (Азия и государства Тихого океана) были отключены от *YouTube*. Проблему обнаружили быстро, анализ ситуации провела компания *Renesys* (ныне *Dyn*), профессионально и на постоянной основе занимающаяся мониторингом маршрутизации в интернете. Среди сетевых инженеров эта ошибка считается *детской*, но время от времени она происходит — чаще по недосмотру, но не исключены случаи злонамеренного перехвата трафика[23]. Через взлом *BGP hijack* можно направить трафик чужого ресурса через свою сеть и проанализировать состав этого трафика. Это серьезная угроза, но она не приводит к разрушению связанности критической инфраструктуры интернета.

Вторая угроза существенно серьезнее — уничтожение информации о маршрутах в базе данных *IRR*. Информация об исчезновении объекта маршрутизации из базы данных *IRR* распространяется не быстро, но по мере обновления таблиц маршрутизации у провайдеров и операторов удаленная из базы *IRR* сеть перестает быть доступной в других сетях. Это непосредственная угроза инфраструктуре.

Проблемы с *кривыми руками*[24] или злонамеренный перехват маршрута *BGP hijack*, как правило, обнаруживают дежурные инженеры. Для рядового пользователя аномалия может снизить скорость передачи данных или, как в пакистанском случае, сделать ресурс недоступным. Обнаружение неправильного BGP-анонса в режиме реального времени и проверка данных IRR на корректность — весьма непростая задача. Во-первых, нужно иметь список всех автономных систем всех российских участников интернет-отношений. Это тысячи записей операторов связи, провайдеров, хостинговых и инфраструктурных компаний, больших

интернет-площадок (*Яндекс, Mail.ru, Google*), банков и т. д. Во-вторых, большинство участников отношений не особо следит за достоверностью маршрутной информации в базе IRR, в этом у них просто нет необходимости, так как соблюдение правильности маршрутов основано на доверии по цепочке между всеми участниками интернет-отношений. В-третьих, для контроля корректности маршрутов необходимо разместить во всех существенных сетях так называемые *пробники* — небольшой и дешевый программно-аппаратный комплекс, который по расписанию запускает тест маршрутизации в проверяемой сети. Эти *пробники* должны передавать данные на центральный сервер, на котором сравнивается предыдущий маршрут с новым, и делаются выводы о корректности маршрута. Построение системы мониторинга маршрутов — это отдельная сложная задача, которую на сегодняшний день реализовали в *RIPE NCC* и в компании *Dyn* (бывшая *Renesys*). Также мониторингом маршрутов и анонсов сетей занимается отечественная компания *Qrator Labs*.

Для ликвидации *BGP hijack* операторы используют метод изоляции сети, которая анонсирует неправильный маршрут. Одновременно технические специалисты связываются с владельцем сети и сообщают об обнаруженных проблемах. Какого-либо единого механизма взаимодействия всех сетей всех операторов не существует по причине тотальной децентрализации.

Удаление данных о маршрутах сети из базы данных маршрутизации *IRR* — еще более серьезная угроза. На сегодняшний день известны только случаи ошибок, когда владелец сети случайно удалял собственные данные. Случаев злонамеренного использования публичной базы данных маршрутизации *IRR* региональной регистратурой *RIPE NCC* не зарегистрировано.

Для снижения угрозы исчезновения данных из базы маршрутизации *IRR* можно использовать точную копию базы данных маршрутизации *IRR*, которой могли бы пользоваться российские операторы сетей и инфраструктуры — этот метод похож на тот, который используется для снижения риска для корневых DNS-серверов. Эта задача решена частично. По имеющейся у автора информации, системы единого мониторинга маршрутизации российских сетей пока не существует.

УГРОЗА ФИЗИЧЕСКОЙ ИНФРАСТРУКТУРЕ

Главным и максимально эффективным средством отключения интернета является физическое отключение каналов передачи данных, которые используются операторами-провайдерами. Не имеет смысла рассматривать модель, в которой сеть оператора или критического узла интернета соединена с внешним миром только одним каналом связи. Такая архитектура в принципе неприемлема для оператора критической инфраструктуры или ресурса.

Определить, какое место занимает то или иное государство по степени устойчивости интернета к угрозам физического отключения, достаточно просто. Общее правило гласит, что чем больше физически независимых каналов соединяет страну с внешним миром, тем лучше. Большая и разветвленная внутренняя архитектура сети в стране поддерживает устойчивость внутри государства. Единый принцип устойчивости сети таков: чем больше операторов и чем сложнее связи между

ними, тем лучше[25]. Безусловно, сложной архитектурой дорого управлять. Однако в модели, где каждый участник интернет-отношений следит за состоянием своей сети, расходы распределяются сообразно размеру каждой сети. Россия входит в число стран-лидеров по устойчивости инфраструктуры интернета. При этом вызывает опасение, что традиционный охранительный подход к защите чего-либо заключается в укрупнении, слиянии и контроле. Централизация и контроль могут сыграть плохую службу для Рунета. Простая логика диктует ответ на вопрос, что проще сломать: распределенную систему со сложными связями или супероператора, через которого проходит весь трафик?[26]

Лекарством от угрозы физического дисконнекта служит наличие множества точек соединения и разнообразие маршрутов при грамотном планировании сетей и надежной коммуникации между операторами при возникновении кризиса.

DDOS-АТАКА

DDoS-атака **я**вляется самым варварским методом нарушения работы инфраструктуры и ресурсов интернета. DDoS может наносить серьезный ущерб всем без исключения сайтам, финансовым и государственным организациям, хостинговым площадкам и провайдерам облачных сервисов. Также DDoS-атаки предпринимаются на DNS-серверы для отказа в обслуживании пользовательских запросов из-за занятости сетевых и вычислительных ресурсов. Принцип работы DDoS-атак описан достаточно подробно. Можно кратко повторить, что злоумышленник отправляет запрос к открытому для публичного доступа интернет-сервису[27], размещенному на мощной инфраструктурной платформе. В запросе, отправленном компьютером под контролем злоумышленника, например к открытому DNS-серверу или серверу точного времени NTP[28], подставляется IP-адрес получателя, куда сервер должен отправить ответ. Так как запрос о домене или точном времени очень маленький, а размер сообщения-ответа от сервера существенно больше, то имея под рукой несколько тысяч зараженных компьютеров, объединенных в ботнет, несколько открытых серверов могут засыпать ответами хороший кусок инфраструктуры, являющийся целью атаки. Этот метод называется *усиление* (amplification).

Мощную атаку хорошего ботнета на цель в сети немедленно видят многие. Страдает ресурс, на который направлена атака. Страдают магистральные каналы и точки обмена трафиком операторов. Первой реакцией оператора может быть остановка маршрутизации по направлениям, откуда приходит атака. Потом наступает время разбора ситуации и ведется поиск источника атаки. Для этого требуется достаточно плотная координация с *сетевыми соседями*. Сегодня все инфраструктурные операторы федерального уровня имеют механизмы контроля DDoS-трафика. У многих применяется технология очистки трафика. Сейчас на рынке появились достаточно качественные сервисные решения по борьбе с DDoS[29].

Перечисленные три угрозы критической интернет инфраструктуре применительно к России можно свести в таблицу:

Угроза	Степень влияния	Лечение	Координация
Удаление записи о домене .RU на корневых серверах DNS или сетевая изоляция корневых серверов для российских сетей	Очень высокая. Нарушения в адресации сайтов и элементов инфраструктуры в домене .RU	Облачная инфраструктура *двойника* корневого сервера под контролем российской компании	Максимальная. Между всеми участниками интернет-отношений и ответственными ведомствами. Необходимо осуществить подмену адресов корневых серверов DNS на адрес *двойника* в сетях операторов связи федерального значения
Нарушение маршрутизации или потери связанности сети — *BGP hijack*, взлом маршрута	Низкая. Возможен анализ трафика перехватчиком	Повсеместное использование средств мониторинга маршрутов российских сетей и постоянный контроль правильности маршрутов самими операторами	Минимальная. Решается оператором взломанного маршрута
Нарушение маршрутизации или потери связанности — удаление записи о сети в базе данных маршрутизации *IRR*	Высокая. Действует не быстро, но верно. Потеря доступности сетей операторов, включая интернет-ресурсы	Мониторинг записей маршрутов российских операторов. Наличие резервной копии базы данных IRR под управлением российского оператора	Максимальная. Между всеми участниками интернет-отношений и ответственными ведомствами. При выявлении аномалий в маршрутизации — переключение на резервную российскую базу данных IRR
Угроза физической инфраструктуре	Высокая. Мгновенное отключение от интернета целых регионов. При авариях внутри страны — потеря связанности сетей	Чем больше маршрутов и каналов, тем лучше. Заранее продуманные политики маршрутизации между ведущими российскими операторами	Максимальная. Между существенным числом участников интернет отношений и ответственными ведомствами. При возникновении аварий на физической инфраструктуре возникает необходимость переключения на резервные каналы
DDoS-атака	От низкой до высокой	Отражение атаки на пограничных рутерах[30]. Очистка трафика	Средняя. Плотная работа с операторами — сетевыми соседями, от которых *льется* DDoS-трафик

С развитием инструментария для мониторинга элементов критической инфраструктуры интернета каждый оператор по мере сил устанавливает средства контроля собственных критических узлов. Вместе с тем, быть готовым к серьезному кризису означает заблаговременную подготовку сценариев реагирования и регулярные тренировки по их исполнению. Для этого должны быть задействованы многие интернет-игроки, отвечающие за функции критической инфраструктуры. В первую очередь. это касается операторов связи и провайдеров адресной и информационной интернет-инфраструктуры. Главным элементом успешной ликвидации глобальных аварий на интернет-инфраструктуре являются проработанные сценарии и отлаженная координация.

КООРДИНАЦИЯ — ГЛАВНЫЙ ЭЛЕМЕНТ ЗАЩИТЫ ИНФРАСТРУКТУРЫ

Существует два метода координации. Первый, децентрализованный, действует в рамках неформального общения ответственных инженеров операторов связи, провайдеров и операторов интернет-инфраструктуры. При отсутствии катастрофических аварий или злонамеренных отключений эта схема в полной мере реализована в России и других странах.

Второй метод, кризисный, должен быть реализован на государственном уровне, так как разрушительное воздействие на интернет-инфраструктуру государства может быть вызвано весьма серьезными причинами, требующими государственного контроля по определению. Вывод о том, что координация является ключевым элементом схемы противодействия угрозам критической инфраструктуры интернета, достаточно очевиден. Посмотрим, что нам в ближайшее время предложит государство.

Сегодня в России действует несколько центров реагирования на сетевые угрозы. В их число входит *RU-CERT*, старейшая группа экспертов, занимающаяся координацией сетевых угроз в России и за рубежом. Существует государственный *GOV-CERT*, группа в рамках ФСБ, реагирующая на угрозы, связанные с государственными ресурсами в сети интернет. *GIB-CERT* организован компанией *GROUP-IB*, профессионально занимающейся сетевыми инцидентами, взломами и анализом криминальных действий злоумышленников. Также центр реагирования на инциденты работает в Роскомнадзоре. Перечисленные центры работают в рамках неформальных связей с операторами и провайдерами, а также с площадками хостинга и информационными ресурсами. В настоящее время методы взаимодействия интернет-акторов при критических авариях в сети не закреплены правом и нормами. Также ничего не известно о регламентах такого взаимодействия. Хотя в контексте поручения Совета Безопасности подготовка таких регламентов и законодательных актов — это первый и необходимый шаг, который должен быть предпринят со стороны государства.

СКРЫТЫЕ УГРОЗЫ

Стоит вкратце упомянуть другие угрозы сетевой инфраструктуре, о которых часто говорят, но которым нет фактических подтверждений.

Перехват маршрутизации или полное отключение взаимодействия сетей. Теоретически эти действия можно осуществить, имея недокументированные функции

в главных магистральных маршрутизаторах (*задняя дверь*, *back door*). Обладая этой информацией, группа злоумышленников может удаленно выключить интернет в отдельно взятой стране. Ходят не подкрепленные фактами слухи, что таким образом был отключен интернет в Сирии.

Задняя дверь в алгоритме шифрования RSA. Этот стандарт шифрования используется в 99% всех устройств в интернете. Так как стандарт является американским, ходят слухи, что в самом алгоритме существует *закладка*, позволяющая перехватывать и расшифровывать информацию. Этот устойчивый миф, так как закладки бывают не в алгоритме, который легко повторить и проверить. Но они встречаются в *обвязке* к математике — как на аппаратном уровне, так и на уровне программ.

Подводные лодки обрежут оптоволоконные кабели, соединяющие континенты[31]. Эта статья наделала много шума. Но основными реакциями на публикацию были недоумение и смех. Интернетом пользуется весь мир, и разрушение одного такого кабеля не нанесет ущерба отдельно взятой стране.

Несмотря на разнообразие, разветвленность и динамическую маршрутизацию интернет-трафика, угрозы базовой инфраструктуре адресации и маршрутизации, а также риск физического отключения должны быть приняты в расчет при построении моделей противодействия угрозам. Причины, которые могут вызвать глубокий интернет-кризис в отдельно взятой стране, не столь важны для специалистов, в обязанность которых входит ликвидация последствий. Даже полная передача контроля над функциями IANA из-под юрисдикции США в руки прогрессивного мирового интернет-сообщества или под управление правительств не даст 100%-ной гарантии от ошибки в записи в файле корневой зоны DNS. Наличие новых регуляторных требований по наведению порядка с учетом автономных систем российских операторов и крупных интернет-площадок не даст гарантии от удаления блоков сетей из базы данных IRR. База эта основана на добровольной передаче информации о собственных маршрутах участников интернет-отношений. Защита инфраструктуры должна быть основана на глубоком понимании архитектуры и уязвимостей, а также на четких сценариях и отработанных практикой действий главных участников интернет-отношений в России.

Что делать, если перестал работать интернет в городе, в области, в стране? Вероятно, к этому моменту также перестала работать мобильная связь и наблюдаются перебои в работе фиксированной связи. Это непременно приведет к некоторому коммунальному коллапсу, так как системой мобильной передачи данных пользуются различные службы.

Рядовому пользователю придется просто ждать, пока инженеры восстанавливают связь. Инженеры канальной инфраструктуры и специалисты по маршрутизации непременно установят между собой контакт и будут совместно латать бреши в инфраструктуре.

Огорчает, что не существует единого телефонного номера центра реагирования на угрозы интернет-инфраструктуре. Конечно, инженеры сделают все от них зависящее, чтобы восстановить Рунет, воспользовавшись наработанными частными связями. Представляется, что создание единого центра координации и есть главный вывод, который должен получить Совет Безопасности России по результатам

учений 2014 г. Отработки сценариев должны продолжаться с учетом наличия такого центра.

Примечания

1 А. А. Платонов, генеральный директор АО *Технический центр интернет*. Ранее директор РОСНИИРОС, под контролем которого находились серверы домена .RU, — RIPN.NET.

2 Также над вопросом в разное время работали М. Якушев (ICANN), Д. Бурков (RU-CENTER, RIPE). Активное участие в работе группы принимали И. Химченко и О. Чутов из министерства связи.

3 Провайдеры и операторы интернета, не связанные друг с другом контрактными обязательствами, пропускают трафик между пользователями и ресурсами третьих сторон. Это ключевое правило, позволяющее интернету быть глобальным. Фундаментом доверия выступают интернет-протоколы.

4 Доктрина информационной безопасности Российской Федерации, 9 сентября 2000 г. http://www.scrf.gov.ru/documents/5.html

5 Атака посредника, Википедия https://ru.wikipedia.org/wiki/Атака_посредника

6 «Совет безопасности обсудит отключение России от глобального интернета» — Ведомости http://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet

7 «Совет безопасности обсудит отключение России от глобального интернета» — Коммерсантъ http://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet

8 Серверы имен DNS https://ru.wikipedia.org/wiki/DNS-сервер

9 Корневые серверы интернет http://www.root-servers.org/

10 Сегодня имя домена исполняет две функции: адресную и маркетинговую. *Красивые* домены обладают повышенной стоимостью, как часть бренда компаний.

11 RIPN — это английское название АНО *Российский научно-исследовательский институт развития общественных сетей* — РОСНИИРОС.

12 На самом деле RIPN.NET — это не отдельно стоящий сервер, а *облако*, с использованием протокола anycast обеспечивающее кратчайший отклик с точки ближайшего сетевого присутствия. Аналогично устроены и корневые серверы, и серверы обслуживающие национальные домены (.RU, .RS, .AZ и т. п.), и домены общего пользования (.COM, .ORG, .MUSIC и т. п.). Доступность сервиса RIPN.NET — 100%, т. е. перерывов в обслуживании за более чем 20-летний срок работы не было.

13 Кэширующий сервер DNS — сервер, пропускающий через себя DNS-запросы клиентов. Сервер поддерживает актуальную таблицу соответствия имени домена и IP-адреса во всех доменных зонах, тем самым обеспечивая скорейший отклик на запрос клиента из его сети.

14 Администратором (регистратурой) национальных доменов .RU и .РФ является АНО *Координационный центр национального домена сети интернет*

15 Internet assigned numbers authority https://www.iana.org/about

16 Внесение изменений в записи о корневых доменах является частью функции IANA, которую исполняет выделенное подразделение ICANN.

17 RIPE Internet Routing Registry FAQ https://www.ripe.net/manage-ips-and-asns/db/faq

18 Border Gateway Protocol https://ru.wikipedia.org/wiki/Border_Gateway_Protocol

19 Pakistan causes YouTube outage for two-thirds of world http://abcnews.go.com/Technology/story?id=4344105&page=1 ABC news

20 Сетевой сосед — оператор или провайдер, с которым имеется соединение и осуществляется маршрутизация интернет-трафика.

21 В данном контексте *black hole* — распространенный (и весьма варварский) способ фильтрации по IP-адресам.

22 Peer (пир) — примерно то же самое, что и *сетевой сосед*.

23 Someone's Been Siphoning Data Through a Huge Security Hole in the Internet http://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/ — Wired

24 Кривые руки — мягкий и весьма распространенный термин среди технического сообщества.

25 Syria, Venezuela, Ukraine: Internet Under Fire http://research.dyn.com/2014/02/internetunderfire/

26 Минсвязи не допустит повторного массового отключения интернета в Азербайджане http://www.trend.az/business/it/2459139.html

27 Для DDoS-атак используются открытые сервисы DNS и точного времени.

28 Сервер NTP https://ru.wikipedia.org/wiki/NTP

29 Например, *Qrator Labs* http://qrator.net/ru/. В сети *Ростелеком* установлено средство защиты *Arbor* и применяются средства очистки трафика для клиентов.

30 Пограничный маршрутизатор (border router) установлен на границе сети оператора/провайдера и подключен либо к международному провайдеру, либо к точке обмена трафиком с другими операторами.

31 Russian Ships Near Data Cables Are Too Close for U.S. Comfort http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=1

Андрей Баклицкий

ИРАНСКОЕ ЯДЕРНОЕ СОГЛАШЕНИЕ: ПО КАНАТУ БЕЗ СТРАХОВКИ

Октябрьским вечером 1994 г. президент США Б. Клинтон выступил с давно ожидаемым брифингом для СМИ по итогам переговоров между Соединенными Штатами и КНДР. Он объявил собравшимся журналистам, что после шестнадцати месяцев напряженных переговоров Вашингтон и Пхеньян достигли соглашения по ядерной программе Северной Кореи. В обмен на поставку энергоресурсов и строительство двух легководных ядерных реакторов КНДР согласилась вывести из эксплуатации реактор в Йонбене, остановить работы по переработке ядерного топлива и остаться в Договоре о нераспространении ядерного оружия. Президент отметил, что соглашение отвечает интересам США, их союзников и всего мира и особо подчеркнул, что оно «не основывается на доверии. Выполнение [соглашения] будет контролироваться МАГАТЭ»[1].

Текст договора будет подписан в Женеве 21 октября 1994 г. и станет известен как *Рамочное соглашение* между США и КНДР, но его реализация практически сразу столкнется с серьезными сложностями. 10 января 2003 г. Пхеньян объявит о выходе из ДНЯО, а 9 октября 2006 г. проведет свое первое ядерное испытание.

Когда в июле 2015 г. шестерка международных посредников (Великобритания, Германия, КНР, Россия, США, Франция) и Иран согласуют Совместный всеобъемлющий план действий по урегулированию ситуации вокруг иранской ядерной программы, аналогии не замедлят последовать. И пока авторы иранского соглашения будут пытаться убедить внутренних и внешних оппонентов в достоинствах достигнутых договоренностей, экспертное сообщество задастся вопросом, насколько же, на самом деле, устойчивым является соглашение по иранской ядерной программе.

СОВМЕСТНЫЙ ВСЕОБЪЕМЛЮЩИЙ ПЛАН ДЕЙСТВИЙ

Следует начать с того, что история противостояния вокруг иранской ядерной программы длится более десяти лет, и согласованный в июле 2015 г. Совместный всеобъемлющий план действий (СВПД) стал не первой договоренностью, призванной разрешить ситуацию.

Предыдущая попытка датируется маем 2010 г., когда Иран, Бразилия и Турция представили *Тегеранскую декларацию*[2]. Согласно документу, Тегеран должен был передать Анкаре 1200 кг низкообогащенного урана в обмен на поставку 120 кг топлива для Тегеранского исследовательского реактора, обеспеченную МАГАТЭ, США, Францией и Россией. В случае невыполнения соглашения в течение года Турция должна была вернуть Ирану его запас урана. Тем не менее, несмотря на предварительное согласие президента США Б. Обамы и близость положений *Тегеранской декларации* к плану, предложенному Францией, Россией и США годом раньше, соглашение было отрицательно воспринято в Вашингтоне, а после и в других столицах *шестерки*, и так и не было реализовано. Если прибавить к этому срыв договоренностей между *евротройкой* и Ираном в 2003–2004 гг., а также негативный опыт переговоров по ядерной программе КНДР, становится понятно, почему многие в экспертном сообществе встретили попытку достичь всеобъемлющего и окончательного соглашения с Ираном со здоровым скептицизмом.

Главы делегаций на переговорах прекрасно представляли себе эти и другие сложности. Итоговое соглашение должно было продемонстрировать, что все пути для создания Ираном ядерного оружия были закрыты, при этом условия не должны были включать положения, неприемлемые для Тегерана. Соглашение не могло быть международным договором, потому что он никогда бы не был ратифицирован Конгрессом США, и в тоже время оно должно было обладать широкой международной легитимностью и предусматривать инструменты обеспечения выполнения. Соглашение должно было стать компромиссом между крайними позициями Ирана и США и учитывать интересы Великобритании, Германии, Китая, России и Франции. Учитывая столь значительное количество противоречащих друг другу требований, Совместный всеобъемлющий план действий в итоге оказался, пожалуй, наилучшим возможным вариантом.

В общем виде СВПД выглядит следующим образом: Иран значительно сокращает и ограничивает на 10 лет свои обогатительные мощности, уровень обогащения урана в течение 15 лет не должен превышать 3,67%, а его общие запасы — 300 кг. Запасы тяжелой воды также будут ограничены. Обогатительный центр в Фордо будет перепрофилирован в исследовательский центр, а исследовательский реактор в Араке — модернизирован, чтобы избежать излишней наработки плутония.

Иран также обязуется временно применять Дополнительный протокол к соглашению о гарантиях МАГАТЭ (с перспективой его ратификации парламентом), принять положения измененного кода 3.1 Дополнительных положений соглашения о гарантиях МАГАТЭ и будет сотрудничать с МАГАТЭ для прояснения прошлых и настоящих нерешенных вопросов. Тегеран предоставит МАГАТЭ дополнительные возможности для мониторинга и доступ к любым подозрительным объектам, будет предоставлять Агентству информацию о запасах природного урана и центрифугах. В течение 15 лет международное сотрудничество в ядерной сфере будет осуществляться только после одобрения специально созданной Совместной комиссией.

В течение этих же 15 лет Иран не будет перерабатывать отработавшее ядерное топливо, откажется от обладания высокообогащенным ураном и оружейным плутонием, а также ураном и плутонием в металлической форме. Тегеран не будет использовать компьютерные модели для имитации ядерных взрывных устройств,

ЛИСТАЯ СТАРЫЕ СТРАНИЦЫ

С. КИСЛЯК

Мы будем делать все возможное для того, чтобы программа мирного развития ядерной энергетики Ирана развивалась на путях сотрудничества. Это значит, что Иран должен продемонстрировать транспарентность и предсказуемость своей программы и своих намерений. Это также значит, что и Ирану нужно иметь уверенность в том, что не будет помех в поставках оборудования и материалов для развития его мирной ядерной программы.

Надо сказать, что у наших друзей из европейских стран свой диалог с Ираном, но мы отнюдь не сидим в кабинетах и не ждем, чем он закончится. Россия — очень активный участник многосторонних дискуссий вокруг этого вопроса. И мы также очень серьезно по всем этим вопросам самостоятельно, в двухстороннем формате разговариваем с Ираном. И я надеюсь, что, в конечном счете, если мы, наконец, снимем все эти вопросы, мы сами себе сможем сказать, что Россия сыграла в снятии напряженности не последнюю роль, — а это полностью отвечает долгосрочным интересам России.

Иран: ситуация стала понятнее, но не все вопросы сняты
***Ядерный Контроль*. 2005. Т. 11, № 2 (76).**
http://www.pircenter.org/media/content/files/1/13415732140.pdf

многоточечные системы детонации взрыва, системы диагностики взрывов и нейтронные источники взрывного типа. Иран продолжит исследования в области обогащения в ограниченном масштабе, используя в течение 10 лет только газоцентрифужную технологию. Страна подготовит план деятельности в области обогащения урана и сопутствующих исследований. МАГАТЭ будет ежегодно подтверждать соответствие иранской ядерной программы заявленному плану.

Взамен резолюция СБ ООН 2231 отменит все предыдущие санкционные резолюции, связанные с иранской ядерной программой. Евросоюз отменит все односторонние санкции против Ирана. США отменит все санкции, введенные исполнительной властью, и приостановит действие остальных санкций с перспективой их дальнейшего снятия. Выполнение обязательств сторон будет взаимным и будет осуществляться в соответствии со сложным поэтапным планом.

Первое, что бросается в глаза при знакомстве с СВПД, — это объем и сложность текста. Рамочная договоренность между США и КНДР 1994 г., призванная остановить развитие ядерной программы Пхеньяна, состояла из четырех страниц[3]. В те же четыре страницы уместилась рамочная договоренность по уничтожению сирийского химического оружия[4], согласно которой свыше тысячи тонн боевых отравляющих веществ и прекурсоров должны были быть вывезены из страны, находящейся в состоянии гражданской войны. Для сравнения: в Совместном всеобъемлющем плане действий — 20 страниц, а с учетом пяти приложений объем документа превышает 150. По объему и сложности СВПД скорее похож на новый договор СНВ между США и Россией. Тщательная проработанность текста внушает оптимизм относительно устойчивости соглашения при наличии доброй воли к его выполнению.

Второе, что нужно иметь в виду, — несмотря на отмеченную выше сложность, соглашение не является международным договором. Это именно план действий,

согласованный сторонами, но не подписанный, не ратифицированный и не являющийся обязательным к исполнению. Как справедливо отмечает бывший советник по правовым вопросам Совета национальной безопасности и Государственного департамента США Дж. Беллингер, резолюция Совета Безопасности ООН 2231 включает в себя текст СВПД, но не делает его юридически обязывающим[5]. Резолюция только *одобряет* план действий и *настоятельно призывает* к его полному осуществлению, что не является обязывающей формулировкой. В то же время Резолюция 2231 абсолютно четко отмечает как юридически обязывающие («постановляет, действуя на основании статьи 41 Устава Организации Объединенных Наций») отдельные положения СВПД, преимущественно ограничительного характера (повторное введение в силу отмененных резолюций, сотрудничество с Ираном в атомной сфере и т. д.)[6]. Таким образом, выполнение соглашения сторонами в значительной мере было поставлено в зависимость от интересов участников.

Успех СВПД, как и любой другой международной договоренности, не может быть гарантирован. На пути выполнения соглашения стоит множество препятствий. Угрозы выполнению СВПД можно разделить на две основные категории:

- Полный отказ одной из сторон от участия в СВПД по причинам, не связанным с выполнением плана действий. Это, в свою очередь, может спровоцировать распад соглашения;
- Кризис, вызванный противоречиями, которые неизбежно возникнут в ходе реализации СВПД. В случае если механизмы разрешения споров окажутся неэффективными, эскалация кризиса может привести к прекращению действия СВПД.

Данная статья не включает в себя рассмотрение устойчивости СВПД в случае, если Иран пойдет на явное нарушение соглашения и попытается создать ядерное оружие. Подобный сценарий не выглядит сколько-нибудь реалистичным. Вышедший 2 декабря 2015 г. отчет генерального директора МАГАТЭ, посвященный спорным аспектам иранской ядерной программы, подтвердил, что «скоординированная деятельность Ирана, которая могла быть использована для создания ядерного взрывного устройства», прекратилась в 2003 г.[7]. Возобновление военных исследований несмотря на беспрецедентное внимание и контроль со стороны МАГАТЭ едва ли можно рассматривать как вероятную стратегию действий иранского руководства.

Наконец, нужно отметить, что несмотря на то, что Совместный всеобъемлющий план действий носит многосторонний характер, его устойчивость преимущественно зависит от выполнения своих обязательств США и Ираном. Россия и КНР последовательно поддерживали соглашение, при этом обязательства Пекина и Москвы, не вводивших односторонних санкций против Тегерана, в рамках СВПД сводятся к точечным вопросам (модификация Китаем реактора в Араке, модификация Россией двух каскадов центрифуг в Фордо для производства стабильных изотопов и вывоз излишков обогащенного урана из Ирана), их невыполнение не может помешать реализации соглашения. Что касается Великобритании, Германии и Франции, то их действия могут представлять угрозу СВПД только на первом этапе. После того как ЕС снимет с Ирана большую часть санкций, их возможности

саботировать соглашение значительно уменьшатся. Санкции Европейского Союза вводятся и отменяются единогласным решением Совета министров ЕС[8]. В случае если один из европейских участников СВПД решит по внутриполитическим причинам выйти из соглашения, то, чтобы возобновить европейские санкции против Ирана, государству придется убедить в своей правоте 27 других членов Европейского союза, что служит сильным сдерживающим фактором.

СЦЕНАРИЙ 1: *СВЕРХУ ВНИЗ*

Совместный всеобъемлющий план действий был согласован президентами США и Ирана, но в обеих столицах осталось немало недовольных. Враждебные отношения между Тегераном и Вашингтоном на протяжении последних тридцати с лишним лет создали атмосферу взаимного недоверия, отбрасывающую тень и на достигнутое соглашение.

14 июля 2015 г., в день, когда было объявлено о согласовании Совместного всеобъемлющего плана действий *шестеркой* международных посредников и Ираном, спикер Палаты представителей Конгресса США Дж. Бейнер назвал соглашение *неприемлемым* и пообещал не допустить его реализации. Реакция спикера Палаты представителей была отчасти обусловлена позицией ключевого союзника США — премьер-министр Израиля Б. Нетаньяху успел объявить сделку *ошибкой исторического масштаба* — но учитывала и настроения американского электората. В середине июля только 33% населения одобряли соглашение с Ираном, тогда как 45% опрошенных выступали против (к сентябрю соотношение только ухудшится: 21% и 49% соответственно)[9].

В Тегеране новость о достижении договоренности была встречена массовыми гуляниями, но реакция руководства страны была не столь однозначной. Ряд парламентариев поспешили обвинить иранских переговорщиков в игнорировании интересов страны и пересечении обозначенных *красных линий*. Верховный лидер Ирана А. Хаменеи заявил, что текст соглашения должен быть тщательно изучен, а ряд государств, с которыми Иран вел переговоры, не заслуживает доверия.

США

В Соединенных Штатах первоочередной угрозой для всеобъемлющего соглашения с Ираном был Конгресс.

Еще 14 мая 2015 г. обе палаты парламента одобрили *Акт о рассмотрении ядерного соглашения с Ираном 2015 г.*[10] (*Iran Nuclear Agreement Review Act of 2015*). Законопроект, прошедший Палату представителей и Сенат с широкой двухпартийной поддержкой и подписанный Б. Обамой 22 мая 2015 г., обязал президента представить соглашение с Ираном на рассмотрение парламента и последующее голосование. Согласно новому закону, снятие санкций с Тегерана могло быть заблокировано совместной резолюцией палат Конгресса, не одобряющей СВПД.

При этом подавляющая поддержка законопроекта в парламенте вовсе не отражала общего неодобрения соглашения с Ираном американскими законодателями.

Поддержку закону обеспечило совместное голосование ряда групп с различными, зачастую противоположными интересами: радикального крыла республиканской партии, готового противостоять любым инициативам президента, республиканцев и демократов, опасающихся заключения *плохой* сделки, и сторонников соглашения, *покупающих* время, необходимое для завершения международных переговоров.

К маю 2015 г. иранский вопрос успел получить четкое *партийное* измерение. В нарушение установленного порядка республиканцы *через голову* демократической Администрации пригласили премьер-министра Израиля выступить перед Конгрессом, чем подлили масла в огонь. Несмотря на внутренние противоречия, межпартийное противостояние требовало от конгрессменов-демократов поддержать соглашение, подготовленное Администрацией. Таким образом, против договоренностей шестерки международных посредников и Ирана с неизбежностью должно было выступить республиканское большинство Конгресса. Демократическая поддержка обещала быть минимальной. Вероятность успеха была далека от стопроцентной.

Чтобы вступить в силу, совместная резолюция, как и любая инициатива законодателей, должна была не только получить большинство в обеих палатах парламента, но и быть подписанной президентом. Б. Обама неоднократно заявлял, что наложит вето на любое действие парламента, встающее на пути реализации соглашения. Это означало, что конгрессмены должны были готовиться преодолеть президентский запрет. В итоге, дело не дошло и до этого — противодействие демократов в Сенате в итоге похоронило угрозу СВПД со стороны законодательной власти.

Согласно правилам процедуры верхней палаты парламента США, сенаторы могут отложить голосование по законопроекту, пользуясь правом на неограниченные дебаты, известным как *флибустьерство*. В подобном случае для того, чтобы просто вынести документ на голосование, необходимы голоса трех пятых состава Сената. Республиканцы верхней палаты трижды пытались провести голосование по соглашению с Ираном и трижды не набирали необходимых 60 голосов. 17 сентября 2015 г., в последний день, когда, согласно майскому закону, Сенат мог одобрить или отклонить соглашение, 45 сенаторов-демократов выступили против вынесения вопроса на голосование, фактически сняв соглашение с Ираном с повестки дня.

В обозримом будущем Конгресс едва ли сможет отменить соглашение по иранской ядерной программе. Совместный всеобъемлющий план действий стал ключевым внешнеполитическим достижением демократической Администрации. В резко поляризованной по партийному признаку вашингтонской среде большинство конгрессменов-демократов будет вынуждено защищать соглашение от республиканских атак. Что касается изменения состава парламента, которое позволило бы республиканцам игнорировать оппозицию демократов, то это едва ли представляется возможным. Даже в чрезвычайно ослабленном состоянии (по итогам выборов 2014 г. республиканцы получили большинство в Конгрессе, которого партия не видела с 1929 г.[11]) демократы в Сенате успешно блокировали законопроекты большинства. Дальнейшее снижения демократического представительства в парламенте было бы аномалией, более реалистичен обратный тренд. На ближайших выборах в Конгресс 8 ноября 2016 г. будет переизбран весь состав Палаты пред-

ставителей и треть Сената. Учитывая, что в Сенате будут разыгрываться 24 места, занимаемых республиканцами, и только 10 демократических, вполне реалистично ожидать усиления демократов в верхней палате.

В то же время другая потенциальная угроза участию Соединенных Штатов в СВПД исходит от Администрации страны. На текущий момент исполнительная власть и лично президент Б. Обама являются главными сторонниками соглашения с Ираном в США. Администрация готова использовать свои полномочия приостанавливать действие санкций для реализации СВПД, мобилизовать демократов в Конгрессе в поддержку своего амбициозного проекта и инвестировать в соглашение значительный политический капитал.

Столкнувшись с сильным двухпартийным давлением со стороны парламента, настаивающего на участии в оценке сделки с Ираном, президент Б. Обама прибегнул к тактическому отступлению. Он согласился поддержать закон, согласно которому итоговое соглашение вносилось на голосование в Конгресс, что дало американским дипломатам возможность завершить переговоры, не опасаясь саботажа со стороны парламента. Президент разумно решил, что защищать готовый текст соглашения, подписанный иранской стороной, поддержанный европейскими союзниками, Россией и КНР, и одобренный резолюцией Совета Безопасности ООН (пусть и не вступившей в силу), будет значительно проще.

В борьбе за соглашение Б. Обама также опирался на поддержку иностранных лидеров. Одобрение со стороны Британии, Германии и Франции — ключевых партнеров США по НАТО — помогало президенту противостоять обвинениям в том, что соглашение с Ираном заключается в ущерб американским союзникам. В январе 2015 г. министры иностранных дел трех стран и Высокий представитель ЕС по иностранным делам Ф. Могерини в совместной статье обратились к Конгрессу с просьбой не вводить новые санкции против Тегерана. В мае послы европейских держав предупредили, что в случае отказа от соглашения режим санкций будет все больше ослабляться. Наконец, 10 сентября 2015 г. премьер-министр Великобритании, канцлер Германии и президент Франции опубликовали в газете *Washington Post* совместную статью с призывом к Конгрессу поддержать соглашение с Ираном[12].

Приближение президентских выборов ноября 2016 г., по итогам которых в Белом доме должна появиться новая Администрация, означает критический момент для участия США в СВПД. В случае сохранения Белого дома за демократами соглашению по иранской ядерной программе ничего не угрожает. Оба ключевых кандидата от демократической партии — бывший Госсекретарь Х. Клинтон и сенатор Б. Сандерс — поддерживают СВПД.

В то же время все ведущие республиканские кандидаты высказали свое негативное отношение к соглашению с Ираном. Сенаторы М. Рубио[13] и Т. Крус[14] в случае своего избрания готовы сразу отказаться от СВПД и возобновить санкции против Тегерана. Другие кандидаты от республиканской партии настроены менее радикально, миллиардер Д. Трамп заявил в сентябре 2015 г., что «никогда в жизни я не видел сделки, подготовленной столь неумело, как наше соглашение с Ираном», но в дальнейшем СВПД не играл сколько-нибудь заметной роли в его кампании. Для части республиканских кандидатов соглашение с Ираном не относит-

ся к списку приоритетов, нужно также учитывать, что позиции кандидатов часто смягчаются после вступления в должность. В этом случае многое будет зависеть от состава новой Администрации, внутри- и внешнеполитического положения США в конце 2016 г. Тем не менее, как показал пример Договора об ограничении систем противоракетной обороны 1972 г., новая Администрация Соединенных Штатов может выйти даже из полноценного международного соглашения по контролю над вооружениями в случае, если считает его невыгодным для себя.

ИРАН

Исламский консультативный совет (Меджлис) — однопалатный парламент Ирана — известен своей независимостью от исполнительной власти и стремлением к надзору за последней. Не стали исключением и отношения между Меджлисом и администрацией президента Х. Роухани. В августе 2013 г. депутаты отклонили кандидатуры на пост глав трех министерств, представленных президентом на утверждение парламента, а год спустя отправили в отставку министра науки, исследований и технологий (утвердить нового главу министерства удалось только с третьей попытки). Переговоры по ядерной программе Тегерана ожидаемо оказались под пристальным вниманием парламента.

Еще до заключения *политического* соглашения в Лозанне иранские парламентарии неоднократно заявляли, что итоговая договоренность по ядерной программе должна быть вынесена на голосование в Меджлисе. При этом они ссылались на статью 77 конституции Ирана, согласно которой «Договоры, соглашения и иные международные документы должны проходить ратификацию в Меджлисе исламского совета». Не последнюю роль в решимости иранских парламентариев играл пример их американских коллег, настаивавших и настоявших на обязательном одобрении будущего соглашения Конгрессом.

Представители исполнительной власти во главе с президентом Ирана Х. Роухани предпочли бы, чтобы СВПД одобрил Высший совет национальной безопасности. Возглавляемый президентом орган включает в себя глав трех ветвей власти, ключевых министров, председателя Генерального штаба и двух представителей Верховного лидера. Решения совета вступают в силу после их утверждения лидером страны. Согласно конституции Ирана, к ведению совета относится «определение политики страны в области обороны и безопасности». До 2013 г. Высший совет национальной безопасности играл ключевую роль в переговорах по ядерной программе, а секретарь совета был главным иранским переговорщиком (в 2003–2005 гг. в этом качестве выступал будущий президент Х. Роухани), поэтому утверждение соглашения по ядерной программе вполне вписалось бы в существующую практику.

Но уже 3 сентября 2015 г. на встрече с представителями Совета экспертов Верховный лидер Ирана А. Хаменеи сказал: «У меня нет рекомендаций для парламента относительно того, как его члены будут рассматривать соглашение, будут ли они ратифицировать его или отклонят его. Это должны решать парламентарии»[15]. На следующий день глава парламентской комиссии А. Р. Закани объявил, что согласно решению Совета стражей конституции, высшего контрольного органа Ирана, законопроект, одобряющий СВПД, должен быть внесен в парламент.

Тем не менее, когда 13 октября 2015 г. парламент Ирана вынес на голосование законопроект под названием *Пропорциональный и взаимный план действий по выполнению СВПД*, он был принят с комфортным перевесом (161 голос *за*, 59 *против*). Согласно закону[16], Высший совет национальной безопасности должен следить за соблюдением взаимности при выполнении СВПД; в случае если санкции не будут сниматься вовремя, будут вводиться повторно или будут инициированы новые санкции, правительство должно прекратить выполнение своих обязательств и нарастить ядерную программу; кроме того, разрешение на посещение военных объектов инспекторами МАГАТЭ должно выдаваться Высшим советом национальной безопасности. На следующий день законопроект был утвержден Советом стражей конституции и стал законом.

Часть консервативных парламентариев раскритиковала действия спикера Меджлиса А. Лариджани, не предоставившего, по их мнению, достаточно времени для обсуждения и внесение поправок в столь важный законопроект. Но в целом, соглашение по иранской ядерной программе было поддержано Меджлисом. Угроза существованию СВПД со стороны иранского парламента на ближайшее время исчезла.

По итогам парламентских выборов февраля 2016 г. можно ожидать усиления в Меджлисе умеренных сил и ослабления консерваторов, что приведет к росту поддержки президента Х. Роухани и политики администрации в ядерной сфере. Текущий состав парламента был избран весной 2012 г., когда и внутренняя, и внешняя политика Ирана способствовали победе консервативных сил: либеральное движение было разобщено и ослаблено в результате протестов 2009–2010 гг., президентом страны был консервативно настроенный М. Ахмадинежад, Европейский Союз готовился ввести против Тегерана нефтяное эмбарго, а в западных столицах не исключали военного решения ситуации вокруг иранской ядерной программы. В 2016 г. разрядка в международной напряженности и успехи администрации могут помочь получить более либеральный и дружественный президенту Х. Роухани парламент.

Поддержка следующих созывов Меджлиса будет важна при наступлении этапа СВПД, следующего за *Переходным днем*. Соглашение предусматривает, что с наступлением *Переходного дня* Иран «приложит, действуя в соответствии с конституционным распределением полномочий между президентом и парламентом, усилия в целях ратификации Дополнительного протокола».

Как видно из предыдущей цитаты, ратификация протокола иранским парламентом не является обязательным условием для выполнения СВПД. При этом нужно учитывать, что Тегеран уже применял Дополнительный протокол добровольно в 2003–2006 гг., после чего прекратил его применение, резко снизив возможности МАГАТЭ по верификации мирного характера своей ядерной программы. В этом контексте ратификация Дополнительного протокола стала бы важным символом устойчивости соглашения и готовности Ирана гарантировать мирный характер своей ядерной программы в долгосрочной перспективе.

При этом, несмотря на важную роль Меджлиса, его позиция по соглашению является важной, но не решающей. В рамках политической системы страны итоговое решение по всем ключевым вопросам остается за Верховным лидером.

Согласно Конституции Ирана, Верховный лидер является главой государства и обладает широким набором полномочий, включая «определение общей политики государства», «контроль за [ее] правильным исполнением» и «решение споров и упорядочение отношений между тремя ветвями власти». На практике нынешний Верховный лидер А. Хаменеи редко вмешивается в решения ветвей власти лично, предпочитая обозначать границы, в рамках которых непосредственные исполнители могут действовать по своему усмотрению, и использовать существующую в Исламской республике разветвленную систему сдержек и противовесов для поддержания баланса.

Отношение Верховного лидера к переговорам по ядерной программе Ирана укладывается в этот общий тренд. Ведение переговоров было бы невозможно без одобрения аятоллы Хаменеи, при этом у него не было причин не доверять президенту Х. Роухани, который на протяжении 24 лет был представителем Верховного лидера в Высшем совете национальной безопасности. На всем протяжении переговоров по ядерной программе Тегеран Верховный лидер обозначал свою поддержку иранским дипломатам, но призывал не преувеличивать важность договоренностей с Западом для будущего страны.

А. Хаменеи также регулярно обозначал *красные линии* для переговоров, которые создавали журналистские сенсации, но на практике либо успешно учитывались в тексте соглашения, либо аккуратно обходились. Поскольку заявления аятоллы А. Хаменеи часто звучали в преддверии ключевых этапов переговоров, западные эксперты задавались вопросом, не играет ли Верховный лидер *злого полицейского*, усиливая позиции команды иранских переговорщиков. Вот лишь несколько примеров:

- За две недели до 20 июля 2014 г., очередной даты, установленной для заключения всеобъемлющего соглашения, Верховный лидер заявил, что Ирану необходима обогатительная программа мощностью в 190 000 единиц работы разделения. Поскольку на тот момент Организация по атомной энергии Ирана обладала ресурсами примерно в 10 000 единиц работы разделения, подобная цель потребовала бы двадцатикратного наращивания обогатительных мощностей. Впрочем, в самой речи А. Хаменеи пояснил, что заявленная цифра будет нужна «не в этом году и не через пять лет».[17] В итоге Тегеран согласился ограничить свою обогатительную программу пятью тысячами единиц работы разделения на десять лет.
- После заключения *политической* договоренности весной 2015 г. Верховный лидер четко обозначил, что санкции с Ирана должны быть сняты в момент вступления соглашения в силу. Поскольку договориться с США и ЕС о снятии санкций без предварительного выполнения ряда условий не представлялось возможным, была выработана система, при которой вступлению соглашения в силу предшествовал ряд этапов, в рамках которых стороны *готовились* к выполнению своих обязательств. Иран приводил свою ядерную программу в соответствие с согласованными параметрами, а западные страны принимали постановления об отмене санкций, вступавшие в силу после выполнения Тегераном его части сделки.

- В конце мая 2015 г. А. Хаменеи спровоцировал бурное обсуждение, заявив, что Иран не позволит интервьюировать своих ученых-ядерщиков, не предоставит доступ к военным объектам и не потерпит *чрезвычайных мер проверки*. Поскольку два первых пункта являлись ключевыми в готовящемся СВПД, возник вопрос о принципиальной возможности соглашения с Ираном. В итоге иранская сторона на переговорах сделала упор на том, что посещение военных объектов и интервью с учеными должны быть ограничены рядом условий. Внутри страны иранские дипломаты разъяснили, что подобные меры проверки являются стандартной частью Дополнительного протокола к соглашению о гарантиях МАГАТЭ, действующего во многих странах, и не будут *чрезвычайными*.

- После того как СВПД был поддержан иранским парламентом, Верховный лидер в письме на имя президента Х. Роухани от 21 октября 2015 г. обозначил, что модификация тяжеловодного реактора в Араке и вывоз обогащенного урана из страны в обмен на природный уран могут начаться только после того, как МАГАТЭ объявит о полном закрытии всех вопросов к Ирану, включая вопрос о так называемом *возможном военном измерении* иранской ядерной программы[18]. Поскольку согласно СВПД разрешение вопросов о *возможном военном измерении* не являлось условием для снятия с Ирана санкций, это требование грозило усложнить структуру реализации соглашения. Несомненно, эта позиция учитывалась представителями *шестерки* при подготовке и принятии резолюции Совета управляющих МАГАТЭ, *закрывшем* иранское ядерное досье 15 декабря 2015 г.[19]

В том же письме А. Хаменеи максимально полно представил свою позицию относительно итогового текста СВПД и его выполнения. Верховный лидер одобрил заключенное соглашение, но с оговорками, ключевой из которой стала следующая:

- В течение восьми лет введение любых санкций против Ирана любой из стран *шестерки* международных посредников будет расцениваться как нарушение СВПД, и в этом случае правительство должно будет прекратить выполнять свою часть соглашения и начать наращивать ядерную программу в соответствии с законом.

Этот пункт, появлявшийся до этого в разных формах, поставил под угрозу само существование соглашения в случае введения против Тегерана новых санкций. Последнее нельзя исключить. В случае ареста американского журналиста в Иране или столкновений Израиля с союзной Тегерану *Хезболлой* могут последовать новые западные санкции на основании обвинений в нарушении прав человека или спонсировании терроризма.

Впрочем, как показывает опыт, Верховный лидер готов гибко подходить к формальным критериям в случае, если ключевые интересы страны будут учтены. Снятие с Ирана многосторонних и односторонних санкций в ходе выполнения СВПД с высокой долей вероятности трансформируется в экономический рост и повышение благосостояния населения страны. В этом случае А. Хаменеи будет сложнее пойти на шаги, которые будут расценены как намеренное ухудшение экономического положения страны. Ему придется соизмерять экономический и репутацион-

ный ущерб от введенных санкций с возможными потерями в случае срыва соглашения по ядерной программе.

СЦЕНАРИЙ 2: *СНИЗУ ВВЕРХ*

Хотя сценарий, при котором одна из сторон полностью отказывается от выполнения соглашения, по-прежнему нельзя исключить, после голосования в парламентах США и Ирана он на некоторое время отошел на второй план. С началом выполнения плана действий самой значимой угрозой соглашению становится нарушение положений СВПД одной из сторон (или обвинение в подобном нарушении) и следующая за этим реакция.

ПЛАН В ПЛАНЕ

Совместный всеобъемлющий план действий был презентован международному сообществу как ряд последовательных этапов, основанных на взаимных уступках. Как отметил 14 июля 2015 г. министр иностранных дел России С. Лавров, «договоренность Ирана и *шестерки* была достигнута с помощью предложенного Президентом РФ В. Путиным принципа поэтапности и взаимности»[20]. Действительно, важная часть СВПД отведена последовательности реализации его положений, а в тексте соглашения фигурирует множество реперных точек. Для определения устойчивости соглашения важно понимать суть и взаимную зависимость этапов СВПД.

Первой датой, отмеченной в плане действий, стало 14 июля 2015 г. — согласно терминологии СВПД, *День окончания* (*Finalisation Day*) переговоров. Затем, в полном соответствии с СВПД, 20 июля 2015 г. Совет Безопасности ООН принял резолюцию 2231, одобрившую план действий.

После того как прошло 90 дней после принятия резолюции Советом Безопасности, а государства-участники не выразили своего несогласия с принятыми договоренностями, 18 октября 2015 г. наступил *День принятия* (*Adoption Day*), и начался второй этап СВПД. С этого дня стороны начали практические приготовления к выполнению своих обязательств согласно плану действий. США и Европейский союз начали готовить документы, снимающие санкции с Ирана либо приостанавливающие их действие. Тегеран приступил к сокращению своей ядерной программы и приведению ее в соответствие с СВПД.

Следующей и, пожалуй, наиболее важной точкой плана действий должен стать *День начала реализации* (*Implementation Day*), знаменующий начало третьего этапа СВПД. В этот день МАГАТЭ должно представить доклад, подтверждающий выполнение Ираном своих обязательств по ограничению ядерной программы. Параллельно ЕС и США отменяют либо приостанавливают большую часть односторонних санкций против Ирана. Также прекращается действие всех предыдущих резолюций Совета Безопасности ООН, введенных в отношении ядерной программы Тегерана[21]. У *Дня начала реализации* нет фиксированной даты, его наступление зависит от выполнения Ираном своей части СВПД и верификации этого МАГАТЭ.

Отдельно будут сняты ограничения на поставки Тегерану вооружений, определенных Регистром обычных вооружений ООН (не позже, чем через пять лет после даты принятия СВПД), и ведение деятельности, связанной с разработкой и созданием баллистических ракет (не позже, чем через восемь лет после даты принятия СВПД).

Через 8 лет после *Дня принятия* либо когда Генеральный директор МАГАТЭ представит Совету управляющих и СБ ООН доклад, констатирующий, что Агентство пришло к *расширенному* заключению о том, что весь ядерный материал в Иране остается в мирной деятельности, наступит *Переходный день* (*Transition Day*). Начиная с этого дня Европейский Союз прекратит действие всех ранее приостановленных санкций и приостановит действие оставшихся, США приложат усилия для принятия законодательных мер, необходимых для прекращения действия санкций, а Иран приложит усилия для ратификации Дополнительного протокола.

Наконец, спустя десять лет после *Дня принятия* наступит *День прекращения действия резолюции СБ ООН* (*UNSCR Termination Day*). Как следует из названия, в этот день прекратится действие резолюции СБ ООН 2231, а Совет Безопасности завершит рассмотрение ситуации вокруг иранской ядерной программы.

Впрочем, выполнение СВПД на этом не заканчивается, значительная часть обязательств Ирана останется в силе на протяжении пятнадцати лет, а некоторые меры продлятся двадцать (предоставление МАГАТЭ данных по производству центрифуг) и даже двадцать пять лет (предоставление МАГАТЭ данных по приобретению и добыче природного урана).

Как видно из вышеприведенной информации, фактически СВПД состоит из двух основных этапов: до *Дня начала реализации*, когда стороны работают над выполнением своих обязательств согласно плану действий, и после *Дня начала реализации*, когда с Ирана будут сняты санкции в обмен на ограничения в ядерной сфере, которые также будут постепенно отменяться. Остальные этапы СВПД, при всей важности их соблюдения, служат обрамлением этой ключевой структуры.

ПЕРВАЯ ПРОВЕРКА НА ПРОЧНОСТЬ

Таким образом, ближайшей точкой для *замера* устойчивости СВПД станет приближающийся *День начала реализации*. Иран должен будет завершить выполнение достаточно объемного плана работ, а МАГАТЭ — проверить и подтвердить выполнение договоренностей. Хотя, как упоминалось выше, сроки выполнения обязательств не фиксированы, Иран будет стремиться к скорейшему завершению своей части работ, чтобы добиться снятия санкций. Стоит ожидать, что президент Х. Роухани, избранный под лозунгом нормализации экономической ситуации в стране, приложит для этого все усилия. 14 октября 2015 г. в интервью иранскому телеканалу президент объявил, что санкции будут сняты с Ирана через один-два месяца[22].

Обозначенные им сроки были мало реалистичными, но подчеркивали важность временного фактора. 26 февраля 2016 г. в Иране пройдут парламентские выборы, которые могут позволить президенту увеличить свою поддержку в парламенте. На ту же дату приходятся выборы в Совет экспертов (орган, избирающий нового Верховного лидера Ирана), будущий созыв которого проработает до 2024 г. Сня-

тие санкций с Тегерана до конца февраля 2016 г. стало бы мощным фактором поддержки для пропрезидентских сил на предстоящих выборах.

Обязательства Ирана в рамках первого этапа выглядят значительными, но вполне выполнимыми. Помимо прочего Тегеран должен снять и залить бетоном корпус реактора в Араке, обеднить или вывезти из страны превышающие 300 кг запасы урана, обогащенного не более чем до 3,67%, ликвидировать запасы урана, обогащенного свыше 3,67%, вывезти из страны излишки тяжелой воды, превышающие 130 метрических тонн, демонтировать центрифуги свыше согласованного количества в 5060 машин типа IR-1 и элементы инфраструктуры, не относящиеся к этим центрифугам, вывезти все ядерные материалы с завода по обогащению ядерного топлива в Фордо, представить МАГАТЭ первоначальный список всех существующих труб роторов центрифуг и сильфонов и разрешить МАГАТЭ проверять этот список, заявить все места и виды оборудования, используемые для их производства.

Иран активно приступил к выполнению своих обязательств в рамках СВПД. Согласно отчету Генерального директора МАГАТЭ от 18 ноября 2015 г.[23], за месяц выполнения СВПД Тегеран сократил количество центрифуг на обогатительном комплексе в Натанзе с 15 420 до 11 308. Работая с той же скоростью, иранские специалисты могут завершить данную часть проекта в январе 2016 г.

Другими трудоемкими пунктами плана остаются вывоз из Ирана излишков низкообогащенного урана и тяжелой воды, а также демонтаж и заливка бетоном корпуса реактора в Араке. Вывоз излишков урана иранская сторона будет координировать с Россией, а демонтаж корпуса реактора — с КНР и США. По заявлению заместителя министра иностранных дел России С. Рябкова, Россия может завершить вывоз урана из страны до конца 2015 г.[24] По информации из российских и иранских источников, завершения необходимых работ в Араке можно ожидать в конце декабря 2015 г. — начале января 2016 г.[25]

После того как Совет управляющих МАГАТЭ закрыл имевшиеся ранее вопросы относительно иранской ядерной программы, не осталось политических аспектов, которые могли бы помешать выполнению Тегераном своих обязательств в рамках СВПД. На данном этапе также не стоит ожидать разночтений относительно реализации Ираном своей части плана действий, она довольно легко верифицируется МАГАТЭ. Если после выполнения Ираном оговоренных пунктов плана ЕС и США выполнят свои обязательства по снятию санкций, что представляется вполне вероятным (ЕС и США завершили всю необходимую подготовительную работу 18 октября 2015 г.[26]), СВПД перейдет в фазу соблюдения за ходом выполнения соглашения, которая будет длиться многие годы.

NEW NORMAL

После *Дня начала реализации* в истории иранской ядерной программы начнется новый этап. В обмен на снятие и приостановку санкций Иран примет на себя ряд обязательств и ограничений, превышающих договоренности промежуточного соглашения от ноября 2013 г., выполнявшиеся Тегераном до того. Полный список обязательств, принятых иранской стороной, приведен в Приложении I к СВПД[27].

Авторы СВПД приложили значительные усилия, чтобы максимально четко прописать обязанности сторон в рамках соглашения и обеспечить МАГАТЭ возможностью их полной и своевременной верификации.

Так, ограничения, касающиеся количественных показателей (количество центрифуг и их компонентов, запасы обогащенного урана и тяжелой воды), легко поддаются контролю. Поскольку обладание дополнительной сотней или даже тысячей центрифуг принципиально не изменит технические возможности Тегерана, а Агентство с легкостью сможет обнаружить нарушение, едва ли стоит ожидать от Ирана умышленного превышения согласованных уровней. В любом случае, они будут сняты по прошествии четко ограниченного периода.

Это, конечно, не исключает возможности неумышленного превышения Тегераном некоторых показателей. В частности, необходимость поддерживать уровень низкообогащенного урана (НОУ) на уровне в 300 кг представляет собой непростую задачу с учетом сложности координирования обогащения урана, производства и облучения топлива, а также разубоживания или вывоза из страны излишков. Кроме того, нельзя исключить, что даже небольшое превышение Ираном оговоренных запасов НОУ может вызвать резкую реакцию у противников СВПД. В этом случае важно понимать, что временное превышение лимита на несколько килограммов не представляет никакой угрозы. В частности, МАГАТЭ определяет *значимое количество* низкообогащенного урана в 75 кг[28], колебание значений ниже данного уровня не должно считаться критичным.

В тоже время ряд сфер деятельности в рамках СВПД оказался не столь однозначно определенным. Принятие решений относительно доступа инспекторов МАГАТЭ к иранским объектам и определение допустимости сотрудничества с Ираном в ядерной сфере будет зависеть от каждого конкретного случая. Выносить итоговые заключения будет Совместная комиссия, состоящая из представителей *шестерки* международных посредников, Ирана и ЕС. Именно в этих сферах стоит ожидать наибольших угроз для выполнения СВПД.

Согласно СВПД, МАГАТЭ имеет право запрашивать доступ к любым объектам на территории Ирана, «чтобы проконтролировать отсутствие незаявленных ядерных материалов и видов деятельности или видов деятельности, не соответствующих СВПД». Если Иран не сочтет доводы МАГАТЭ достаточно вескими и в течение 14 дней Агентство и Тегеран не смогут разрешить вопрос, он будет вынесен на заседание Совместной комиссии. В течение 7 дней комиссия примет решение консенсусом либо большинством голосов. Иран будет должен исполнить решение в течение трех дней.

Учитывая, что необходимым минимумом для принятия решения комиссией будут являться голоса пяти из восьми членов, при совместном голосовании представители Запада (Великобритания, Германия, США, Франция и ЕС) всегда будут обладать нужным большинством. В случае если Иран будет считать посещение какого-либо из военных объектов неприемлемым из соображений секретности, поддержка подобного требования только западными странами может укрепить подозрения в политической подоплеке запроса МАГАТЭ. В этом случае правительству Ирана будет сложно дать разрешение на посещение объекта, что, в свою очередь, будет считаться нарушением СВПД.

Международное сотрудничество Тегерана в ядерной сфере также будет поставлено под контроль Совместной комиссии. Для оперативной работы в рамках СВПД предусмотрена Рабочая группа по закупкам, состоящая из представителей семи государств под председательством ЕС[29]. Рабочая группа должна рассматривать и одобрять (или не одобрять) поставку Ирану товаров и оказание услуг в ядерной сфере. Решения будут приниматься консенсусом в срок, не превышающий тридцати дней. Охват товаров и услуг, относящихся к кругу ведения Рабочей группы по закупкам, очень широк и представляет собой два списка Группы ядерных поставщиков (ГЯП): исходный список ГЯП и список оборудования, материалов, программного обеспечения и соответствующей технологии двойного назначения[30], а также любые другие товары, если государство-экспортер «определяет, что они могут способствовать деятельности, не совместимой с СВПД». На настоящий момент сложно оценить масштаб работы, который встанет перед Рабочей группой, но учитывая включение в список материалов двойного назначения и просто подозрительных сделок, участникам СВПД придется задействовать значительные человеческие ресурсы для обработки запросов в ограниченный срок. Как отмечает Я. Стюарт из Королевского колледжа Лондона, Управление МАГАТЭ по ядерному контролю в Ираке за десять с небольшим лет своего существования рассмотрело около 18 000 контрактов[31].

Если ограничения на поставку товаров двойного назначения могут помешать иранским компаниям приобрести оборудование, необходимое для нефтехимической и космической промышленности, то другие положения соглашения могут вызвать еще большее неудовольствие иранской стороны. Согласно пункту 6.6 приложения IV к СВПД, «Любой участник СВПД может передать вопрос о какой-либо деятельности, связанной с закупками, на рассмотрение Совместной комиссии в рамках механизма урегулирования споров, если он обеспокоен тем, что такая деятельность не совместима с настоящим СВПД». Это означает, что поставки Ирану товаров, подпадающих под довольно неопределенную формулировку «предметы, которые могут способствовать деятельности, не совместимой с СВПД», могут быть опротестованы.

При этом нужно понимать, что в рамках Совместного всеобъемлющего плана действий каждое обвинение в невыполнении обязательств превратится в испытание соглашения по иранской ядерной программе на прочность.

МЕХАНИЗМ РАЗРЕШЕНИЯ СПОРОВ

Высокая сложность СВПД и взаимное недоверие сторон обусловили особую важность механизма разрешения споров. Помимо этого, сказалась *высокая концентрация* взаимных действий в рамках соглашения. Уже первый день соглашения (*День начала реализации*) Иран должен был встретить со значительно ограниченной ядерной программой, а *шестерка* международных посредников — сняв с Тегерана подавляющее большинство санкций. Стороны оказались сильно ограничены в возможностях реагирования на нарушение соглашения. *Шестерка* могла возобновить санкции против Ирана, Тегеран мог начать увеличивать количество центрифуг и уровень обогащения урана. Никаких промежуточных этапов для наращивания давления на нарушителя не было.

В итоге сторонам пришлось разработать длительный многоступенчатый механизм разрешения споров, сводящийся к многочисленным консультациям на разных уровнях. Главным компонентом механизма стала Совместная комиссия, предусмотренная приложением IV к СВПД. В состав комиссии вошли представители *шестерки* международных посредников, Ирана и ЕС. Помимо разрешения споров, Совместная комиссия будет рассматривать и утверждать планы по модификации иранских ядерных объектов и осуществлению проектов в атомной сфере, утверждать планы Ирана по международному сотрудничеству в области ядерных технологий, принимать решения относительно доступа инспекторов МАГАТЭ на иранские объекты и т. д.

Каждый участник комиссии имеет один голос. Решения будут приниматься консенсусом кроме описанных выше случаев разрешения споров между Ираном и МАГАТЭ относительно допуска инспекторов на иранские объекты.

Если одна из сторон соглашения решит, что другая сторона не соблюдает свои обязательства по СВПД, вопрос будет вынесен на рассмотрения Совместной комиссии. У комиссии будет 15 дней на разрешение вопроса (этот период может быть продлен консенсусом). В случае если обратившаяся в комиссию сторона посчитает, что ее претензия не была удовлетворена, она может выбрать один из двух путей: либо перевести обсуждение на уровень министров иностранных дел (рассмотрение в течение 15 дней, может быть продлено консенсусом), либо созвать Консультативный совет, состоящий из трех членов (по одному представителю от каждой из сторон спора и один независимый член), который должен в течение 15 дней вынести необязывающее заключение по вопросу. В случае необходимости у Совместной комиссии будет 5 дополнительных дней для рассмотрения заключения Консультативного совета и разрешения ситуации.

Если вопрос по-прежнему не будет разрешен, а сторона, подавшая жалобу, будет считать, что речь идет о серьезном нарушении соглашения, она передает вопрос в СБ ООН и может прекратить выполнять свои обязательства по СВПД.

В рамках СВПД обращение в СБ ООН является крайней мерой по принуждению стороны к выполнению ее обязательств. В результате этого обращения запускается механизм возобновления действия предыдущих резолюций Совета Безопасности в отношении Ирана и, соответственно, повторное введение международных санкций против страны. Поскольку СВПД не содержит дальнейших процедур и механизмов разрешения ситуации, подобное развитие событий будет также означать прекращение действия Совместного плана действий и договоренностей по иранской ядерной программе.

Механизм возврата предыдущих санкционных резолюций представляет особый интерес. Вместо того, чтобы вынести на голосование вопрос о возобновлении санкций в отношении Тегерана, СБ ООН, несколько контринтуитивно, должен будет рассмотреть резолюцию о сохранении *status quo*. Выглядеть это будет следующим образом: после получения от участника СВПД уведомления о существенном нарушении исполнения плана действий, Совет Безопасности ООН выносит на голосование проект резолюции, подтверждающей, что отмена предыдущих санкционных резолюций в отношении Ирана сохранится (или, говоря поэтическим

языком резолюции 2231, «резолюции о продолжении режима прекращения действия положений, предусмотренного в пункте 7 (a) настоящей резолюции»).[32]

У членов Совета Безопасности будет 10 дней на подготовку проекта резолюции, а если такой проект внесен не будет, его подготовит Председатель СБ. Если резолюция, подтверждающая отмену санкций, не будет принята в течение 30 дней с момента обращения (для чего достаточно противодействия любого из постоянных членов СБ), все положения предыдущих санкционных резолюций в отношении Ирана возобновляются со всеми вытекающими отсюда последствиями.

Решение по механизму возврата международных санкций стало интересным (и первым в истории) прецедентом обхода права вето постоянного Совета Безопасности в рамках резолюции СБ ООН. Подобное решение стало вынужденной уступкой со стороны ряда постоянных членов Совета Безопасности, уступкой, впрочем, ограниченной рамками одной отдельной резолюции. Механизм, использовавшийся в иранском соглашении, станет одним из возможных вариантов действия для дипломатов, готовящих будущие резолюции. Однако, учитывая, что для его повторного использования понадобится согласие всех постоянных членов Совета Безопасности ООН, — вариантом довольно экзотическим.

Таким образом, для разрешения вопроса о нарушениях соглашения у государств — членов СВПД будет минимум 60 дней (период может быть продлен консенсусным решением всех участников). На протяжении этого срока стороны будут должны урегулировать ситуацию, используя дипломатические средства убеждения и согласования позиций. В противном случае Совместный всеобъемлющий план действий прекратит свое существование.

ЗАКЛЮЧЕНИЕ

Всеобъемлющее соглашение по иранской ядерной программе стало итогом сложного процесса, растянувшегося более чем на десять лет. В случае реализации оно станет первым прецедентом снятия санкций, введенных в соответствии с Главой VII Устава ООН («Действия в отношении угрозы миру, нарушений мира и актов агрессии»), не предварявшимся военными действиями. В отличие от многих похожих договоренностей, СВПД выглядит достаточно эффективным и позволяет надеяться на достижение своих главных целей — снятия на ближайшие 10–15 лет опасений относительно военной составляющей иранской ядерной программы, расширения возможности для мониторинга мирной атомной деятельности и снятия препятствия для полной интеграции Тегерана в мировое сообщество.

Тем не менее, как и любой компромисс, СВПД несет в себя ряд уязвимостей. Ключевые из них: отсутствие юридических обязательств выполнять соглашение, усиливающее его зависимость от внутриполитической динамики в странах-участницах, и механизм принуждения к выполнению, в результате полного применения которого сам СВПД может быть завершен.

Первое означает, что и Вашингтон, и Тегеран могут выйти из соглашения при определенных внутри- и внешнеполитических обстоятельствах, не связанных с выполнением другой стороной СВПД.

В случае если новый президент США решит выйти из соглашения, руководствуясь исключительно узкопартийными подходами, другие стороны СВПД могут и должны оказать на него сдерживающее влияние. Важную роль здесь могут сыграть представители ЕС, союзники США по НАТО, но также Россия и КНР. Даже если повинуясь внутриполитическому импульсу США покинут соглашение, это не будет означать конец СВПД. Добрая воля остальных участников может сохранить процесс. Снятие санкций СБ ООН и ЕС может оказаться достаточным условием для Ирана, чтобы продолжать выполнение своей части договоренностей. Евросоюз должен подтвердить свою позицию не вводить санкции в отсутствие иранских нарушений и, в случае необходимости, активно вести переговоры с Ираном по модификации соглашения. В случае восстановления односторонних американских санкций против Тегерана ЕС, Россия и КНР, а также другие торговые партнеры Ирана должны быть готовы противостоять им. Евросоюз может обратиться к опыту постановления № 2271/96[33], вводящего защитные меры для европейских компаний от американских экстерриториальных санкций, связанных с эмбарго против Кубы. Перечисленные выше меры могут заставить американского президента пересмотреть свою позицию.

Что касается возможного выхода Ирана из соглашения, государства-члены СВПД должны с максимальной ответственностью и осторожностью подходить к введению новых санкций против Тегерана, особенно в первые годы действия соглашения. Ярким примером возможных трений может служить ситуация вокруг иранской ракетной программы, вернувшейся на передовицы СМИ в связи с испытанием ракеты *Имад*[34]. Развитие программы баллистических ракет, хоть и запрещенное резолюциями Совета Безопасности ООН, без обладания ядерным оружием не представляет собой серьезной угрозы. Было бы нелогично рисковать соглашением по ядерной программе, гарантирующим, что Иран не создаст подобное оружие, чтобы отстоять позицию, основанную на реалиях пятилетней давности, которая в любом случае будет отменена через восемь лет успешного выполнения СВПД.

Руководство Ирана, в свою очередь, должно продолжать свою политику гибкости и готовности к компромиссу, которая позволила достичь соглашения по ядерной программе. СВПД не ограничивает введение санкций в других сферах, и прекращение Тегераном выполнения своих обязательств на этом основании едва ли найдет поддержку в столицах европейских и азиатских союзников США. Чтобы не делать выполнение соглашения заложником внешних факторов, иранская сторона могла бы ограничиваться мягкой реакцией на незначительные изменения санкционного характера, не относящиеся к ядерной сфере.

Вторым фактом, который важно учитывать, является то, что, несмотря на свое название, соглашение по иранской ядерной программе фактически является одномоментным обменом ограничения ядерной программы Тегерана на снятие санкций. В связи с этим у СВПД сильно ограничен инструментарий наращивания давления в случае несоблюдения договора. На практике единственным инструментом принуждения является угроза отменить все положения соглашения. Более того, согласно механизму СВПД, в случае если эта угроза будет реализована, обратный путь не предусмотрен.

В этих условиях главной задачей стран-участниц соглашения должен являться не поиск повода для срыва СВПД, а определение *серых* зон и согласование правил поведения, которые бы обеспечили взаимно выгодный результат.

Важно также уважать национальную гордость иранской стороны. Это удалось при подготовке СВПД и должно учитываться в ходе его выполнения. Газета *New York Times* со ссылкой на анонимный источник сообщила о реакции представителей американской Администрации на условие Ирана сохранить часть центрифуг на обогатительном комплексе в Фордо[35]. Американцы были удивлены тем, что иранская сторона была готова разместить пятую часть своих центрифуг на объекте, где было запрещено использовать уран. При этом для Ирана было важно продемонстрировать, что ни один из центров по обогащению урана не был закрыт, и иранские дипломаты добились взаимоприемлемого компромисса.

В этом свете МАГАТЭ должно максимально серьезно следовать принципам СВПД, согласно которым «количество таких просьб [по предоставлению доступа к иранским объектам] будет сведено к такому минимуму, который необходим для эффективного выполнения обязанностей по контролю в соответствии с настоящим СВПД». Члены Совместной комиссии должны тщательно разобраться в сути вопроса при голосовании, а не действовать на основании блоковой или групповой логики.

В случае расхождения позиций между Тегераном и МАГАТЭ, *шестерке* международных посредников важно сохранять единую позицию и достигать консенсуса до того, как вступать в переговоры с Ираном. В случае *раскола шестерки* относительно допуска инспекторов МАГАТЭ на иранские объекты у пяти представителей Запада в Совместной комиссии будет достаточно голосов, чтобы заставить Иран принять инспекцию. Но это решение будет обладать низкой легитимностью в глазах иранского руководства и общества.

Наконец, ключевым принципом участия сторон в СВПД должно стать стремление не доводить ситуацию до рассмотрения и голосования в Совете Безопасности ООН. Грань, отделяющая действующее соглашение от возврата к состоянию 2012 г., оказалась очень тонкой. В случае если Совместный всеобъемлющий план действий и Резолюция СБ ООН 2231 прекратят существование, головоломку будет практически невозможно собрать заново.

Примечания

1 Remarks on the Nuclear Agreement with North Korea. William J. Clinton. October 18, 1994 http://www.presidency.ucsb.edu/ws/index.php?pid=49319&st=north+korea&st1

2 Joint Declaration by Iran, Turkey and Brazil. May 17, 2010. http://www.theguardian.com/world/julian-borger-global-security-blog/2010/may/17/iran-brazil-turkey-nuclear

3 Рамочная договоренность между Соединенными Штатами Америки и Корейской Народно-Демократической Республикой от 21 октября 1994 г. https://www.iaea.org/sites/default/files/publications/documents/infcircs/1994/infcirc457_rus.pdf

4 Российско-американская рамочная договоренность по уничтожению сирийского химического оружия, 14 сентября 2013 г. http://archive.mid.ru//brp_4.nsf/0/29EF49726E408D4D44257BE80060EC9E

5 John Bellinger. The New UNSCR on Iran: Does it Bind the United States (and future Presidents)? Lawfare. 18.07.2015 https://www.lawfareblog.com/new-unscr-iran-does-it-bind-united-states-and-future-presidents

6 Резолюция 2231 (2015), принятая Советом Безопасности на его 7488-м заседании 20 июля 2015 г. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/225/30/PDF/N1522530.pdf?OpenElement

7 Final Assessment on Past and Present Outstanding Issues regarding Iran's Nuclear Programme. Report of IAEA Director General. GOV/2015/68. December 2, 2015. http://isis-online.org/uploads/isis-reports/documents/IAEA_PMD_Assessment_2Dec2015.pdf

8 Aims and Strands of EU Sanctions. Steven Blockmans. Iran in the Regional and Global Context. P.18. http://www.pircenter.org/media/content/files/13/14296310520.pdf

9 Support for Iran Nuclear Agreement Falls. Pew Research Center. 08.09.2015 http://www.people-press.org/2015/09/08/support-for-iran-nuclear-agreement-falls/2/

10 Iran Nuclear Agreement Review Act of 2015. https://www.congress.gov/bill/114th-congress/house-bill/1191/text/pl

11 It's all but official: This will be the most dominant Republican Congress since 1929. Philip Bump. Washington Post. November 5, 2014 https://www.washingtonpost.com/news/the-fix/wp/2014/11/05/its-all-but-official-this-will-be-the-most-dominant-republican-congress-since-1929/

12 Cameron, Hollande and Merkel: Why we support the Iran deal. David Cameron, Fran ois Hollande and Angela Merkel. *Washington Post.* 10.09.15 https://www.washingtonpost.com/opinions/cameron-hollande-and-merkel-why-we-support-the-iran-deal/2015/09/10/a1ce6610–5735-11e5-b8c9-944725fcd3b9_story.html

13 Sen. Marco Rubio on Iran nuclear deal, Clinton and Trump. CBS News. July 24, 2015. http://www.cbsnews.com/videos/sen-marco-rubio-on-iran-nuclear-deal-clinton-and-trump/

14 CNN Reagan Library Debate: Later Debate Full Transcript. September 16, 2015 http://cnnpressroom.blogs.cnn.com/2015/09/16/cnn-reagan-library-debate-later-debate-full-transcript/

15 Khamenei says sanctions must be removed, not suspended. Arash Karami. Al-Monitor. 03.09.15. http://www.al-monitor.com/pulse/originals/2015/09/khamenei-sanctions-remove.html

16 Factbox: Iran's law approving nuclear deal — full translation. Reuters. 18.10.15 http://www.reuters.com/article/2015/10/18/us-iran-nuclear-law-factbox-idUSKCN0SC14P20151018#ilVUzRC6ZiyVXoCO.97

17 Arash Karami. Chief of Iran's Atomic Energy Organization clarifies nuclear needs. Al-Monitor. 09.07.2014. http://www.al-monitor.com/pulse/originals/2014/07/iran-nuclear-chief-clarifies-nuclear-needs.html

18 Letter to President Hassan Rouhani. Seyyed Ali Khamenei. 21.10.15 http://en.mfa.ir/index.aspx?siteid=3&fkeyid=&siteid=3&fkeyid=&siteid=3&pageid=1997&newsview=363361

19 Joint Comprehensive Plan of Action implementation and verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council Resolution 2231 (2015). Resolution adopted by the Board of Governors. 15 December 2015. https://www.iaea.org/sites/default/files/gov-2015–72.pdf

20 Лавров: в основе соглашения Ирана и «шестерки» лежит подход России. РИА Новости. 14.07.15 http://ria.ru/world/20150714/1128465765.html

21 Резолюции СБ ООН 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), 1929 (2010) и 2224 (2015)

22 Lifting sanctions imminent in two months. Информационное агентство MEXP. 14.10.15 http://en.mehrnews.com/news/111013/Lifting-sanctions-imminent-in-two-months

23 Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran. Report by the Director General. GOV/2015/65. 18.11.15 http://isis-online.org/uploads/isis-reports/documents/gov-2015-65.pdf

24 Рябков: Иран реализует план действий по атому в 2016 году. РИА Новости. 15.12.2015. http://ria.ru/world/20151215/1342268918.html

25 См., например: Постпред РФ: Иран демонтирует ядро реактора в Араке за две-три недели. ТАСС. 16.12.2015. http://tass.ru/politika/2531815

26 Iran nuclear deal: Council adopts the legal acts to prepare for the lifting of all nuclear-related economic and financial EU sanctions. Council of the EU. 18.10.2015. http://www.consilium.europa.

eu/en/press/press-releases/2015/10/18-iran-nuclear-deal/; JCPOA Contingent Waivers. US Department of State. 18.10.2015. http://www.state.gov/e/eb/rls/othr/2015/248320.htm

27 Приложение I к СВПД — меры, касающиеся ядерной области. Резолюция СБ ООН 2231. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/225/30/PDF/N1522530.pdf?OpenElement

28 IAEA Safeguards Glossary. International Nuclear Verification Series No. 3. P. 23. https://www.iaea.org/sites/default/files/iaea_safeguards_glossary.pdf

29 Приложение IV к СВПД — Совместная комиссия, раздел 6. Резолюция СБ ООН 2231. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/225/30/PDF/N1522530.pdf?OpenElement

30 См. информационные циркуляры МАГАТЭ INFCIRC/254/Rev.12/Part 1a https://www.iaea.org/sites/default/files/infcirc254r12p1_rus.pdf и INFCIRC/254/Rev.9/Part 2a https://www.iaea.org/sites/default/files/infcirc254r9p2_rus.pdf

31 The Iranian Nuclear Procurement Channel: the most complex part of the JCPOA? Ian J. Stewart. World Export Control Review. http://www.worldecr.com/wp-content/uploads/Iranian-Nuclear-Procurement-Channel_WorldECR1.pdf

32 Резолюция 2231 (2015), принятая Советом Безопасности на его 7488-м заседании 20 июля 2015 года, пункт 11. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/225/30/PDF/N1522530.pdf?OpenElement

33 Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom. Official Journal L 309, 29/11/1996 P. 0001–0006. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271: EN: HTML

34 Александр Левченко. МИД Ирана: испытание баллистической ракеты не нарушает ядерное соглашение. ТАСС. 13.10.2015 http://tass.ru/mezhdunarodnaya-panorama/2344795

35 David E. Sanger, Michael R. Gordon. An Iran Nuclear Deal Built on Coffee, All-Nighters and Compromise. New York Times. April 3, 2015

Ольга Макарова

УЯЗВИМОСТЬ ИНТЕРНЕТА: МИФЫ И РЕАЛЬНОСТЬ

Dear Mr. Andropov,

My name is Samantha Smith. I am ten years old. Congratulations on your new job. I have been worrying about Russia and the United States getting into a nuclear war. Are you going to vote to have a war or not? If you aren't please tell me how you are going to help to not have a war. This question you do not have to answer, but I would like to know why you want to conquer the world or at least our country. God made the world for us to live together in peace and not to fight.

Sincerely,
Samantha Smith

Это письмо американской школьницы С. Смит, адресованное Председателю Президиума Верховного Совета и Генеральному Секретарю ЦК КПСС Ю. Андропову, было отправлено в ноябре 1982 г. и опубликовано в газете *Правда* в 1983 г.

Написать его Саманту побудили фотографии Ю. Андропова и Р. Рейгана на обложке журнала *Time Magazine*. Они были названы *людьми года*, однако в посвященной этому событию статье говорилось, что новый руководитель Советского Союза — человек крайне опасный и представляет реальную угрозу для безопасности США. Сегодня очевидно, что Ю. Андропов не планировал начинать ядерную войну с США, но для журналистов все годы, пока он был у власти, эта тема оставалась неисчерпаемым информационным поводом.

Сегодня мало кто всерьез задумывается об угрозе ядерной войны. Современный жупел и бесконечный информационный повод — безопасность глобального интернета и вероятность его полного или частичного отключения. Страсти накалились настолько, что того гляди появится новая С. Смит, которая напишет президентам России и США письмо с просьбой сохранить глобальный интернет.

Слухов, действительно, ходит немало. Можно вспомнить историю о якобы имевших место учениях по отключению российских пользователей от глобального интернета или о российской подлодке, намеревавшейся не то взорвать, не то перерезать кабельные системы, соединяющие материки. Звучит драматич-

но, но для специалистов очевидно, что силами одного провайдера, даже уровня глобального Tier 1, невозможно отключить интернет даже для всех пользователей одной страны, что и говорить о глобальном *блэкауте*. Также непонятно, как именно российская подводная лодка угрожала межконтинентальным кабельным системам. Ведь континенты соединены между собой по принципу *каждый с каждым*, причем не одной и не двумя, а значительно большим числом кабельных систем[1].

Интернет представляет собой весьма сложную структуру, и проанализировать все возможные типы угроз для его функционирования — задача, выходящая далеко за рамки нашего исследования. В этой статье мы попробуем разобраться в том, насколько уязвима та часть инфраструктуры глобального интернета, которая отвечает за пропуск трафика. Мы намеренно не будем касаться уязвимостей системы доменных имен. Это большая тема, требующая отдельного обсуждения. В этой статье мы будем исходить из предположения, что стабильности работы системы доменных имен ничего не угрожает, и преобразование доменного имени в IP-адрес осуществляется во всех случаях.

ИНФРАСТРУКТУРА ОПОРНЫХ РЕГИОНАЛЬНЫХ СЕТЕЙ

Для целей этой статьи под термином *инфраструктура опорных региональных сетей* мы будем понимать инфраструктуру кабельных, спутниковых и радиорелейных линий связи, задействованных для организации связи между городами одной страны. На территории Российской Федерации термин *инфраструктура опорной региональной сети* часто заменяют термином *магистральные сети связи Российской Федерации*.

Для организации инфраструктуры опорных региональных сетей (backbone/core networks) операторы, как правило, используют волоконно-оптические кабельные системы. Системы спутниковой связи и радиорелейные системы используются для организации линий связи в удаленных и труднодоступных регионах, в которых строительство и обслуживание волоконно-оптических линий связи экономически нецелесообразно или технически невозможно.

На рисунках 1, 2, 3 представлены карты сетей отдельных крупных операторов связи, входящих в состав инфраструктуры опорной региональной сети США, и карта инфраструктуры опорной региональной сети США.

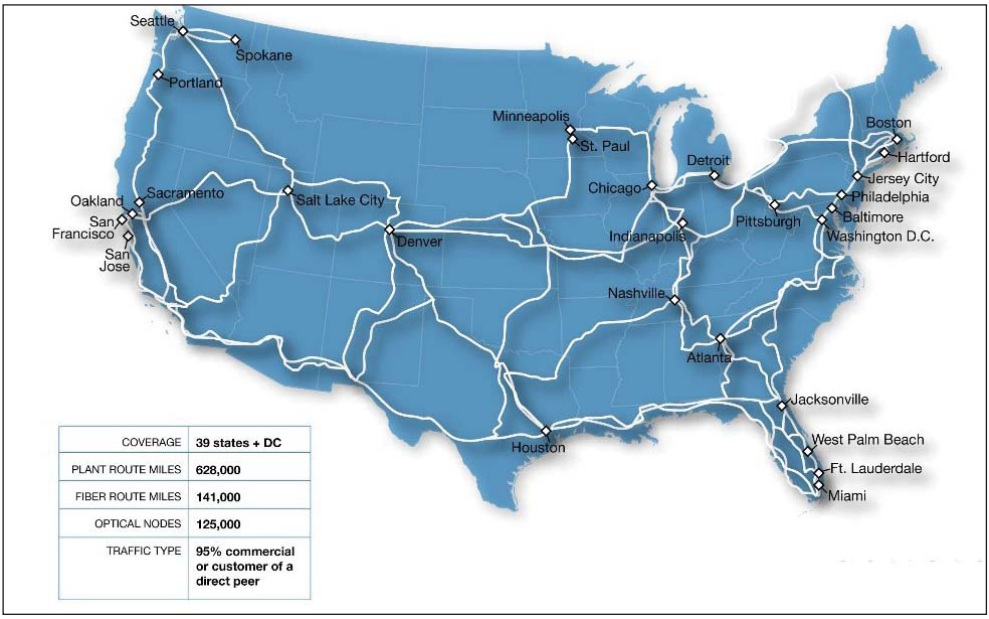
Следует обратить внимание на то, что инфраструктура опорных сетей резервируется по кольцевому принципу. Аналогичным образом организована инфраструктура сетей связи других крупных операторов, работающих в разных странах и на разных континентах.

Основу инфраструктуры опорной региональной сети Российской Федерации составляют сети следующих операторов связи: ПАО *Ростелеком*, ПАО *МТС*, ПАО *Мегафон*, ПАО *Вымпелком*, ЗАО *Компания ТрансТелеком* (рис. 4–6).

ТРАНСГРАНИЧНЫЕ ПЕРЕХОДЫ

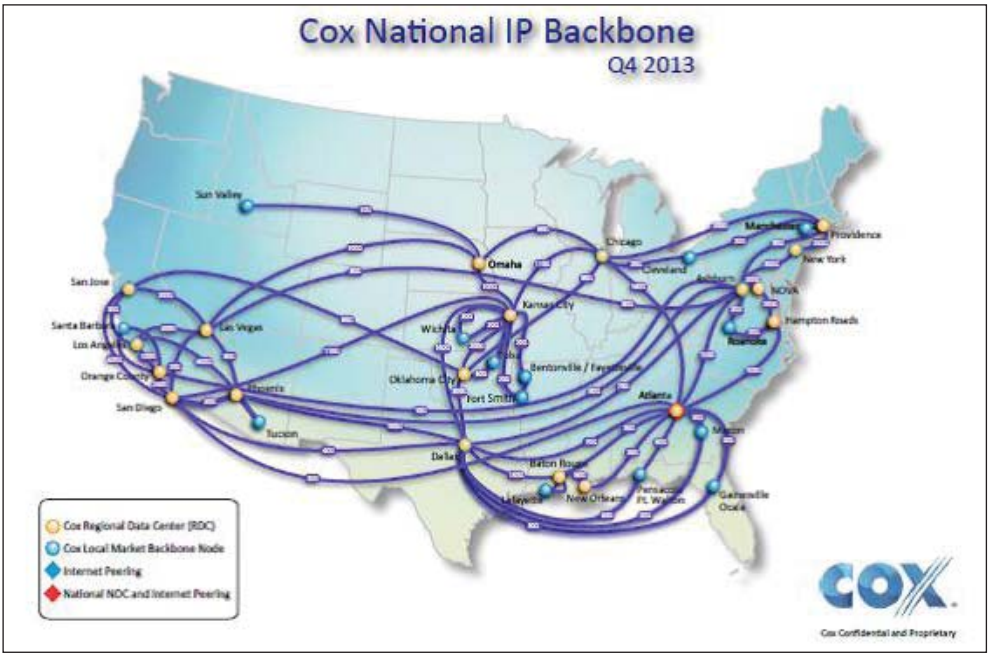
Для организации инфраструктуры, связывающей сети в составе опорных региональных инфраструктур, находящихся в разных странах, но на одном континенте,

Рисунок 1. **Карта сети оператора Comcast, обслуживающего более 15 млн домохозяйств в США, входящей в состав инфраструктуры опорной региональной сети США**



Источник: http://business.comcast.com/about-us/our-network

Рисунок 2. **Карта сети оператора Cox Communications, входящей в состав инфраструктуры опорной региональной сети США**



Источник: http://www.cox.com/wcm/en/business/datasheet/national-ip-backbone-map.pdf

Рисунок 3. **Инфраструктура опорной региональной сети США**

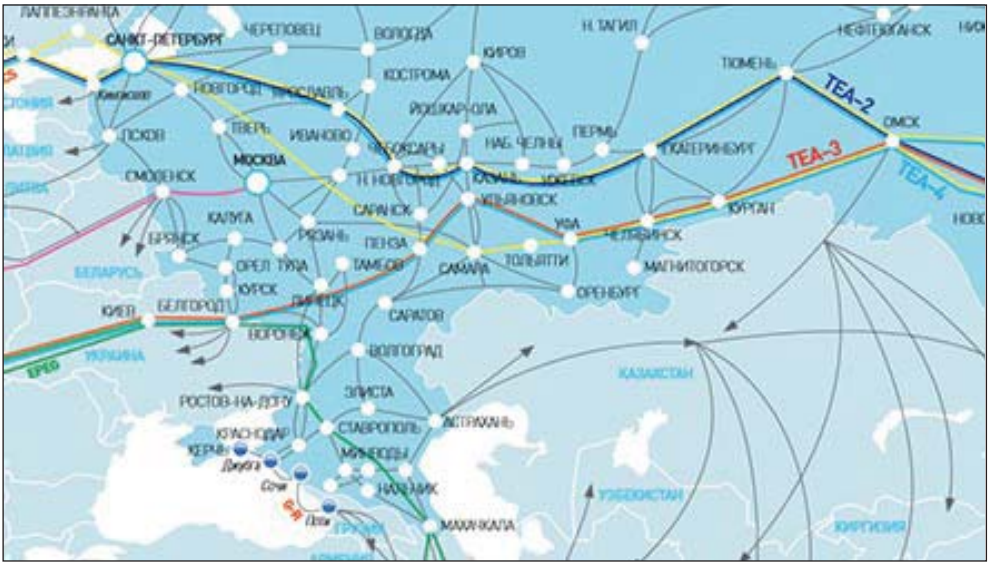
Источник: http://www.hughandbecky.org/2013/internet-access-to-africa/

операторы строят трансграничные переходы (в терминологии законодательства в области связи Российской Федерации *пограничные переходы*), преимущественно с использованием наземных волоконно-оптических линий связи.

Операторы, претендующие на роль региональных Tier 1, в обязательном порядке имеют собственные трансграничные переходы, которые используются для организации каналов связи для присоединения к глобальным Tier 1, а также к региональным точкам обмена трафиком. Термины *глобальный* и *региональный Tier 1* будут раскрыты в следующих разделах настоящей статьи.

На текущий момент в Российской Федерации зарегистрировано порядка 89 трансграничных переходов.

Рисунок 4. **Карта сети оператора ПАО Ростелеком, входящей в состав инфраструктуры опорной региональной сети Российской Федерации**



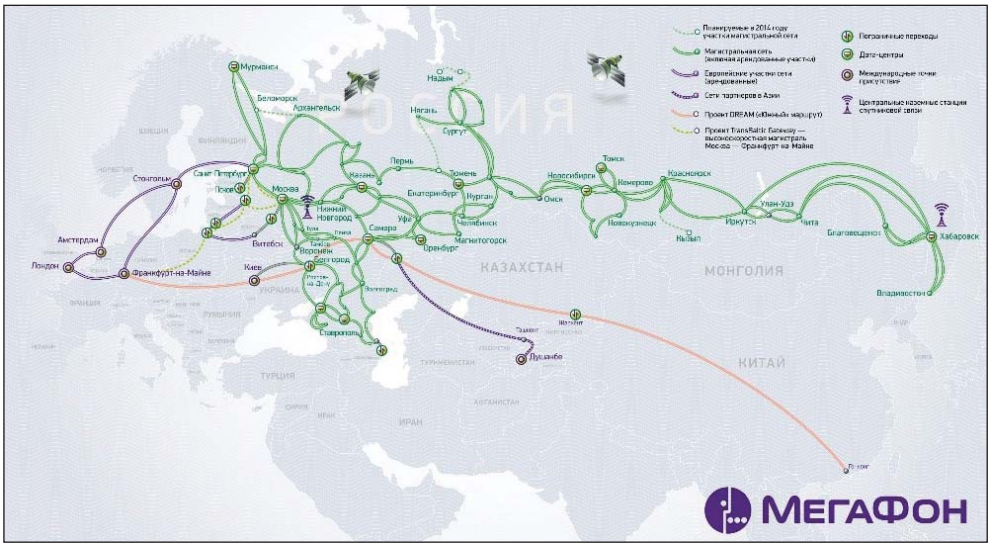
Источник: http://www.rt.ru/data/doc/backbone_map.pdf

Рисунок 5. **Карта опорной сети оператора ПАО МТС, входящей в состав инфраструктуры опорной региональной сети Российской Федерации**

Источник: ПАО МТС

Строительству трансграничных переходов уделяется большое внимание, в том числе в рамках Тунисской программы Всемирной встречи на высшем уровне по вопросам информационного общества 2005 г., как основному фактору, ускоряющему решение проблемы цифрового неравенства.

Рисунок 6. **Карта сети оператора ПАО Мегафон, входящей в состав инфраструктуры опорной региональной сети Российской Федерации**



Источник: http://moscow.megafon.ru/operators/help/megafon_network/main_map/

ТРАНСГРАНИЧНЫЕ ПЕРЕХОДЫ МЕЖДУ КОНТИНЕНТАМИ, ПОДВОДНЫЕ КАБЕЛЬНЫЕ СИСТЕМЫ

Для организации межконтинентальных трансграничных переходов формируются консорциумы, которые прокладывают подводные кабельные системы.

На сегодняшний день связь между Европой и Америкой обеспечивают 7 подводных кабельных систем: Hibernia Atlantic, TAT-14, Atlantic — Crossing 1, TAT — TNG — Atlantic, Flag Atlantic — 1, Yellow и Appolo. Система Greenland Connect соединяет Исландию, Гренландию и Северную Америку. В свою очередь, Исландию с материком соединяют системы FARICE-1, CANTAT-3. DANICE. Азию и Северную Америку соединяют TATA TNG-PACIFIC, TRANS-PACIFIC EXPRESS, CHINA US, JAPAN US, PACIFIC CROSSING, UNITY/EAC PACIFIC. В 2016 г. планируется завершить строительство системы FAST, а в 2017 г. — системы NEW CROSS PACIFIC. Относительно недавно Европу и Азию соединяли преимущественно подводные кабельные системы: SEA-ME-WE 3, FLAG EUROPA ASISA, SEA-ME-WE 4. Однако в настоящее время для пропуска трафика между Европой и Азией наряду с подводными кабельными системами активно строятся и развиваются наземные кабельные системы, проходящие через Российскую Федерацию, Монголию, Казахстан, Белоруссию, Украину, Польшу, Финляндию, Швецию и прибалтийские страны. Полную карту подводных кабельных систем можно найти на сайте *TeleGeography* по адресу http://submarine-cable-map-2015.telegeography.com/[2].

Таким образом, сегодня в кабельных системах существует возможность резервирования маршрутов не только на уровне одного направления (задействуя ресурсы разных наземных и подводных кабельных систем попутного направления, к примеру Европа — Азия), но и возможность частичного резервирования маршрутов

путем задействования различных кабельных систем на различных направлениях, например частичное резервирование направления Азия — Америка через Европу.

Наряду с этим, глобальные игроки рынка продажи контента и информационно-коммуникационных сервисов, в первую очередь американские, за которыми вплотную следуют китайские, на данный момент стремятся разместить свое оборудование (серверы) в наиболее востребованных точках обмена трафиком на разных континентах, в так называемых *телехаусах* (датацентрах для телеком-инфраструктуры) — местах сосредоточения узловой инфраструктуры крупных, средних и мелких операторов. Кроме точек обмена трафиком и телехаусов, контент-сервис-провайдеры и провайдеры информационно-коммуникационных сервисов активно размещают оборудование в сетях региональных операторов. Для этого не всегда выбираются операторы регионального уровня Tier 1, так как в данном случае провайдерам главное встать как можно ближе к конечному потребителю. Это один из наиболее важных аспектов современного ландшафта предоставления доступа к контенту и информационно-коммуникационным сервисам и один из способов максимального охвата, а иногда и захвата целевой аудитории, ценность которой возрастает пропорционально росту числа пользователей контента и информационно-коммуникационных сервисов.

При такой организации раздачи контента и услуг контент-сервис-провайдер имеет возможность экономить на закупке услуг IP-транзита у upstream-провайдеров. Действуя по принципу *любое подключение, в любом месте, в любое время* контент-сервис-провайдеры получают максимально возможную гибкость при организации подключений. Такой ландшафт предоставления контента и информационно-коммуникационных сервисов фактически лишает продавцов услуг IP-транзита и upstream-провайдеров их рыночной силы. Они уже не могут активно влиять ни на принятие контент-сервис-провайдером решения об установлении соединений, ни на раздачу трафика с платформы контент-сервис-провайдера.

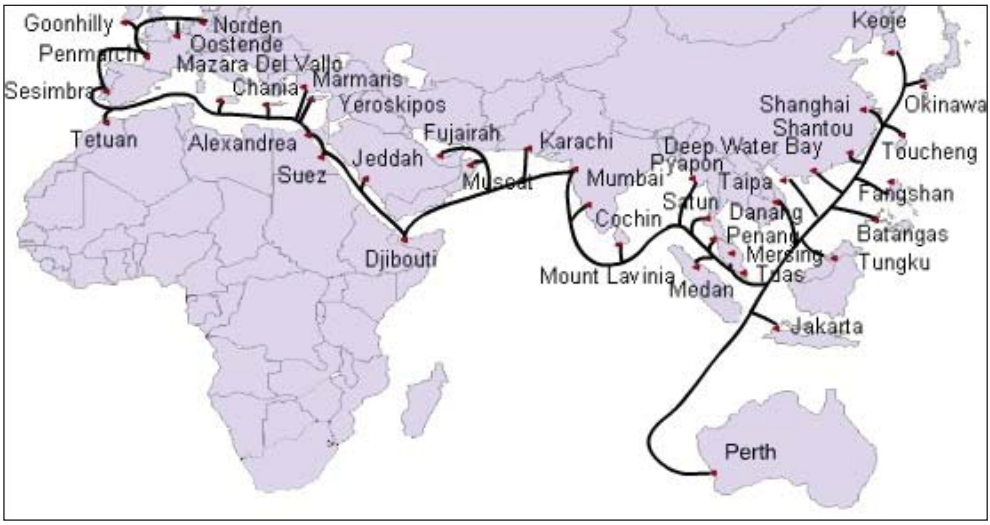
Тем не менее, чтобы понять, что реально влияет на качество услуг, оказываемых конечным клиентам, будет полезно проанализировать некоторые наиболее серьезные аварии на подводных кабельных системах.

В июле 2005 г. возникло повреждение кабеля подводной кабельной системы SEA-ME-WE 3. Некоторые источники утверждают, что в повреждении кабеля виноваты излишне любопытные морские обитатели. Повреждение произошло в 35 км к югу от г. Карачи. Поврежден был не опорный кабель системы SEA-ME-WE 3, а так называемый *кабельный отвод* — кабель, соединяющий береговой колодец с опорным кабелем (см. рис. 7). Поэтому ухудшение качества услуг наблюдалось только в Пакистане.

В результате аварии в Пакистане возникли серьезные проблемы со всеми видами связи, включая доступ к интернету. Следует отметить, что в то время в Пакистане собственные информационные ресурсы были развиты достаточно слабо, кэширующие серверы ведущих поставщиков информации на территории Пакистана не размещались, поэтому в структуре потребления трафика присутствовала значительная доля зарубежного трафика, получить который можно было только через подводную кабельную систему. Впрочем, с тех пор ситуация изменилась незначительно.

26 декабря 2006 г. из-за землетрясения у берегов Тайваня случилось очередное повреждение кабельной системы SEA-ME-WE 3. Ухудшение качества связи имело место у пользователей на Тайване и частично в Южной Корее и Китае[3].

Рисунок 7. **Подводная кабельная система SEA-ME-WE-3. Место повреждения кабеля выделено красным**



Источник: http://hlaoo1980.blogspot.ru/2013/07/leaked-underground-cable-disrupting.html, http://www.smh.com.au/news/breaking/communication-breakdown-in-pakistan/2005/06/29/1119724673577.html?from=moreStories, http://timesofindia.indiatimes.com/world/pakistan/Pakistan-cut-off-from-the-world/articleshow/1154683.cms?referral=PM

30 января 2008 г. в Египте, в районе Александрии, якорем судна была повреждена резервная кабельная система SEA-ME-WE 4. В результате обрыва кабеля пользователи из Соединенных Штатов и Европы не могли осуществлять международные звонки в страны Ближнего Востока и Южной Азии. Услуги связи были недоступны более чем для 70% пользователей Египта[4].

Следует отметить, что Египет, как и Пакистан, не имеет собственных сколь-нибудь значимых информационных ресурсов, основное потребление трафика составляют зарубежные ресурсы, кэширующие серверы на территории страны не размещались.

19 декабря 2008 г. вновь были серьезно повреждены кабельные системы SEA-ME-WE 4, FLAG FEA и GO-1. Также происходили аварии 10 января 2013 г., 30 января 2014 г. и 8 января 2015 г.

15 сентября 2015 г. возник очередной обрыв кабеля. Проблемы с доступом к интернету испытывали пользователи Сингапура и Австралии. Особые проблемы возникли у пользователей продукции *Apple*, так как именно в это время осуществлялось обновление операционных систем iOS 9 и OS X[5].

Следует отметить, что проблемы со скачиванием обновлений *Apple* в этот период испытали не только пользователи из Сингапура и Австралии. Летом 2015 г. компания *Apple* поменяла подходы к организации каналов распространения своих продуктов. Если до лета 2015 г. обновления *Apple* были доступны через сети доставки контента (CDN) глобальных контент-провайдеров, таких как *Akamai*, *Level 3* и др.,

то по состоянию на 15 сентября 2015 г. обновления *Apple*, поменявшего стратегию раздачи контента, должны были стать доступными для операторов и их пользователей исключительно через прямые соединения между оборудованием *Apple* и оборудованием каждого оператора связи в точках обмена трафиком и телехаусах.

К сожалению, специалисты *Apple* на момент раздачи новых версий iOS не смогли корректно настроить таблицы маршрутизации, и большую часть обновлений пользователи операторов получили через сети глобальных Tier 1, у некоторых из которых из-за создавшейся внештатной ситуации ряд стыков оказались перегруженными. Представители *Apple* не смогли дать однозначный ответ на вопрос, что произошло с маршрутизацией трафика.

Статистика аварийных ситуаций в других кабельных системах аналогична статистике аварийных ситуаций, приведенных выше.

Таким образом, основные причины аварийных ситуаций — природные явления, гражданские суда, чуть реже морские обитатели.

При возникновении аварийных ситуаций наименее защищенными оказываются пользователи тех стран, где:

- отсутствуют собственные информационные ресурсы;
- отсутствуют развитые точки обмена трафиком;
- не развита структура телехаусов;
- не установлены прямые соединения между основными региональными Tier 1 (пиринговые соединения);
- региональные Tier 1 не сформировались или вытеснены с рынка западными игроками — продавцами услуг IP-транзита;
- ведущие глобальные контент-сервис-провайдеры не размещают кэширующие серверы в виду отсутствия технической возможности, наличия политической воли не допускать размещения кэширующих серверов зарубежных контент-сервис-провайдеров или отсутствия экономической целесообразности такого размещения.

Иными словами, наиболее уязвимыми являются пользователи тех стран, где отсутствует национальная интернет-экосистема. Но в большинстве случаев интернет оказывается относительно устойчив к авариям на подводных кабельных системах.

Гораздо сильнее страдают голосовые сервисы, в первую очередь, услуги международной телефонной связи. Несмотря на достаточно широкое распространение интернет-технологий, многие операторы до сих пор используют системы цифровой иерархии (SDH) для пропуска междугородного телефонного трафика. В договорах такая организация услуг по пропуску готового трафика относится к категории *premium*, то есть высшего качества. Одновременно с этим специализированные услуги для корпоративных клиентов, в числе которых онлайн-доступ к торгам на бирже, также являются очень уязвимыми в случае аварии на кабельных системах.

В последнее время отчетливо прослеживается новый тренд — постепенная миграция международного голосового трафика в IP-сети. В отдельных странах этот процесс идет очень быстро, в других достаточно медленно и тяжело. В первую оче-

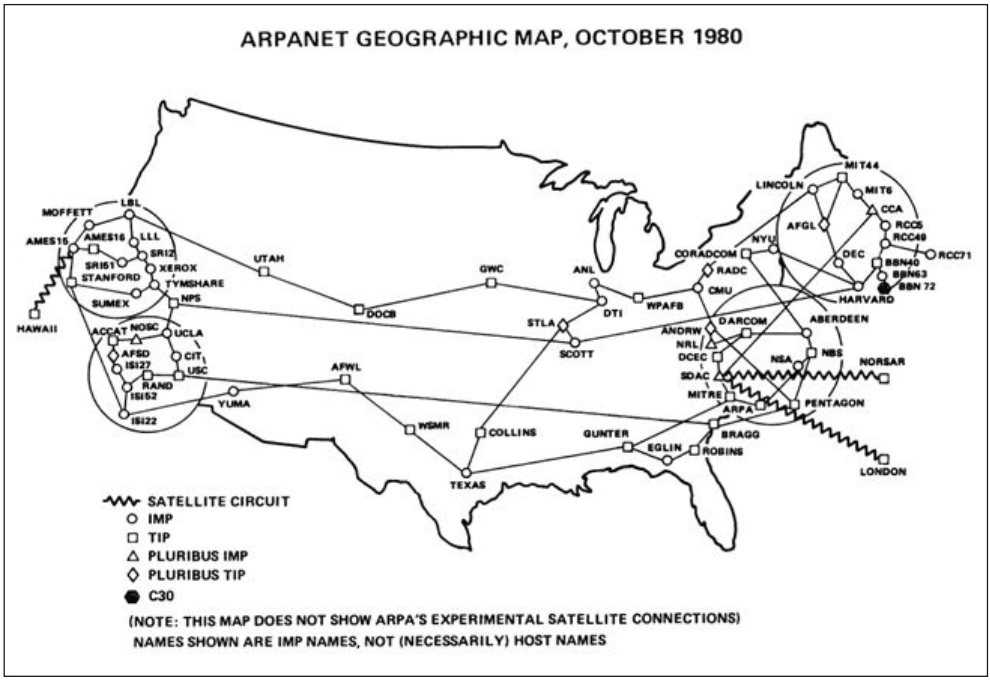
редь, сложность перехода определяется привычками и привязанностями, а также мифами о ненадежности IP-сетей, бытующими в среде профессионалов. На самом деле такой переход был бы вполне оправданным, ведь, как мы видим на практике, любой обрыв на подводной кабельной системе оказывает меньшее воздействие на функционирование глобального интернета, чем на телефонию, так как за счет своей распределенности и присутствия многих глобальных ресурсов в различных точках земного шара интернет страдает значительно меньше, чем международная телефония, организованная в SDH-системах, или специализированные услуги для корпоративных клиентов.

Впрочем, чтобы IP окончательно закрепился на международном телефонном транзите, с высокой степенью вероятности потребуется смена поколений, то есть смена людей, а не оборудования или программного обеспечения.

ИНТЕРНЕТ-ЭКОСИСТЕМЫ: ГЛОБАЛЬНЫЕ И РЕГИОНАЛЬНЫЕ

Для того чтобы разобраться в структуре современного интернета и убедиться в ее устойчивости, нам придется вернуться на много лет назад, в те времена, когда интернет перестал быть спонсируемым министерством обороны США проектом и начал свое движение по планете. Инфраструктура интернета того времени выглядела примерно так:

Рисунок 8. **Инфраструктура интернета 1980 г.**



Источник: http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html

Как только проект стал коммерческим, возникла необходимость научиться зарабатывать на нем деньги. И тогда появились правила.

КЛУБ ГЛОБАЛЬНЫХ TIER 1 — ОСНОВА ИНФРАСТРУКТУРЫ ПЕРВОЙ ОПОРНОЙ СЕТИ ГЛОБАЛЬНОГО ИНТЕРНЕТА

Нашлось шесть компаний, часть которых получила в наследство, а часть достроила зачатки инфраструктуры глобального интернета. Они образовали между собой прямые связи по принципу *каждый с каждым* (см. рисунок 8). Эти связи получили название *пиринговых соединений*, а взаимоотношения между владельцами этих связей стали называться *пирингом*. Таким образом, сформировалась сущность глобальных Tier 1, сети которых составили основу инфраструктуру самой первой опорной сети глобального интернета.

Пиринг-партнеры могли обмениваться друг с другом трафиком своих клиентов и присоединенных к ним операторов, интернет-сервис провайдеров, контент-сервис-провайдеров и пр., которые имели собственные автономные системы. Но ни один из пиринг-партнеров не мог осуществлять транзит (передачу) трафика клиентов, присоединенных операторов и др. одного пиринг-партнера другому пиринг-партнеру через свою автономную систему.

НЕСКОЛЬКО СЛОВ ОБ АВТОНОМНЫХ СИСТЕМАХ

В настоящее время автономная система (AS) может использовать несколько протоколов внутренней маршрутизации, а в некоторых случаях и несколько наборов метрик в рамках одной AS. При этом администрирование автономной системы для других автономных систем выглядит как единый план внутренней маршрутизации и показывает согласованную картину доступности ресурсов в этой автономной системе.

Каждая автономная система имеет уникальный идентификатор — номер автономной системы — Autonomous System Number (ASN). Номер автономной системы используется при обмене маршрутными данными между соседними автономными системами, а также в качестве обозначения самой автономной системы. Обычно автономная система использует один или несколько протоколов внутренней маршрутизации (IGP) для передачи сведений о маршрутизации в пределах данной AS. Рекомендуемым протоколом внешней маршрутизации сегодня является Border Gateway Protocol (BGP).

МОДЕЛИ РАСЧЕТОВ В ИНТЕРНЕТЕ

Все присоединявшиеся к глобальному Tier 1 операторы, контент-сервис-провайдеры, клиенты и пр. должны были платить Tier 1 за пропуск трафика, независимо от того, является ли этот трафик входящим или исходящим. Если оператор, клиент или контент-сервис-провайдер с целью резервирования осуществлял подключение к двум или более Tier 1, оплата осуществлялась в адрес каждого Tier 1, к которому было осуществлено подключение.

Ни один глобальный Tier 1 не должен был платить никому. Разрыв пиринговых соглашений и стыков между членами клуба Tier 1 был невозможен, так как грозил серьезными последствиями для устойчивости функционирования глобального интернета. В следующих разделах будет показано, к каким серьезным последствиям приводили попытки глобальных Tier 1 разорвать пиринговое соединение с несговорчивым пиринг-партнером из-за невозможности достижения приемлемых коммерческих договоренностей путем ведения переговоров.

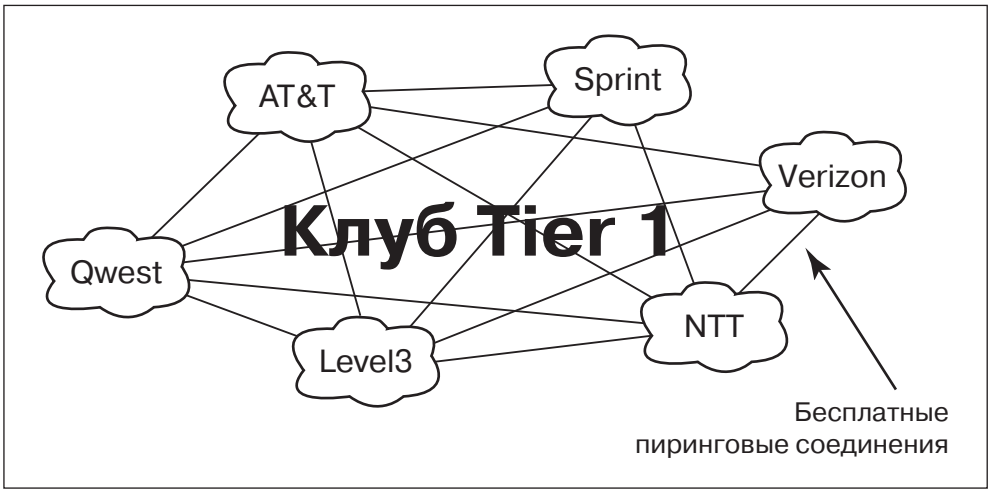
Условием вступления в клуб глобальных Tier 1 было установление пиринговых соединений со всеми членами клуба. Это требование было вполне обоснованным. В соответствии с имеющимися договоренностями, члены клуба предлагали клиентам (операторам или контент-сервис-провайдерам) трафик не только своей сети, но и сетей (ресурсов) своих клиентов, включая присоединенных операторов и контент-сервис-провайдеров, а также трафик всех своих пиринг-партнеров. Другие члены клуба с этими клиентами не работали. Сделано это было, чтобы избежать конкуренции и не лишать партнеров дохода.

Очень многие крупные операторы для входа в клуб глобальных Tier 1 вынуждены были осуществить покупку компаний-членов этого клуба. Например, *Level 3* купила *Genuity*.

Присоединенным операторам не запрещалось продавать трафик другим операторам, которые по тем или иным причинам не смогли присоединиться ни к одному из глобальных Tier 1.

При осуществлении такой продажи оператор, присоединенный к глобальному Tier 1, становился Tier 2 и получал право продавать трафик своей сети, сетей своих клиентов, сетей присоединенных операторов и контент-сервис-провайдеров, сетей своих пиринг-партнеров и весь трафик, который Tier 2 получал от глобального Tier 1.

Рисунок 9. **Клуб глобальных Tier 1 после покупки отдельных игроков крупными операторами**[6]



Отношения по продаже трафика получили название IP-транзит. Оператор или провайдер, продающий услугу IP-транзит, именовался upstream, оператор или провайдер, покупающий услугу IP-транзит, именовался downstream.

Уровень вложенности такой системы был не ограничен.

В это же время был выработан и установлен еще один очень важный принцип: независимо от того, является ли компания контент-сервис-провайдером, то есть компаний, создающей трафик для конечных потребителей, или оператором связи, то есть компанией, потребляющей трафик за счет своих потребителей, все должны платить своему upstream-партнеру. Никогда и ни при каких условиях upstream-партнер не должен платить компании, генерирующей трафик, даже если этот трафик в дальнейшем потребляется его клиентами или клиентами присоединенных к нему downstream-операторов. Контент-сервис-провайдер должен зарабатывать деньги на рекламе, операторы — на конечных клиентах, но и те, и другие должны оплачивать своим upstream-партнерам услуги IP-транзита.

Американские Tier 2 довольно быстро поняли, что, устанавливая пиринги с равными себе, можно сэкономить на оплате услуг глобальных Tier 1, а дальше это понимание спустилось вниз по цепочке по уровням вложенности. Вопрос, как определить, кто равен тебе, а кому ты можешь продавать трафик, требовал индивидуального подхода и креативного мышления пиринг-менеджеров.

Устанавливать соединения с равными себе можно было через точки обмена трафиком или напрямую. В США, откуда пошел интернет, большая часть операторов предпочитает устанавливать пиринговые соединения с равными себе напрямую, минуя точки обмена трафиком. В Европе ситуация выглядит несколько иначе.

Само собой разумеется, что на начальных стадиях развития глобального интернета европейские операторы, желающие подключиться к нему, вынуждены были оплачивать не только услуги IP-транзита глобальных Tier 1, но и платить за каналы связи, организованные через подводные кабельные системы. Поэтому европейские операторы были крайне заинтересованы в развитии пиринговых отношений на своей территории, а также в приближении контента к европейскому потребителю.

Следует отметить, что глобальные контент–сервис провайдеры, крайне заинтересованные в расширении своей аудитории, были готовы поставить свое оборудование в Европе для того, чтобы снизить платежи глобальным Tier 1, Tier 2, а иногда и Tier 3.

Приходить в Европу и арендовать каналы для подключения к каждому из операторов глобальным контент-ресурсам на этапе становления европейского сегмента сети Интернет было экономически нецелесообразно. Поэтому в Европе начали активно развиваться точки обмена трафиком.

В своих работах исследователь экономических отношений в интернете У. Нортон[7] выделяет следующие предпосылки для появления востребованных точек обмена трафиком:

Теория здоровой пиринговой интернет-экосистемы:

- востребованные точки обмена трафиком появляются и процветают там, где существует большая концентрация потребителей контента и большой объем контента;

- когда объем локального (регионального) трафика значителен, международные интернет-провайдеры и CDN заинтересованы в создании новой точки обмена трафиком в регионе, чтобы разгрузить собственные международные маршруты.

Теория точки вывода кабелей:

- точки вывода должны быть расположены топологически близко к местам выхода подводных кабелей, например в портах.

Теория географической близости:

- Лондон — удачное место для продвижения интернета внутри Европы;
- Франкфурт-на-Майне — удобная площадка для сбора ближневосточного трафика и трафика провайдеров Восточной Европы;
- Австралия лежит *на пути в никуда*.

Теория финансового центра (предложена А. Нипером):

- финансовые рынки являются драйвером роста точек обмена трафиком;
- финансовое сообщество выступает за максимальное сокращение задержек, стимулируя операторов размещаться вблизи финансовых центров;
- самые большие точки обмена трафиком расположены в Лондоне, Франкфурте, Амстердаме, Нью-Йорке, Чикаго и Токио, потому что там расположены ведущие финансовые биржи. На очереди Милан.

Теория бизнес ориентированности (предложена М. Мойл-Крофтом):

Рисунок 10. **Динамика падения цены за единицу трафика**[8]

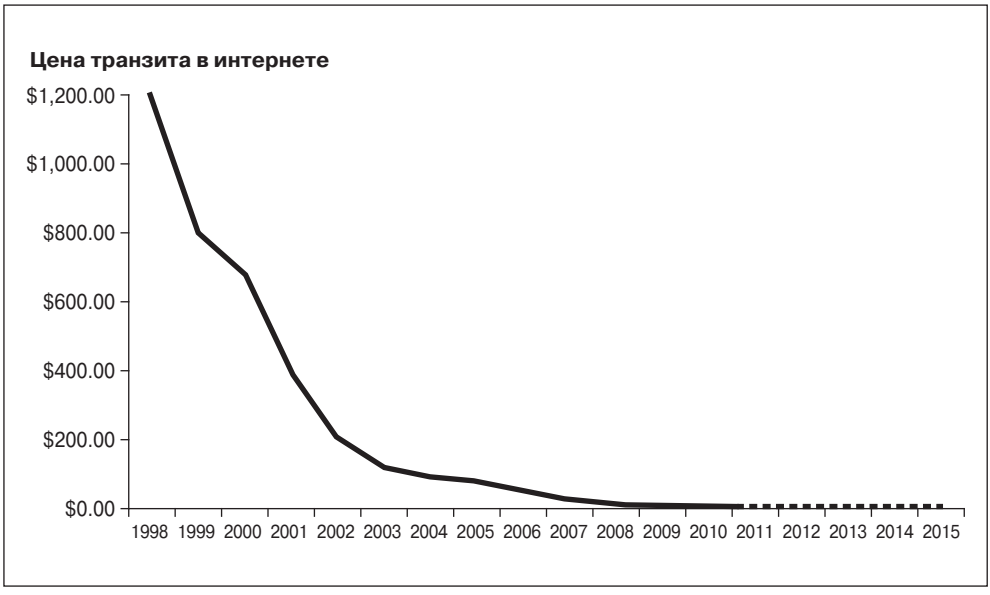
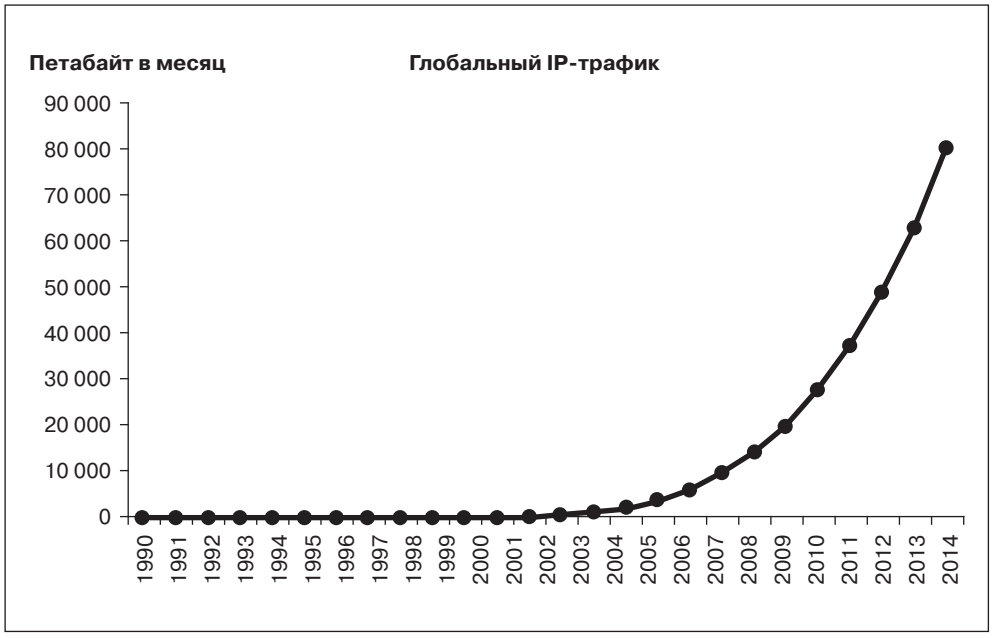


Рисунок 11. **Рост объемов передаваемого трафика**[9]



- нестабильная правовая и регуляторная среда сводит на нет любые попытки строить региональные точки обмена трафиком и привлекать международных игроков;
- для деловых людей работа в рамках запутанных и обременительных правил, установленных национальным регулятором и отличных от общемировых практик, не представляет интереса.

Развитие точек обмена трафиком и замыкание трафика внутри региона привело к возникновению региональных интернет-экосистем со своими региональными Tier 1. Развитие региональных информационных ресурсов, а также стремление глобальных контент-сервис-провайдеров присутствовать во всех крупных точках обмена трафиком привели к значительному снижению зависимости от американских провайдеров и к повышению устойчивости функционирования глобального интернета.

Все это привело к стремительному падению цен на услуги IP-транзита, что заставило глобальных Tier 1 начать региональную экспансию. Результатом экспансии в Европу стал следующий размен: глобальных Tier 1 допустили до уровня конечных пользователей, предоставив им доступ к европейской инфраструктуре на участках *последней мили*. За это ряд крупных европейских провайдеров, включая *Deutsche Telekom*, *Telefonica*, *France Telecom*, *Telecom Italia* были включены в клуб глобальных Tier 1, что не привело к увеличению объемов построенной инфраструктуры, но увеличило надежность функционирования сети. Была сформирована региональная европейская интернет-экосистема.

Сегодня таблица глобальных Tier 1 выглядит так[10]:

Наименование компании	Страна	Номер AS	Число подключенных AS
Level 3 Communications (бывшие Level 3, *Global Crossing*)	США	3356/3549/1	4402
AT&T	США	7018	2365
XO Communications	США	2828	2904
Verizon Business (бывший *UUNET*)	США	701, 702	1946
CenturyLink (бывший *Qwest* и *Savis*)	США	209/3561	1367
Sprint	США	1239	1183
Zayo Group (бывший *AboveNet*)	США	6461	1066
GTT (бывший *Inteliquent*)	США	3257	886
NTT Communications (бывший *Verio*)	Япония	2914	718
TeliaSonera International Carrier	Швеция	1299	630
Tata Communications (бывший *Teleglobe*)	Канада	6453	569
Deutsche Telekom AG	Германия	3320	535
Telecom Italia Sparkle (Seabone)	Италия	6762	344
Telefonica	Испания	12956	150
OpenTransit (France Telecom)	Франция	5511	146
*AOL Transit Data Network (ATDN)**	США	1668	
*Cogent Communications**	США	174	3537
*Hurricane Electric**	США	6939	2180

** Существует мнение, что эти операторы осуществляют пиринг на платной основе с отдельными Tier 1.*

На формирование азиатской интернет-экосистемы значительное влияние оказали Китай и Япония. В Китае был поставлен *Великий китайский брандмауэр* с целью не допустить выхода на массовый китайский рынок глобальных сервисов типа *Google* и пр. Это дало возможность активно развивать собственные информационные ресурсы, в том числе *Baidu*, *Alibaba* и пр. Япония самостоятельно производит значительный объем контента, в том числе с использованием *Вокалоид* (*Vocaloid*) — программного обеспечения производства компании *Yamaha Corporation* с технологией полного синтеза речи по правилам с использованием предварительно занесенных в память фрагментов естественного языка.

Поэтому более 80% трафика интернет-экосистем замыкаются внутри этих стран, что делает их слабо зависимыми от авариных ситуаций как на подводных кабельных системах, так и в сетях глобальных Tier 1. Японская компания *NTT Communications* входит в клуб глобальных Tier 1.

В Гонконге и Токио построены крупнейшие точки обмена трафиком, в которых присутствуют фактически все операторы и контент-сервис-провайдеры Тихоокеанского — Южно-Азиатского регионов.

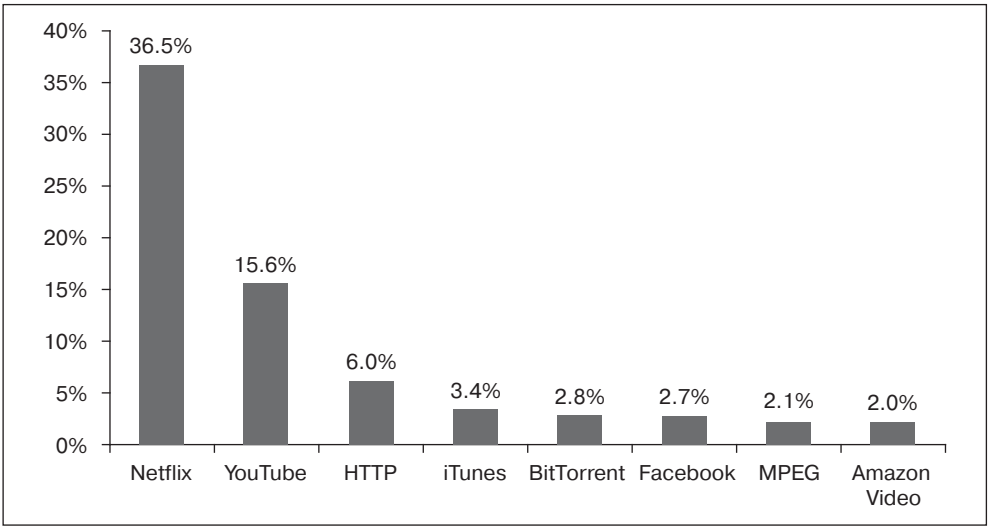
По сообщению издания *New York Times,* в настоящее время Китай ужесточил требования к работе иностранных мессенджеров, в том числе *WhatApp*, *Telegram* и др. По данным *New York Times*, полиция Китая по указу правительства совместно с операторами начала работу по отключению от услуг мобильной связи абонентов, использующих мессенджеры иностранного производства, а также пользующихся услугами VPN.

Кроме того, в Китае была создана и сейчас апробируется новая технология перехвата трафика при обращении к серверам китайской поисковой системы *Baidu*. Если поступивший запрос соответствует определенным критериям, то система внедряет в ответный трафик вредоносный скрипт, с помощью которого власти Китая проводят DDoS–атаки. Технология получила название *Великая пушка* (*Great Cannon*). Пока информации очень мало, и сложно оценить, насколько это нововведение будет представлять собой угрозу для устойчивого функционирования глобального интернета.

Стоит отметить, что не только японская и китайская, но и североамериканская интернет-экосистема сильно замкнута на себя. Впрочем, устроена она несколько иначе. Ее основой является платное телевидение, которое возникло в США и стало самой востребованной услугой на континенте. Поэтому 36% трафика, потребляемого пользователями США, — это трафик крупнейшего контент-сервис-провайдера *Netflix*, до недавнего времени предоставлявшего услуги доступа к контенту только на территории североамериканского континента.

Для пользователей США опасность представляют не выдуманные угрозы вроде российской подводной лодки, которая по непонятным причинам была заподозрена в попытке вывести из строя некую подводную кабельную систему, а постоянные выяснения отношений между теми, кто продает контент через *чужие сети*, и теми, кто эти сети строит и эксплуатирует.

Рисунок 12. **Распределение потребления трафика пользователями США**[11]



ПИРИНГОВЫЕ ВОЙНЫ МЕЖДУ ГЛОБАЛЬНЫМИ TIER 1: ЧТО ВАЖНЕЕ — КОНТЕНТ ИЛИ СЕТЬ

К реальным угрозам для устойчивого функционирования сети интернет на североамериканском континенте можно отнести пиринговые войны между глобальными Tier 1, которые активно велись с конца 90-х до середины 2000-х гг.

В своей книге *The Art of Peering*[12] У. Нортон называет эту тактику пиринга *chicken*. Для целей этой статьи мы будем именовать ее *куриной возней*. Впервые эта тактика была применена в 1990 г. Компании *Genuity (BBN Planet) и Exodus* обменивались большим количеством трафика. В какой-то момент *Genuity* посчитала, что доставлять трафик *Exodus* по всей стране — дорогое удовольствие, за которое *Exodus* должна платить. *Exodus* посчитала, что *Genuity* пытается получить ее контент бесплатно. *Exodus* была уверена, что *Genuity* не положит пир. *Genuity* пир положила. Обмен трафиком возобновился только после того, как *Exodus* организовала несколько точек обмена трафиком на территории США. Эта битва осталась фактически незамеченной ни пользователями, ни регулятором[13].

Следующая битва, которая произошла между *AOL* и *Cogent* в 2003 г., имела куда более значимые последствия. *AOL* посчитала, что паритет в обмене трафиком был нарушен. *Cogent* потребляла в три раза больше, чем отдавала. *Cogent* решила, что *AOL* хочет получить дополнительные деньги за контент, и возразила, что *AOL* не имеет своей инфраструктуры по стране и использует инфраструктуру *Cogent*. Цена вопроса — 75 000 долл. в месяц. Последствия были значительно более печальными, чем в никем не замеченной войне между *Genuity* и *Exodus*, в том числе в школах, подключенных к сети *Cogent*, был ограничен доступ к национальным ресурсам. Произошла перегрузка соединений на пиринге с Level 3. *Cogent* была вынуждена покупать транзит у *AbobeNet* по цене 35 долл. США за 1 Мбит полосы. Позднее договоренности с *AOL* были достигнуты, и пир восстановлен[14].

В 2005 г. *Cogent* поучаствовала в пиринговых войнах сразу с двумя операторами. Сначала *Level 3* посчитал, что его инфраструктура используется *Cogent* для передачи больших объемов трафика, что коммерчески невыгодно для *Level 3. Cogent* ответила, что *Level 3* пытается заставить ее повысить цену на транзит трафика, так как ценовая политика *Cogent* ведет к оттоку клиентов у *Level 3.* В результате клиенты обеих компаний в течение длительного времени имели проблемы с качеством предоставляемых услуг, в том числе голосовых[15].

В 2005 г. *TeliaSonera* посчитала, что она не должна в одностороннем порядке нести затраты на модернизацию инфраструктуры, используемую в том числе *Cogent*. *Cogent* посчитала несправедливым оплачивать расходы. Пострадали клиенты обеих компаний. В итоге договоренности были достигнуты, пир восстановлен[16].

В 2008 г. аналогичный спор возник у *Cogent* с компанией *Sprint*, которая решила, что паритет трафика был нарушен, и захотела пересмотреть условия соглашения о пиринге. *Cogent* посчитала, что *Sprint* нарушила имевшиеся договоренности. Пострадали клиенты обеих компаний. В итоге договоренности были достигнуты, пир восстановлен[17].

После 2008 г. крупнейшие операторы США вели войну с *Netflix*, пытаясь выставить заградительные цены и ухудшить качество услуг доступа своих клиентов к контенту, распространяемому через платформу *Netflix*. Результатом этих войн стало при-

нятие пакета документов, определивших новые правила для открытого интернета (*Open Internet Order)*[18]. В тексте 400-страничного документа *Cogent* и ее войны упоминаются неоднократно. Чтобы избежать подобных инцидентов, регулирование, в том числе пиринговых отношений, будет осуществляться в рамках прецедентов в режиме *легкого касания*. Основная задача участников рынка — договориться друг с другом.

ФОРМИРОВАНИЕ РОССИЙСКОЙ ИНТЕРНЕТ-ЭКОСИСТЕМЫ

В Российской Федерации развитие интернета в конце 90-х гг. шло неравномерно, со значительным отставанием регионов. Это было связано с достаточно высокими ценами на аренду каналов связи до Москвы и Санкт-Петербурга, куда приходили международные каналы связи и где активно развивались региональные информационные ресурсы.

В 1998 г. ОАО *Ростелеком* (в настоящий момент ПАО *Ростелеком*) начало реализацию первого проекта по созданию опорной сети интернета в Российской Федерации. Позже развитием проекта строительства опорной инфраструктуры занялось ЗАО *Компания ТрансТелеком*. Однако в 2001 г. интернет–бизнес ОАО *Ростелеком* был передан в дочернюю компанию ОАО *РТКомм.РУ* (в настоящий момент ПАО *РТКомм.РУ*, занимается развитием систем спутниковой связи). В это же время ЗАО *МТУ-Интел* начало реализацию масштабного проекта по предоставлению массовых услуг широкополосного доступа с использованием технологии для подключения конечных пользователей в Москве.

В 2001 г. на рынок услуг российского IP-транзита начала активное продвижение компания *Cable&Wireless*, предлагая очень низкие цены на свои услуги в расчете на то, что 75–80% проданного ей трафика окажется российским, в связи с чем затраты на его пропуск будут равны затратам на пропуск трафика между двумя портами одного маршрутизатора.

Одновременно с этим ЗАО *Компания ТрансТелеКом* вышло на рынок с предложением доплачивать всем информационным ресурсам, которые создают трафик, потребляемый клиентами компании. Пиринговые соединения между российскими провайдерами в этот период в основном осуществлялись через точку обмена трафиком без особых правил и условий.

Если бы *Cable&Wireless* удалось реализовать свои идеи о получении значительной доли рынка российского IP-транзита, российская интернет-экосистема не сформировалась бы, а устойчивость функционирования российского сегмента сети интернет во многом определялась бы устойчивостью функционирования европейского сегмента глобальной сети интернет.

В начале 2000-х гг. рынок сформировал экономические предпосылки для прекращения бесплатного или условно бесплатного пиринга между крупными и относительно небольшими сетями в Российской Федерации. В это время крупные игроки рынка осознали, что с точки зрения экономики бесплатный пиринг — это разрыв *value chain*. При сохранении бесплатного пиринга крупные игроки, на тот момент начинающие вкладывать существенные средства в развитие инфраструктуры своих сетей, по сути предоставляли эту инфраструктуру всем своим партнерам по пирингу бесплатно. В результате небольшие операторы стали получать

необоснованное экономическое преимущество, так как бесплатно пользовались инфраструктурой пропуска межрегионального трафика, построенной крупными игроками.

В то же время политика некоторых крупных игроков российского рынка была непродуманной и популистской. Так, например, отдельные игроки лоббировали идею о внедрении в России механизма возмещения владельцам информационных ресурсов в сети интернет затрат на создание, производство и распространение в интернете контента. Основной аргумент, который использовался сторонниками популистских идей о *доплате за контент*, заключался в следующем: без контента интернет никому не будет интересен, и пользоваться им не будут, у владельцев информационных ресурсов нет возможности заработать в интернете, поэтому операторы связи должны делиться с ними своими доходами.

Затраты на создание, производство и распространение контента в интернете предлагалось возместить путем перечисления контент-провайдерам части доходов, собираемых с абонентов, пользователей и операторов за услуги доступа в интернет и услуги транзита трафика (IP-транзита), в виде оплаты за несуществующие услуги по пропуску трафика, сгенерированного информационными ресурсами. За основу предлагалось взять модель расчетов в сетях телефонной связи, работающую по принципу *платит звонящий*.

Иными словами, контент-сервис-провайдерам предлагалось не только бесплатно использовать инфраструктуру операторов связи для доставки информации потенциальной целевой аудитории, но и получать доплату за использование инфраструктуры операторов связи.

Подобные идеи были крайне вредны для развивающегося российского интернет-рынка. Модели расчетов, используемые в сетях телефонной связи, никогда не использовались и не могли использоваться ни в одной стране мира при построении взаимодействия между участниками рынка в сети интернет. Кроме того, реализация подобных идей привела бы к затормаживанию и замораживанию развития рынка интернет-рекламы.

Таким образом, в начале 2000-х гг. экономические предпосылки и непродуманные, популистские идеи отдельных участников рынка подтолкнули трех ведущих на тот момент российских интернет-провайдеров: ЗАО *МТУ-Интел*, ОАО *РТКомм.РУ* и ООО *Телеросс* (входило в группу компаний *Golden Telekom*, присоединено к ОАО *Вымпелком*, в настоящий момент ПАО *ВымпелКом*) к достижению договоренностей о создании *отдельной пиринговой группы*, положившей основу для формирования региональных Tier 1 на территории Российской Федерации.

Условия участия в *отдельной пиринговой группе* включали соглашения о паритетных объемах трафика на пиринговых стыках, которые не могут быть ниже установленного порогового значения, о наличии присоединения к глобальному интернету не менее чем в двух точках за пределами территории Российской Федерации, для чего требовалась аренда международных каналов связи, а также стандартные положения о том, что каждый новый член *отдельной пиринговой группы* должен стать пиринг-партнером всех участников группы.

Несмотря на критику со стороны многих российских интернет-сервис провайдеров, не попавших в *отдельную пиринговую группу* из-за невозможности выполнения всех условий, ее создание привело к:

- значительному снижению цены на аренду международных каналов связи;
- стимулированию строительства трансграничных переходов;
- замыканию российского трафика внутри России, несмотря на то что первое время существовало большое число *зарубежных петель*;
- снижению заинтересованности зарубежных операторов осуществлять продажи трафика на территории Российской Федерации в связи с отсутствием экономической целесообразности и из-за низких объемов продаж;
- активному развитию точек обмена трафиком, в первую очередь московской точки обмена трафиком (*MSK-IX*);
- активному развитию российского рынка интернет-рекламы силами российских контент-сервис-провайдеров.

Число и состав участников *отдельной пиринговой группы* менялись с течением времени. В настоящий момент в нее входят все ключевые операторы, сети которых составляют основу опорной региональной инфраструктуры Российской Федерации.

Следует отметить, что отголоски идей о необходимости на законодательном уровне стимулировать операторов (путем наложения соответствующих обязательств) возмещать производителям контента затраты на его производство и распространение в сети интернет за счет средств, собираемых с абонентов и пользователей, которым предоставляются услуги доступа, нашли свое продолжение в конце 2014 г. в предложениях отдельных представителей правообладателей по внедрению механизма *Глобальной лицензии*, но в 2014 г. указанные предложения встретили жесткую критику со стороны всех без исключения участников интернет-рынка[19].

Формирование *отдельной пиринговой группы* позволило создать в России региональную интернет-экосистему, 80% трафика которой замыкается внутри нее, что в значительной степени снижает зависимость от устойчивости функционирования сетей глобальных Tier 1.

Подавляющее большинство российских операторов уровня региональных Tier 2, Tier 3 и пр. имеют подключения не менее чем к двум региональным российским Tier 1. Российские контент-сервис-провайдеры (в терминах российского законодательства в области информации, информационных технологий и защиты информации *организаторы распространения информации в сети интернет* или *операторы поисковых систем*), как правило, имеют подключение ко всем российским операторам уровня регионального Tier 1, что обеспечивает возможность *лучшего доступа* к ресурсам организаторов распространения информации в сети интернет и операторов поисковых систем к своим пользователям. Поэтому обеспечить отключение всех российских пользователей от глобальной сети интернет силами одного оператора даже уровня регионального Tier 1 не представляется возможным.

С учетом анализа, приведенного выше, можно считать, что рассказ об учениях по отключению российских пользователей от глобального интернета силами одного оператора можно также считать мифом.

Для отключения всех российских пользователей от глобального интернета надо, чтобы все российские операторы, построившие трансграничные переходы, прекратили пропуск трафика через эти переходы. Это невозможно по ряду причин. Во-первых, голосовой (телефонный) трафик передается по той же инфраструктуре, по которой осуществляется передача интернет-трафика, следовательно, пострадает не только доступ в интернет, но и услуги междугородной телефонной связи и роуминга. Во-вторых, российские операторы осуществляют продажу интернет-трафика операторам из других стран, в том числе из Евразийского экономического союза. В-третьих, через территорию Российской Федерации осуществляется транзит трафика, в том числе между Европой и Азией.

РАЗМЕЩЕНИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ ЗАРУБЕЖНЫХ КОНТЕНТ-СЕРВИС-ПРОВАЙДЕРОВ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

В связи с усилением конкуренции и необходимостью обеспечения качественного доступа к создаваемым и эксплуатируемым информационным ресурсам многие глобальные контент-сервис-провайдеры, включая *Google*, *Akamai*, *CDN Level 3* и др. заинтересованы в размещении своих серверов на территории Российской Федерации. Размещение серверов осуществляется по двум основным алгоритмам. Серверы размешаются в точках обмена трафиком или на других независимых площадках (ЦОД, Telehouse). Доступ к серверам предоставляется всем операторам связи, а также юридическим лицам, не являющимся операторами связи в соответствии с законодательством Российской Федерации, но желающим получить доступ к контенту.

Другой алгоритм предполагает размещение кэширующих серверов непосредственно на площадках каждого оператора, чья абонентская база представляет интерес для контент-сервис-провайдера. Размещение серверов глобальных контент-сервис-провайдеров на территории Российской Федерации интересно как российским операторам связи, так и глобальным контент-сервис-провайдерам: оператор получает возможность сократить свои затраты на аренду международных каналов связи и улучшить качество услуг, предоставляемых абоненту, а глобальный контент-сервис-провайдер получает доступ к потенциальной целевой аудитории контент-смотрителей.

Такой подход также позволяет повысить устойчивость функционирования глобального интернета для региональных пользователей.

ЗАКЛЮЧЕНИЕ

«Слух о моей смерти был сильно преувеличен», — писал в телеграмме *Ассошиэйтед Пресс* американский писатель С. Клеменс, творивший под псевдонимом Марк Твен.

Слухи о ненадежности функционирования глобальной инфраструктуры интернета, о возможных нарушениях глобальной связности в случае обрыва одного из кабелей, а также о возможности отключения российских интернет-пользователей силами одного оператора преувеличены значительно больше.

На поверку глобальный интернет оказывается более устойчивым к внешним воздействиям, чем многие другие сервисы, в первую очередь голосовые, а также сервисы, предоставляемые корпоративным клиентам, в том числе транснациональным корпорациям.

Глобальный интернет является величайшим достижением и изобретением человеческого гения. В нем нет центров управления трафиком, нет единой точки отказа, так как нет единой или даже нескольких точек управления или принятия решений.

Протокол IP обеспечивает доставку пакета между любыми двумя подключенными к сети устройствами, если функционирует хотя бы один маршрут (присутствует связность сети). В глобальном интернете нет глобальных элементов за исключением систем уникальных идентификаторов: IP-адресов, номеров AS и системы доменных имен. Именно поэтому интернет бесконечно масштабируем и адаптируется к любому изменению в структуре и технологиях доступа, с одной стороны, и технологиях сервисов, предоставляемых через интернет, с другой.

Но это не означает, что интернет выдержит любые эксперименты, в том числе проводимые отдельными министерствами и ведомствами, которым проще запретить пугающее новое, чем научиться жить в новой реальности. Такие эксперименты не приведут к тому, что глобальный интернет разрушится или исчезнет, но они чреваты тем, что государство, их ставящее, может быть отброшено лет на двадцать назад, и отставание это в век стремительно развивающихся технологий наверстать будет нереально. Сегодня между словами *интернет* и *инновации* можно смело ставить знак равенства. Некоторые эксперты, в том числе выдающийся экономист Й. Шумпетер, ставили знак равенства и между *инновациями* и *экономическим ростом*. Он был убежден, что только страны, в которых делаются открытия, богатеют, а остальные ожидает застой. Й. Шумпетер был также убежден в том, что процесс инноваций никогда не бывает мирным и спокойным, это жестокий цикл разрушения старых и рождения новых отраслей, который безжалостен и неумолим, как и все остальные законы природы.

Чему учит нас эта история? Пожалуй, тому, что интернет — это новая реальность, становление которой еще не завершилось, и в которой нам придется научиться жить, адаптируясь ко все новым переменам.

Примечания

1 Источники: http://www.cablemap.info, http://submarine-cable-map-2015.telegeography.com/

2 Или на сайте Greg's Cable Map по адресу http://www.cablemap.info/

3 Источник: http://news.bbc.co.uk/2/hi/asia-pacific/6213501.stm

4 Источник: http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a3tADKd_tY3g&refer=europe

5 Источник: http://www.itnews.com.au/news/telstra-iphone-mac-users-report-crippling-speeds-to-apple-services-410006

6 Источник: http://drpeering.net/white-papers/Ecosystems/Tier-1-ISP.html

7 Работы можно найти по адресу http://www.drpeering.net/

8 Источник: http://drpeering.net/white-papers/A-Business-Case-For-Peering.php

9 Источник: http://www.drpeering.net/

10 Источник: http://as-rank.caida.org/?mode0=as-info&mode1=as-table&as=3320

11 Источник: http://marketrealist.com/2015/07/youtube-started-replace-tv-viewing/

12 Источник: http://drpeering.net/white-papers/Art-Of-Peering-The-Peering-Playbook.html

13 Источник: http://seclists.org/nanog/2010/Nov/1014

14 Источники: http://www.dslreports.com/shownews/24809, http://legalminds.lp.findlaw.com/list/cyberia-l/msg42080.html

15 Источники: http://www.computerworld.com/article/2559599/networking/level-3--cogent-resolve-peering-dispute — renew-deal.html, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

16 Источник: http://gigaom.com/2008/03/14/the-telia-cogent-spat-could-ruin-web-for-many/

17 Источник: http://arstechnica.com/uncategorized/2008/10/cogent-picks-peering-fight-with-zombie-sprint/

18 Документ можно найти по адресу https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf).

19 Механизм Глобальной лицензии впервые был предложен William Fisher в работе *Promises to Keep Technology, Law, and the Future of Entertainment*, вышедшей в свет в США в 2004 г. В США эта идея внедрения механизма Глобальной Лицензии была отвергнута. В 2008 г. работа Фишера была переведена на русский язык. Попытка законодательно закрепить механизм Глобальной Лицензии была предпринята в России в 2014 году представителями Российского Авторского Общества.

Мария Роскошная, Евгений Харьковский

3D-ПЕЧАТЬ И ЭКСПОРТНЫЙ КОНТРОЛЬ: НАПЕРЕГОНКИ СО ВРЕМЕНЕМ

ВВЕДЕНИЕ

Изменения, происходящие сегодня, позволяют говорить, что мы стоим на пороге новой промышленной революции. Предвестником ее можно назвать появление аддитивных технологий (3D-печати). Страны, сделавшие на них ставку, в будущем займут наиболее выгодные и перспективные позиции в промышленном производстве. Совершенствование существующих и появление новых технологий и производств регулярно вызывают необходимость пересмотра действующих контрольных списков международных режимов экспортного контроля. Наиболее уместно обсуждать вопрос контроля аддитивного производства в рамках трех из четырех действующих международных режимов экспортного контроля: Австралийской группы (АГ), Вассенаарских договоренностей (ВД), Группы ядерных поставщиков (ГЯП), Режима контроля за ракетной технологией (РКРТ).

Справочно

- *Австралийская группа (АГ) — объединение государств, созданное в 1985 г. и состоящее в настоящее время из 40 стран-членов и Европейской Комиссии в качестве дополнительного самостоятельного участника, включает все промышленно развитые страны. Россия не является членом указанного режима, целью которого является выработка экспортно-контрольной позиции по предотвращению распространения химического и биологического оружия.*
- *Вассенаарские договоренности (ВД) по экспортному контролю за обычными вооружениями, товарами и технологиями двойного назначения — объединение государств, созданное в 1996 г. и насчитывающее 41 государство-участник. Россия является одним из сооснователей этого режима, цели которого — укрепление региональной и международной безопасности путем предотвращения дестабилизирующих накоплений обычных вооружений.*
- *Группа ядерных поставщиков (ГЯП) — режим, созданный в 1975 г. для выработки и согласования норм в области ядерного экспортного контроля. В 1978 г. в ГЯП были разработаны Руководящие принципы ядерного экспорта, опубликованные в виде*

Информационного циркуляра МАГАТЭ (INFCIRC/254), которые модифицируются с учетом развития ядерных технологий. Членами Группы являются 48 государств, в том числе все промышленно развитые страны и Россия как правопреемница СССР.

- *Режим контроля за ракетной технологией (РКРТ) — объединение стран, разделяющих общую цель — предотвращение распространения ракет и беспилотных летательных аппаратов, пригодных для доставки ОМУ; режим создан в 1987 г., насчитывает 34 государства, включая все промышленно развитые страны. Россия стала членом РКРТ в 1995 г.*

Аддитивные технологии (АТ), широко известные как технологии 3D-печати, уже отнесены к категории *передовых производств* (advanced manufacturing) по классификации, введенной П. Фоулером (Paul Fowler) из Национального совета по перспективным производственным технологиям США (National Council for Advanced Manufacturing, NACFAM)[1]. К отличительным особенностям такого производства относят возможность его кастомизации, что означает простоту перестройки производства с применением цифровых технологий с целью удовлетворения новых или меняющихся потребностей заказчиков.

Данные технологии позволяют во многих случаях отказаться от избыточного процесса металлообработки, свойственного традиционным способам производства. Различие заключается в том, что традиционные технологии являются *вычитающими*, то есть изготовление происходит посредством обработки первичного материала с неоправданной с экономической и технологической точки зрения потерей большого количества полезного материала. Аддитивное производство (АП) можно отнести к *добавляющей* технологии на основе применения послойного синтеза и трехмерной компьютерной модели. К отличительным особенностям подобного производства можно также отнести возможности по созданию различных деталей с переменными по толщине свойствами материала, сложных конструкций по принципу *деталь в детали*, пустотелых объектов, матричных и сетчатых конструкций, которые не представляется реальным получить при помощи другого существующего производственного и обрабатывающего оборудования.

В отличие от первых комплексов АТ, использующих преимущественно полимерные материалы, появление возможности работы с более высокотехнологичными материалами выводит этот класс оборудования на новый уровень и существенно расширяет варианты его применения. В первую очередь, двигателем развития аддитивных технологий выступают оборонно-промышленный комплекс и медицинская отрасль. Инициируются государственные программы и открываются исследовательские центры по изучению АТ. Активно осваивают эти передовые производства и промышленные гиганты, такие как *General Electric (GE), Airbus, Siemens* и др.

АТ В СТРУКТУРЕ МИРОВОГО ПРОМЫШЛЕННОГО ПРОИЗВОДСТВА

Доля АТ в общей структуре производства постепенно растет, приобретая промышленные объемы. Так, еще в 2013 г. общий объем рынка АТ составлял немногим более 3 млрд долл. США, показывая ежегодный темп прироста в среднем около 25–30%, включая производство оборудования, изготовление материалов, разработку цифровых 3D-моделей и технологические процессы, им сопутствующие. Мировой рынок аддитивных технологий продолжает расти почти на 30%

в год и к 2017 г. приблизится к отметке 6 млрд долл. США, а к 2020 г. по прогнозам достигнет 10,8 млрд долл.[2].

Уже сейчас *Boeing* ежегодно изготавливает с помощью АТ более 20 тысяч деталей трехсот наименований для десяти военных и коммерческих самолетов и даже подала патентную заявку на производство деталей для воздушных судов с помощью 3D-печати[3]. Не отстает и *Airbus*, которая активно использует для своих воздушных судов детали, созданные посредством АТ[4]. В свою очередь, у компании *GE* детали (в т. ч. для газотурбинных и реактивных двигателей), изготовленные с помощью 3D-принтеров, становятся ключевым элементом производственной цепочки[5]. Первые лабораторные эксперименты *GE* показали, что послойная печать инжектора из кобальт-хромового порошка позволяет улучшить его качественные характеристики, делает деталь легче и долговечнее. Инженеры *GE* также придумали использовать технологию лазерного спекания для изготовления кромки лопасти двигателя из титанового порошка. Интеграция деталей в полномасштабный производственный цикл планируется в 2016 г. Вскоре инженеры *GE Aviation* намерены включить в производство новые материалы, такие как титан, алюминий и никель-хромовые сплавы, рассчитывая добиться лучших характеристик деталей, недостижимых при использовании технологии литья[6]. Переход на аддитивные технологии может сэкономить компании порядка 25 тыс. долл. США на каждом двигателе, что говорит не только о возрастающих объемах применения АТ, но и о коммерческой целесообразности широкого внедрения технологии в производственные циклы.

С точки зрения создания благоприятных условий для развития АТ показателен пример США, Европы и КНР[7]. Так, в США порядка трех лет функционирует специализированный институт, развивающий инновационное аддитивное производство — Национальный институт развития инновационных аддитивных технологий (National Additive Manufacturing Innovation Institute) — чей парк включает различное оборудование, умеющее, в том числе, производить детали из металлических порошков[8]. Крупнейшая в мире компания-интегратор АТ — американская *3D-Systems*. Она даже создала собственный университет по подготовке кадров, способных в дальнейшем работать с АТ. В проектах развития АП в США принимают участие не только представители бизнеса, непосредственными игроками являются также федеральные министерства и департаменты, научные фонды и даже NASA[9]. Китай, в свою очередь, также активно фокусируется на создании научной и образовательной среды под дальнейшую разработку и применение АТ. При этом специалисты из Поднебесной уже сегодня активно используют прикладные научные разработки: они способны изготавливать пластины для черепно-мозговой хирургии (краниопластики) не только в мирное время, но и в военно-полевых условиях.

На сегодняшний день головным центром по производству 3D-принтеров является Европа. Первые пять наиболее влиятельных производителей подобного оборудования представлены немецкими компаниями *Voxeljet, SLM Solutions, EOS GmbH, Concept Laser, Realizes*[10]. Далее следуют шведская *Arcam*, французская *Phenix Systems* и компания из Великобритании — *Renishaw*. На этом участие Европы в развитии отрасли аддитивных технологий не заканчивается: с 2012 г. совместно с Европейским космическим агентством запущен проект AMAZE, целью которого является создание металлических изделий высокого качества, способных работать в экстремальных условиях[11]. По данным американской консалтинговой компании *Wohlers Associates*, наибольший спрос на аддитивные технологии наблюдается в потребительском секторе товаров и электроники (22% выручки индустрии 3D-печати по ито-

гам 2012 г.), автомобильной промышленности (19%), медицине и стоматологии (16%), на производстве (13%), в авиакосмической отрасли (10%).[12]

Сказанное выше позволяет сделать вывод о том, что АТ вышла на уровни промышленного производства, и уже уместно говорить о необходимости введения ее экспортного контроля. При этом серьезным вызовом выступает отсутствие стандартизации и сертификации АТ и оборудования, участвующего в АП.

ПРОМЫШЛЕННОЕ ОБЪЕДИНЕНИЕ

Также примечателен факт создания *закрытого клуба* государств-производителей — Глобального альянса ассоциаций быстрого прототипирования (Global Alliance of Rapid Prototyping Associations, GARPA)[13], объединяющего 22 страны с уже созданными национальными ассоциациями по АТ. Альянс проводит ежегодные глобальные саммиты для обмена мнениями и информацией в области АТ на межстрановом уровне. Государства-участники GARPA проводят технические презентации и конференции совместно с представителями промышленности. Кроме того, члены альянса участвуют в бизнес-встречах и социальных мероприятиях, публикуют статьи, кейсы и прочие информационные материалы по тематике АТ. К большому сожалению, у альянса есть и серьезные недостатки. Речь идет о его закрытости, склонности манипулировать рынком за счет санкционных режимов и дифференцированных подходов к ценообразованию, а также об удержании коммерческой тайны в отношении технологии производства (важно отметить, что в интересах нераспространения этот фактор играет положительную роль, поскольку условия производства держатся разработчиками технологии в секрете, большинство эксплуатирующих аддитивное оборудование организаций закупают порошки, а настройки и среда для работы с ними изначально запрограммированы в оборудовании).

Россия не является членом объединения. Условием вступления в GARPA является наличие собственного производства с большими объемами выпускаемой продукции. Пока вклад России в рынок аддитивных технологий оценивается в 1,5% (в основном это результат работ в области лазерной стереолитографии, которые были выполнены еще в СССР под руководством академика РАН В. Панченко в Институте проблем лазерных и информационных технологий (ИПЛИТ) РАН)[14], а за последние 15 лет в нашей стране выдан только 131 патент по различным аспектам аддитивного производства, что составляет 0,14% от общемирового показателя[15].

ТЕХНИЧЕСКИЕ ОСОБЕННОСТИ

Аддитивные технологии включают несколько способов производства, условно подразделяясь по двум способам нанесения материала (струйный и лазерный). Ключевую роль играет производство порошков, поскольку от качества порошка в первую очередь зависит качество получаемых деталей. Материалами изготовления могут выступать как пластик, поликарбонат и др., так и более технологичные металлические порошки и даже живые клетки. Для целей экспортного контроля целесообразно рассматривать именно *чувствительные* с точки зрения распространения материалы, то есть металлические порошки, и оборудование для их производства.

Существует несколько видов АТ, использующих металлические порошки. Сфокусируемся на двух. В обоих случаях процесс изготовления детали начинается

с построения компьютерной модели изделия. Затем модель программно рассекается на тонкие слои, чтобы получить информацию о контуре каждого слоя, который воспроизводится при изготовлении детали. При этом отмечается определенный вызов для системы экспортного контроля, называемый обратное построение (reverse-engineering), сводящийся к тому, что для построения 3D-моделей первично проводится полное оцифровывание и сканирование готового изделия для дальнейшего построения его цифрового прототипа (3D CAD model), а значит, есть риск, что недобросовестные производители могут получить подобные сведения об оригинальных изделиях и их моделях.

Первый вид, именуемый *селективный синтез* или *селективное лазерное сплавление* (SLS — Selective Laser Sintering)[16], предполагает нанесение на рабочую поверхность дозы порошкового материала со вспомогательной платформы и разравнивание его с помощью ролика или *ножа* для создания слоя материала заданной толщины с последующей выборочной обработкой порошка лазером согласно текущему сечению математической модели детали, сплавлением частичек порошка и дальнейшим поднятием вспомогательной платформы на толщину слоя для повторения процесса.

Второй вид выполняется *прямым осаждением материала* (direct deposition)[17]: газопорошковая смесь подается вдоль общей оси лазерного луча (коаксиально), непосредственно в точку, куда подводится энергия и где происходит в данный момент построение фрагмента детали. Плюсом данного вида является возможность не ограничиваться в размерах деталей. Используемое оборудование, как правило, имеет пятикоординатное управление. Три координаты — вращение роботизированной рабочей головки, а в двух координатах перемещается стол.

Описание видов АТ дает возможность сделать вывод о необходимости стандартизации и сертификации оборудования, используемого в АП, и выделить несколько технических параметров в качестве критериев для возможного осуществления экспортного контроля. К ним относятся осевая (координатная) обработка, особенности порошковых материалов, используемое программное обеспечение. Рассмотрим их подробнее.

ОСЕВАЯ (КООРДИНАТНАЯ) ОБРАБОТКА, СТАНДАРТИЗАЦИЯ И СЕРТИФИКАЦИЯ

С осевой обработкой как потенциальным техническим критерием, который может быть использован в контрольных списках для целей экспортного контроля, все относительно понятно: достаточно просто обеспечить контроль пятиосевого оборудования 3D-печати (в случае прямого осаждения материала), так и, вероятно, трехосевого оборудования (для селективного лазерного сплавления)

Более сложными и важным в интересах экспортного контроля представляются вопросы стандартизации и сертификации. Отсутствие базы национальных стандартов для аддитивного производства тормозит развитие национальной аддитивной отрасли и препятствует осуществлению экспортного контроля на международном уровне. В России давно назрела необходимость формирования системы стандартизации и сертификации аддитивных изделий, технологических процессов, порошков и композиций с целью одинакового понимания и соблюдения разработчиками типовых технических требований. Более того, сложности вызывает не только отсутствие стандартов для различных отраслей или даже отставание позиции какого-либо государства по внедрению существующих международ-

ных стандартов. Данная проблема особо остро проявилась в рамках ведущегося в настоящее время обсуждения изменения подходов к контролю высокоточных станков с числовым программным управлением[18*] в рамках Вассенаарских договоренностей и Группы ядерных поставщиков.

Стремясь к либерализации экспортного контроля**, Российская Федерация и ряд других стран в рамках ВД поспешно согласились с принятием нового подхода к контролю станочного оборудования на основе измерения *однонаправленной повторяемости позиционирования* (unidirectional positioning repeatability, UPR) вместо ранее использовавшегося в режиме для целей экспортного контроля критерия *точности позиционирования* (positioning accuracy, PA). В результате в рамках ВД принят новый параметр контроля, а в ГЯП серьезная дискуссия относительно отказа от используемого на сегодняшний день критерия *точности позиционирования* все еще продолжается. В итоге, когда принятый в рамках ВД новый подход будет имплементирован в соответствующие национальные контрольные списки, у государств, которые являются также государствами-участниками ГЯП, контроль должен остаться без изменений — на основе параметра точности позиционирования станков***. В странах, где существует единый экспортноконтрольный список, возникнет еще большая путаница в выборе контрольных параметров станков.

Справочно

* *Числовое программное управление (ЧПУ) станка — это управление обработкой заготовки на станке по специальной программе, в которой данные об обработке заданы в цифровом коде. Система ЧПУ — это совокупность функционально взаимосвязанных технических и программных методов и средств, обеспечивающих числовое программное управление станком.*

** *Достигается, как правило, исключением какого-либо оборудования из контрольных списков, а также изменением пороговых значений контрольного параметра или изменением текста пунктов контрольных списков таким образом, что ранее контролировавшееся оборудование в новой редакции не подпадает под действие контрольных списков, облегчая таким образом участникам внешнеэкономической деятельности процедуры закупки оборудования.*

Стоит при этом отметить, что ряд государств в подобной ситуации могут злоупотреблять механизмом всеобъемлющего контроля (так называемый catch all*) для неподпадающего под действие контрольных списков оборудования. В законодательстве Российской Федерации механизм всеобъемлющего контроля регламентирован:*

- *Статьей 20 Федерального закона № 183-ФЗ «Об экспортном контроле» от 18 июля 1999 г.;*
- *Постановлением Правительства Российской Федерации от 15 августа 2005 г. № 517.*

*** *В ряде случаев, как например, с высокоточными станками с ЧПУ, оборудование может подпадать под действие нескольких контрольных списков. При этом в связи особенностями конкретного списка и его целями для контроля могут использоваться разные технические критерии или разные пороговые значения одного и того же технического критерия.*

В законодательстве Российской Федерации контрольные списки ГЯП имплементированы в качестве Списка ядерных материалов, оборудования, специальных неядерных материалов и соответствующих технологий, подпадающих под экспортный контроль, утвержденного Указом Президента Российской Федерации от 14.02.96 № 202 (Список № 202), а также Списка оборудования и материалов двойного назначения и соответствующих технологий, применяемых в ядерных целях, в отношении которых осуществляется экспортный контроль, утвержденного Указом Президента Российской Федерации от 14 января 2003 г. № 36 (Список № 36).

Список ВД имплементирован в качестве Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль, утвержденного указом Президента Российской Федерации от 17 декабря 2011 г. № 1661 (Список № 1661).

В настоящее время большинство участников ГЯП согласно с актуальностью изменения подхода к экспортному контролю станочного оборудования и с необходимостью сужения сферы охвата контроля. Важно также обратить внимание, что для изготовления ряда ключевых компонентов продукции, используемой в ядерных целях, наприме, цилиндров роторов газовых центрифуг или трубок тепловыделяющих элементов, в силу их цилиндрической симметрии достаточно использования 2 осевой координатной обработки.

Данная трактовка позволяет сделать вывод, что контроль в рамках ГЯП оправданно носит более жесткий характер и должен осуществляться начиная со станков с двумя осями, которые могут быть совместно скоординированы для контурного управления, а не 4- или 5-осевых, как было предложено иностранными делегациями в режимах. Унификация контрольных параметров станков в ВД и ГЯП не является бесспорной, а слепую погоню за гармонизацией контроля в различных международных режимах в части станочного оборудования нельзя оправдывать необходимостью либерализации экспортного контроля.

Стоит также отметить, что изменение контрольного параметра на *однонаправленную повторяемость позиционирования* потребует срочно находить ответы на ряд нерешенных вопросов и может привести к сложностям контроля поставок выпускаемых и ранее выпущенных станков (в ходе дискуссий в рамках режимов используются среди прочих понятия *legacy machine tools* и *used machine tools*), не имеющих в своих технических спецификациях параметра *однонаправленная повторяемость позиционирования*.

Проявились и политические аспекты. Так, отдельные государства (например, Китай и Бразилия) являются членами одного режима (ГЯП) и не являются членами другого (ВД). Это означает, что в случае выведения из-под действия контрольных списков ГЯП высокоточных станков данные государства могли бы экспортировать их, минуя этап лицензирования. Это, в свою очередь, давало бы их промышленным производителям станков значительные конкурентные и временные преимущества, в том время как экспортеры государств-участников обоих режимов (ГЯП и ВД) по-прежнему вынуждены были бы обращаться в контрольные органы за получением разрешительных документов.

Все эти сложности подводят к тому, что в случае начала обсуждения механизмов контроля АТ и сопутствующих материалов, оборудования и программного обеспечения, российская делегация в рамках всех режимов должна иметь позицию, согласованную на национальном уровне. На международном уровне обсуждение АТ в контексте экспортного контроля уместно было бы производить в формате совместных рабочих групп отдельных режимов, а также по аналогии совместных экспертных семинаров ГЯП-ВД по изменению контроля за экспортом высокоточных станков с дополнительным привлечением РКРТ.

МАТЕРИАЛЫ И ОБОРУДОВАНИЕ ПОРОШКОВОГО ПРОИЗВОДСТВА

Существующие контрольные списки международных режимов предполагают контроль ряда материалов, применяемых в АП. Это, к примеру, алюминиевые сплавы, мартенситностареющие стали, титановые сплавы, контролируемые по пунктам 2.3.1, 2.3.11 и 2.3.13 соответственно Списка № 36. Данные позиции контрольного списка соотносятся с пунктами 2.С.1 (алюминиевые сплавы), 2.С.11 (мартенситностареющая сталь), 2.С.13 (титановые сплавы) части 2 Руководящих принципов для передач имеющих отношение к ядерной деятельности оборудования, материалов, программного обеспечения и соответствующей технологии двойного использования (Руководящие принципы) ГЯП (INFCIRC254p2, действующая редакция № 9). Контроль материалов или сплавов предусмотрен также и рядом позиций Списка № 1661. Порошковые композиции обозначены в явном виде, к примеру позицией 4.3.2.3 Списка № 1005. Список оборудования, материалов и технологий, которые могут быть использованы при создании ракетного оружия и в отношении которых установлен экспортный контроль, утвержденный Указом президента Российской Федерации от 08.08.2001 № 1005 (Список № 1005). Однако закономерен вопрос о необходимости широкого контроля порошков, поскольку уже в настоящее время можно обнаружить пробелы в экспортноконтрольном законодательстве.

Вышеназванными пунктами контролируются, к примеру, титановые сплавы с пределом прочности на растяжение не менее 900 МПа (при 293 К/20 град. С) в форме труб или цилиндрических стержней и мартенситностареющая сталь с пределом прочности на растяжение не менее 1950 МПа (при 293 К/20 град. С).

Пробел в данном случае заключается в возможности закупки порошковой композиции и изготовления данных предметов с использованием АТ, обходя экспортноконтрольные процедуры. Похожая ситуация сложилась с алюминиевыми сплавами. Более того, можно произвести не просто металлические заготовки, а создать в точке конечного использования в обход экспортного контроля контролируемое оборудование, такое как детали из мартенситностареющих сталей для газодиффузионного обогащения. В случае обсуждения возможных вариантов контроля порошковых композиций, следует обратить внимание на такой технический параметр, как фракция порошка. На сегодняшний день существует множество их разновидностей.

Получение и применение металлопорошковых композиций является важным технологическим аспектом аддитивного производства. Они могут варьироваться как по своим физическим свойствам (размеру и однородности фракций), так и по химическому составу. В зависимости от используемого порошка меняется рельефность мелких деталей, их поверхность можно сделать более гладкой, либо, в случае значительного уменьшения размера фракции, возможно разбрызгивание расплава, а следовательно, увеличение шероховатости детали и ее микропори-

стости. С точки зрения размера порошки условно подразделяются на нанодисперсные с диаметром частиц менее 0,1 мкм, ультрадисперсные с диаметром 0,1–1,0 мкм, высокодисперсные от 1,0 до 10 мкм, а также мелкие — от 10 до 40 мкм, средние — от 40 до 250 мкм и крупные — от 250 до 1000 мкм.

При этом одна из основных характеристик порошка — это средний диаметр частиц. Однородность исходного материала повышает качество получаемых изделий, а потому больше всего ценится тот порошок, у которого выше содержание частиц одного размера. Не менее важным для любой порошковой композиции является сохранение сферической формы частиц. Это позволяет укладывать их более компактно в определенный объем и обеспечивает *текучесть* порошковой композиции в системах подачи материала с минимальным сопротивлением.

Оборудование, предназначенное для производства порошковых композиций, по существу не подпадает под действие экспортноконтрольных списков. К основным технологиям изготовления порошков для аддитивного производства относят газовую атомизацию (плавление металла в плавильной камере с дальнейшей его обработкой струей инертного газа под давлением), вакуумную атомизацию (растворенный в расплаве газ *выдавливает* металл к соплу, выходящему в распылительную камеру, где создают вакуум) и центробежную атомизацию (распыление расплава, создаваемого электрической дугой между прутком материала и вольфрамовым электродом). Наиболее широко распространена в мире технология газовой атомизации[19].

Стоит также сказать несколько слов об оборудовании и компонентах, используемых в аддитивном производстве, которые по существу не подпадают под действие экспортноконтрольных списков. Согласно представленным в части 2 общим замечаниям Руководящих принципов, «цель контроля не должна быть обойдена путем передачи любого неконтролируемого предмета (включая установки), содержащего один или несколько контролируемых компонентов, если контролируемый компонент или компоненты являются основным элементом этого предмета и могут быть сняты с него (или использованы) в других целях». В аддитивном производстве активно используются лазеры, однако их едва ли можно назвать основным элементом АТ. Еще большую смуту вносит следующее далее по тексту Руководящих принципов примечание о том, что при оценке того, следует ли считать контролируемый компонент основным элементом, правительства должны оценивать соответствующие количественные, качественные и связанные с технологическим *ноу-хау* факторы, а также другие особые обстоятельства, которые могли бы определять контролируемый компонент или компоненты в качестве основного элемента приобретаемого предмета.

В рамках ГЯП достаточно регулярно поднимается вопрос о том, что государства и их контролирующие органы трактуют экспортноконтрольное законодательство и контрольные списки по-разному, зачастую в собственных интересах. В связи с чем крайне необходимо вырабатывать в рамках режимов четкие и не допускающие неоднозначных трактовок правила игры.

И в этом контексте опасения вызывает альянс GARPA, изначально позиционированный как объединение производителей одного вида оборудования, но имеющий предпосылки к перерастанию в новый ограничительный блок стран, в который Российская Федерация рискует не попасть, как не попала в свое время в Австралийскую группу. У создания альянса уже есть политические последствия, которые заключа-

ются в том, что стоимость закупки порошковых композиций для российских участников рынка значительно выше, чем для заказчиков из стран-членов объединения[20].

ЭКОНОМИЧЕСКАЯ СОСТАВЛЯЮЩАЯ

Уже доказано, что металлические изделия, напечатанные на 3D-принтерах, по своим свойствам — плотности, остаточному напряжению, механическому поведению, неравновесной микроструктуре, кристаллографической текстуре — в лучшую сторону отличаются от изделий, изготовленных литьем, методами деформации или механической обработки. При этом, как уже говорилось, традиционные технологии производства являются *вычитающими*, а аддитивные технологии — *добавляющие*, что позволяет изготавливать прототипы будущих изделий быстрее и существенно дешевле.

Может показаться, что экономия на производстве прототипов должна способствовать распространению АТ. Однако это не так: порогом, защищающим от недобросовестных контрагентов, служит дороговизна закупки оборудования, сложность производства и приобретения порошков и программного обеспечения, обусловленные в том числе *закрытостью* GARPA. Несмотря на ощутимую экономию денег и времени, которую обеспечивает 3D-печать, чтобы стать собственником промышленного 3D-принтера и запустить его в работу, а тем более создать полную производственную линию, требуются существенные первоначальные вложения.

Таким образом, отличительная особенность аддитивных технологий заключается в поиске баланса (в т. ч. ценового) между входом на рынок 3D-печати, стоимостью порошков, разработкой дорогостоящих 3D-моделей (алгоритмов по их построению) и непосредственным приобретением 3D-принтеров[21].

НЕОСЯЗАЕМЫЕ ПЕРЕДАЧИ И СОВМЕСТНЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ

В рамках рассматриваемых международных режимов экспортного контроля аддитивные технологии также представляют интерес с точки зрения осуществления контроля за неосязаемой передачей технологий (передача информации по технологическим аспектам неосязаемым способом, куда входят научные конференции, встречи, выступления, лекции, обучение, в том числе обучение иностранных студентов, а также общение по электронным сетям — телефону, факсу, электронной почте, интернету) и программного обеспечения, поскольку к отличительным особенностям АТ можно отнести возможность моментальной передачи цифровых моделей в любую точку мира. Предметному рассмотрению в данном случае подлежат следующие вопросы:

- нормативные стандарты по минимизации рисков и возможностей обхода контроля в сфере неосязаемой передачи с использованием электронных каналов, облачных технологий и киберпространства;
- способы использования киберпространства для целей распространения;
- роль технической поддержки для неосязаемых передач информации и технологий в академической и научной среде;
- специфика контроля неосязаемых передач информации и технологий с точки зрения соблюдения защиты профессиональных интересов участников внешнеэкономической деятельности (ВЭД) и сохранения коммерческой тайны.

Применительно к перечисленным вопросам сейчас широко используются и выделяются такие виды противоправной деятельности, как хакерство, кибершпионаж, кибердезинформирование, киберпреступность, влекущие высокие риски для компаний при осуществлении экономической деятельности.

Такие риски могут возникать в связи с недостаточной политикой безопасности среди участников ВЭД в сфере неосязаемых передач, небольшой чувствительностью по отношению к всплывающим угрозам и отсутствием механизмов регулирования киберпространства. Основные трудности для представителей контролирующих органов с точки зрения минимизации рисков при неосязаемой передаче чувствительных технологий — это непрозрачность используемых бизнес-моделей, а также многоканальность информационных передач и необходимость защиты персональной информации. Все эксперты сегодня сходятся во мнении, что трендом контроля киберпространства является внедрение механизма лицензирования.

ВЫВОДЫ

В обзоре были исследованы причины появления новых угроз и *точек разрыва* в системе экспортного контроля как на региональном, так и на глобальном уровне в связи с активным внедрением в производственный процесс оборудования для аддитивного производства. Отмечены вызовы для международных режимов экспортного контроля, связанные с применением аддитивных технологий и увеличивающие риски распространения. Аддитивные технологии еще только начинают использоваться в промышленных масштабах, количество участников рынка весьма ограничено, соответственно, пролиферационные риски пока достаточно малы, а возможность воздействия аддитивного производства на распространение *чувствительной* продукции можно предвидеть и существенно уменьшить. Технология 3D-печати значительно искажает привычный подход к осуществлению контроля внешнеэкономических сделок со стратегически значимой продукцией, а также усложняет поиск путей нивелирования пролиферационных рисков. Авторами приводятся позиции, выработанные в ходе международных заседаний в рамках экспортноконтрольных режимов, а также формальных встреч с представителями промышленности.

Реакцией на обозначенные вызовы для системы экспортного контроля служит необходимость регулярного взаимодействия экспортно-ориентированных государственных и частных организаций с целью информационного обмена, в том числе путем транслирования лучших практик. Изучается международный и российский опыт в области преодоления рисков для системы экспортного контроля, вызванных аддитивными технологиями, приводятся примеры. Все это позволяет сделать выводы о том, что необходимо вырабатывать унифицированные процедуры в сфере контроля аддитивного производства высокотехнологичной продукции, а также неосязаемой передачи информации и аддитивных технологий.

Примечания

1 Discussion with Paul Fowler from the National Council for Advanced Manufacturing, STPI, 2010

2 Статья *Россия осваивает аддитивные технологии*, официальный сайт Минпромторга России, http://minpromtorg.gov.ru/press-centre/news/#! rossiya_osvaivaet_additivnye_tehnologii, дата обращения: 27 ноября 2015 г.

3 Статья BRIAN KRASSENSTEIN *20,000 3D Printed Parts Are Currently Used on Boeing Aircraft as Patent Filing Reveals Further Plans*, портал 3D.com, http:///3dprint.com/49489/boeing-3d-print/Сканирован-

ная заявка компании Boeing в патентное ведомство США http://www.tctmagazine.com/3D-printing-news/boeing-files-patent-for-3d-printing-aircraft-parts/, дата обращения: 15 ноября 2015 г.

4 Статья Larry Dignan, *Airbus A350 XWB used more than 1,000 3D printed parts*, ZDNet, May 6, 2015, http://www.zdnet.com/article/airbus-a350-xwb-used-more-than-1000-3d-printed-parts/, дата обращения: 25 ноября 2015 г.

5 Статья Andrew Zaleski, *GE's Bestselling Jet Engine Makes 3-D Printing a Core Component* Fortune, March 5, 2015

6 Статья *Аддитивные технологии: перспективы 3D печати в промышленности, раздел Применение в промышленности*, журнал *Атомный эксперт*, № 5–6 2014 г., http://www.up-pro.ru/library/innovations/niokr/additive-3d.html, дата обращения: 22 ноября 2015 г

7 Статья *Аддитивные технологии: перспективы 3D печати в промышленности*, раздел *География: от Вашингтона до Токио*, журнал *Атомный эксперт*, № 5–6 2014 г., http://www.up-pro.ru/library/innovations/niokr/additive-3d.html, дата обращения: 22 ноября 2015 г.

8 http://www.manufacturing.gov/nnmi_pilot_institute.html, дата обращения: 20 октября 2015 г.

9 https://www.nasa.gov/press/2014/august/sparks-fly-as-nasa-pushes-the-limits-of-3-d-printing-technology/#.VmHGVnbhDIU, дата обращения: 2 декабря 2015 г.

10 The Rapid Prototyping Industry Vendors Outside the US, http://www.additive3d.com/ind_22.htm; http://www.3ders.org/articles/20121019-global-additive-manufacturing-market-expected-to-reach-billion-by-2017.html, дата обращения: 1 декабря 2015 г.

11 Статья James Morgan *Amaze project aims to take 3D printing 'into metal age'*, новостной портал BBC http://www.bbc.com/news/science-environment-24528306, дата обращения: 17 октября 2015 г.

12 Статья *Железные перспективы*, журнал *Атомный эксперт*, http://atomicexpert.com/content/zheleznye-perspektivy, дата обращения: 25 ноября 2015 г.

13 Официальный сайт GARPA http://www.garpa.org/, информация об объединении https://www.wohlersassociates.com/GARPA.html, дата обращения: 12 ноября 2015 г.

14 Статья *Порошки избавляют от лишнего*, журнал *Эксперт*, http://expert.ru/expert/2014/49/poroshki-izbavlyayut-ot-lishnego/, дата обращения: 22 сентября 2015 г.

15 Статья *Россия осваивает аддитивные технологии*, официальный сайт Минпромторга России, http://minpromtorg.gov.ru/press-centre/news/#! rossiya_osvaivaet_additivnye_tehnologii, дата обращения: 27 ноября 2015 г.

16 Selective Laser Sintering Production Guide (*pdf), Xometry

17 Additive Manufacturing by Direct Metal Deposition, ADVANCED MATERIALS & PROCESSES • MAY 2011, pp.33–36

18 Числовое программное управление (ЧПУ) станка — это управление обработкой заготовки на станке по специальной программе, в которой данные об обработке заданы в цифровом коде. Система ЧПУ — это совокупность функционально взаимосвязанных технических и программных методов и средств, обеспечивающих числовое программное управление станком (информация с сайта http://www.zavod-rekom.ru/products/268/).

19 Статья *Порошки избавляют от лишнего*, журнал *Эксперт*, http://expert.ru/expert/2014/49/poroshki-izbavlyayut-ot-lishnego/, дата обращения: 22 сентября 2015 г.

20 Статья *Порошки избавляют от лишнего*, журнал *Эксперт*, http://expert.ru/expert/2014/49/poroshki-izbavlyayut-ot-lishnego/, дата обращения: 22 сентября 2015 г.

21 Thomas Campbell, Christopher Williams, Olga Ivanova, and Banning Garrett, *Could 3D Printing Change the World? Technologies, Potential, and Implications of Additive Manufacturing*, Strategic Foresight Report, The Atlantic Council, October 2011, p.5, http://www.atlanticcouncil.org/publications/reports/could-3d-printing-change-the-world.

ПРИМЕНЕНИЕ МЕЖДУНАРОДНОГО ПРАВА В КИБЕРПРОСТРАНСТВЕ

Ущерб, нанесенный частным лицам, организациям или объектам инфраструктуры в результате инцидентов в киберпространстве, в частности целенаправленных атак, может быть не менее существенным, чем последствия традиционных вооруженных конфликтов и столкновений. При этом в отличие от случаев применения традиционного кинетического оружия идентификация источника нападения при кибератаке крайне проблематична, а отсутствие международно-признанного определения акта агрессии в киберпространстве и общего понимания границы, за которой применение силы в нем может приравниваться к вооруженной атаке, оставляют обширное пространство для интерпретации намерений и действий сторон конфликта.

Старший советник по правовым вопросам Региональной делегации Международного Комитета Красного Креста (МККК) в Российской Федерации, Беларуси и Молдове Мария Станиславовна ***Гаврилова*** *(Россия), консультант ПИР-Центра Олег Викторович* ***Демидов*** *(Россия), генеральный секретарь Ассоциации международного права (Беларусь) Андрей Леонидович* ***Козик*** *и заместитель директора Института проблем информационной безопасности МГУ имени М. В. Ломоносова Анатолий Александрович* ***Стрельцов*** *(Россия) обсудили эти и другие вопросы на заседании круглого стола, состоявшегося в рамках 15-й Международной школы ПИР-Центра по проблемам глобальной безопасности.*

МАРИЯ ГАВРИЛОВА: Я буду говорить о регулировании киберпространства с точки зрения международного гуманитарного права (МГП) и возможности его применения в условиях вооруженных конфликтов, которые могут произойти с использованием информационных технологий, и постараюсь ответить на три вопроса:

- Почему Международный комитет Красного Креста (МККК) интересуется этой тематикой? Как взаимосвязаны Интернет и МККК?
- Как и в каком объеме МГП применяется в ситуации киберконфликта?
- С какими сложностями могут столкнуться органы государственной власти и эксперты при непосредственном применении МГП к киберпространству?

Позволю себе небольшую ремарку. МГП имеет две основные цели: ограничение средств и методов ведения войны во избежание лишних страданий мирного населения и защита гражданского населения и гражданских объектов, направленная на минимизацию материального и физического ущерба для лиц, не принимающих непосредственное участие в вооруженном конфликте.

МККК является хранителем МГП и, безусловно, заинтересован в его развитии. Даже если на данный момент мы не наблюдаем конфликтов в киберпространстве, можно предположить, что с развитием информационных технологий они будут играть все большую роль в вооруженных конфликтах. Таким образом, цель МККК — помогать развитию МГП, стремясь предотвратить, предусмотреть, урегулировать и, по возможности, предотвратить ситуации, которые потенциально могут нанести большой ущерб гражданскому населению.

Обращаясь к вопросу применимости МГП в киберпространстве, следует отметить, что большая часть его норм создавалась достаточно давно. В то время, когда мы и предположить не могли, что войны в киберпространстве возможны. Тогда это казалось научной фантастикой. Во многом именно с этим связаны споры о применимости МГП в киберпространстве. В самом деле, могли ли авторы международных договоров в 1949 и даже в 1977 г., которыми датируются основополагающие положения, потенциально подлежащие применению в ситуации киберконфликта, описать правила поведения, распространяющие свое действие на еще не существовавшее пространство?

Дополнительные сложности вызывает терминологическая путаница. Во-первых, как в средствах массовой информации, так и в научной литературе очень широко используется понятие *информационные войны*, которое смущает публику, потому что применяется оно не только к конфликтам, но и к пропаганде, работе СМИ и т. д. Безусловно, к информационным войнам, которые заключаются, например, в намеренной дезинформации населения в определенных политических целях, МГП не имеет никакого отношения. Оно применимо только к *классическим* вооруженным конфликтам, связанным с применением определенного рода силы. Хотя и тут есть свои особенности.

Киберконфликты, вне всяких сомнений, уникальны: во-первых, они не связаны с применением обычного, кинетического оружия, в связи с чем достаточно трудно определить место ведения боевых действий. Кибератаки могут происходить в разных точках планеты, находиться под юрисдикцией разных государств, и определить так называемый театр ведения военных действий, ограничить эту территорию порой бывает достаточно сложно.

Второй особенностью этих конфликтов является сложность, связанная с определением состава участников вооруженного конфликта. Для МГП крайне важно определить, кто именно принимает участие в военных действиях и от чьего имени. От этого зависят не только квалификация конфликта, но и более практические моменты, такие как объем защиты, предоставляемый каждому конкретного лицу, и определение законных целей для нападения. Также для МГП ключевое значение имеет определение лиц, ответственных за совершение военных преступлений, и привлечение последних к ответственности.

Но одно дело, когда вполне конкретные, официальные вооруженные силы вступают на территорию чужого государства, применяют на ней оружие, и совсем другое дело, когда мы говорим о хакерских конторах, ИТ-компаниях, разрушительное действие которых может быть не столь очевидно, а сами они могут быть рассредоточены по разным странам. Каким образом в такой ситуации осуществлять контроль, а в случае нарушений МГП выявлять виновных и привлекать к ответственности как государство, так и конкретных индивидов, непонятно. Все это накладывает особенности на применение МГП.

Тесно связан с этим вопрос безграничных возможностей негосударственных акторов. Все-таки в классических вооруженных конфликтах, к которым привычно применяется МГП, мы чаще всего говорим об армиях или о конкретных организованных вооруженных группах. В киберпространстве возможности негосударственных акторов, у которых просто есть доступ к компьютеру и соответствующее образование, значительно шире. Следовательно, мы можем столкнуться с ситуацией вооруженного конфликта, в котором будет принимать участие огромное число лиц, и контроль за всеми их действиями, привлечение их к ответственности станет непростой, если вообще посильной задачей.

Тем не менее, несмотря на то что киберконфликты представляют собой особые ситуации, в соответствии с уже сложившимся международным правом, что, в частности, было подтверждено консультативным решением Международного суда ООН, принципы МГП регулируют все виды, методы и средства ведения войны, которые когда-либо появлялись, существуют на данный момент или появятся в будущем. Также Группа правительственных экспертов ООН в своем последнем докладе отметила, что принцип гуманности — основа МГП — безусловно, применим к киберпространству. Осталось понять, с какими трудностями нам придется столкнуться, чтобы адаптировать МГП к новым реалиям.

Теперь о том, почему в этой тематике заинтересован МККК. Во-первых, в силу того что мы являемся хранителями МГП, мы заинтересованы в его развитии. Во-вторых, на данный момент огромное количество гражданской инфраструктуры, которая играет важную роль в жизни гражданского населения, опирается на компьютерные технологии. Если мы говорим о кибератаках, о киберконфликтах, то одни и те же сети могут использоваться как в военных так и в гражданских целях, в частности обеспечивать функционирование ядерных электростанций, госпиталей, и разрушение таких информационных систем может повлечь огромный ущерб для гражданского населения.

Одним из основных положений в МГП является четкое разделение гражданских и военных объектов. Когда мы имеем дело с киберпространством, когда один и тот же объект используется и в гражданских, и в военных целях, соблюсти это различие становится достаточно трудно. Например, та же GPS-навигация и банальный кабель может использоваться и в гражданских, и в военных целях.

МККК заинтересован в разработке новых или адаптации существующих норм для обеспечения более эффективной защиты гражданской инфраструктуры. В особенности, когда речь идет о защите объектов, необходимых для выживания гражданского населения, которые также могут пострадать в ходе конфликтов в киберпространстве, так как потенциально могут быть разрушены, например водоочистные сооружения.

Первые трудности, с которыми мы сталкиваемся при применении МГП, связаны с квалификацией вооруженного конфликта. Для того чтобы защита, предусмотренная МГП, распространилась на гражданское население конкретной территории, необходимо, во-первых, установить наличие вооруженного конфликта. Ситуация проще, когда в ходе вооруженного конфликта имеет место одновременное применение кинетического оружия и кибероружия. Намного сложнее установить наличие или отсутствие конфликта, когда мы имеем дело исключительно с кибератаками.

Существуют разные мнения и подходы относительно того, достаточно ли для начала применения МГП одних только кибератак. Ряд экспертов полагает, что не важно, какие методы ведения войны применяются — цифровые или кинетические. Сам факт начала применения этих методов и, как следствие, достижение определенного порога насилия, по мнению этих авторов, могут служить достаточным основанием для признания наличия вооруженного конфликта, к примеру, если при помощи кибероружия выводится из строя система навигации, в результате чего нарушается работа аэропортов, сталкиваются самолеты.

Есть и другое мнение на этот счет, которое состоит в том, что для кибероружия должен быть установлен более высокий порог интенсивности: такие операции должны проводиться постоянно, а ущерб от его применения должен быть значительным. Представляется, что это мнение не вполне основано на МГП, поскольку если мы говорим о международном вооруженном конфликте, то для его констатации достаточно и единичного случая применения силы, чтобы гражданское население получило предусмотренную договором защиту, а действия государств подлежали скрупулезной оценке на предмет соответствия критериям пропорциональности, соразмерности и иным ограничениям, о которых мы еще поговорим.

Как и в любой другой ситуации, связанной с применением силы, для киберконфликта принципиальное значение имеет квалификация его как международного или немеждународного. Если международный вооруженный конфликт, как было отмечено ранее, может состоять из единичного случая применения силы, то есть одной кибератаки, повлекшей за собой серьезные последствия, то для того, чтобы МГП начало защищать гражданское население от последствий кибератак, проводимых в ходе вооруженного конфликта немеждународного характера, необходимо преодоление определенного порога интенсивности, а в отдельных случаях — наличие организованной вооруженной группы. Если с интенсивностью все более-менее понятно, то установить участие в конфликте организованной вооруженной группы бывает не так просто.

Кроме того, от квалификации конфликта будет зависеть объем и содержание применимых норм. Часть положений МГП регулирует исключительно поведение участников классических международных конфликтов с участием государств. В случае же вооруженного конфликта немеждународного характера, где, по крайней мере, в роли одной из сторон выступает организованная вооруженная группа, круг применимых норм значительно уже, да и содержание отдельных требований может существенно отличаться. Именно поэтому анонимность в Интернете — это серьезная проблема для МГП.

Чтобы определить, какой блок норм применять, сначала нужно определить, кто воюет. В реальных боевых действиях это значительно проще — можно съездить и посмотреть на месте. Когда мы имеем дело с боевыми действиями с примене-

нием компьютерных технологий, далеко не всегда можно определить, откуда произошла атака, кто ее осуществлял, и уж тем более контролировалась ли она государством, с территории которого производилась, и в какой мере.

В данном случае нас спасает тот факт, что постепенно нормы обычного права восполняют пробелы в регулировании вооруженных конфликтов немеждународного характера и практически приравнивают две эти системы, в какой-то степени упрощая задачу защиты гражданского населения.

Какие положения регулируют вооруженные конфликты и защиту жертв в ситуации вооруженного конфликта? Во-первых, статья 36 Дополнительного протокола к Женевским Конвенциям. Эта норма является своеобразным ответом на критику в отношении МГП, которое якобы не адаптировано для кибероружия. В статье 36 говорится, что если государство разрабатывает новое оружие, не обязательно принимать новый договор или конвенцию, чтобы это оружие регулировалось МГП. МГП уже содержит ряд принципов, например пропорциональность, проведение различия, гуманность и т. д., которые регулируют применение любого вида оружия, независимо от того, когда оно появилось. И первое, с точки зрения МГП, что должно сделать государство, когда оно разрабатывает новое оружие, — это проверить его на соответствие МГП.

Также есть более общее положение, которое призывает государства обеспечить защиту гражданского населения и гражданских объектов. Это общая обязанность для атакующего и для защищающегося.

Сложности начинаются дальше, поскольку МГП содержит и более развернутые положения: запрет на нападение на объекты, необходимые для выживания гражданского населения; запрет на нападение на установки, содержащие опасные силы; принцип пропорциональности; меры предосторожности при нападении. Но для того чтобы эти нормы были применимы, необходимо установить факт нападения.

В рамках Дополнительного протокола к Женевским Конвенциям нападение определялось исходя из того, как это видели его создатели на момент принятия документа — а это 1977 г. Так, под нападением понимались «акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне». Однако практика пошла таким образом, что под актами насилия понимались в том числе военные операции, которые сами по себе используют ненасильственные методы без применения огня, но ведут к разрушениям и гибели гражданского населения. Таким образом, еще до возникновения вопроса о применимости МГП к кибератакам практика признала, что исходно ненасильственные методы в совокупности могут составлять нападения по смыслу договора.

В рамках *Таллинского руководства по международному праву, применимому при ведении кибервойны*, кибератака понимается как кибероперация, как наступательная, так и оборонительная, которая причиняет ранения или смерть людям либо ущерб объектам. С точки зрения МККК, не только ущерба и разрушения, но и нейтрализации объектов может быть достаточно, чтобы расценивать факт как нападение. Если обесточен, лишен возможности функционировать какой-то объект на АЭС, тот факт, что станция не разрушена, не говорит о том, что это не было нападением. Нейтрализован гражданский объект, что является достаточным основанием для применения МГП.

Один из важнейших для нас принципов — принцип пропорциональности, который означает, что ущерб гражданскому населению и гражданским объектам не может превышать то военное преимущество, которое сторона рассчитывает получить при помощи кибератаки. Самые большие трудности в данном случае возникают из-за тесной взаимосвязи гражданских и военных объектов, гражданской и военной инфраструктуры в киберпространстве. Военные объекты с точки зрения МГП — это те объекты, которые своим расположением, целью, использованием вносят эффективный вклад в военный успех государства.

Очень тяжело провести это разграничение в киберпространстве, когда, к примеру, GPS-навигация, компьютерные сети, Интернет работают как на гражданское население, так и на успех военной операции. Очень велик риск того, что гражданские объекты будут расценены как объекты двойного назначения и разрушены — в киберпространстве практически все будет являться объектом двойного назначения. Как в данном случае расценить эту пропорциональность, каким образом обезопасить гражданское население и посчитать, будет ли ущерб для гражданского населения перевешивать военное преимущество или нет?

Кроме того, от государства потребуется огромная техническая экспертиза, чтобы предвидеть и рассчитать, будет ли вообще нанесен какой бы то ни было ущерб. С точки зрения МГП это входит в обязанности государства — участника конфликта: просчитать ущерб, предусмотреть возможности для обратного пути, если станет ясно, что в ходе атаке пострадают гражданские объекты. Но намного проще дать указание остановить танк, который едет в город, чем остановить работу вирусов, которые уже были запущены в компьютерную систему, а результатом стало выведение объектов из строя.

Таким образом, несмотря на то что мы можем утвердительно говорить, что МГП регулирует киберконфликты, оно, очевидно, требует немалой доработки. Особую актуальность в контексте применения МГП в киберпространстве имеют следующие вопросы: противоречие между анонимностью в Интернете и необходимостью привлечения к индивидуальной уголовной ответственности за военные преступления, обязательство государства по обеспечению соблюдения МГП со стороны государств в условиях киберпространства, непосредственное участие в киберконфликтах и его возможные последствия для ИТ-компаний и иных возможных негосударственных участников боевых действий с применением компьютерных технологий.

ОЛЕГ ДЕМИДОВ: 22 июля 2015 г. был опубликован новый доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ ООН). Значение доклада, который стал плодом годовой работы уже четвертого по счету созыва Группы, история работы которой отсчитывается с 2001 г., состоит прежде всего в выработке свода политических норм, предлагаемых государствам — членам ООН в качестве первого шага к режиму ответственного поведения в киберпространстве.

Значение одиннадцати *добровольных и необязательных норм, правил или принципов ответственного поведения государств* уже стало предметом анализа в работах международных и российских экспертов, включая представителей ПИР-Центра. Выработка подобных правил, даже в качестве общих и сугубо добровольных предложений международному сообществу, стала значительным прогрессом как для

самой Группы, так и вообще для диалога об ответственном поведении государств в киберпространстве. Любопытно, что еще до публикации доклада деятельность ГПЭ стала ключевым предметом обсуждения на площадке 4-й Глобальной конференции по киберпространству, прошедшей в апреле 2015 г. в Гааге, Нидерланды.

Разворот западных дипломатов и экспертного сообщества, включая экспертов частного сектора, государственных и неправительственных научных центров, навстречу ГПЭ, проявившийся в Гааге, отразил две тенденции. Во-первых, сам дискурс о необходимости выработки норм поведения в киберпространстве для государств к 2015 г. окончательно утвердился, победил альтернативную точку зрения, согласно которой киберпространство по большому счету не нуждается в обязывающих нормах. Во-вторых, стало очевидно, что несмотря на хронические противоречия по ключевым вопросам между членами ГПЭ (прежде всего РФ и США) и ее неоднозначный для Запада имидж российской инициативы, служащей прежде всего интересам Москвы, работа Группы все же плодотворна и по большому счету безальтернативна. Последний факт легко объясним: ООН — единственная глобальная площадка, на которой имеет смысл договариваться об общих правилах для трансграничного киберпространства.

Однако росту внимания к работе ГПЭ во всем мире также послужило то, что с третьего созыва Группы в ее повестку была включена еще одна фундаментальная задача — адаптация к киберпространству существующих норм международного права, включая такие основополагающие его акты, как Устав ООН. В докладе ГПЭ 2013 г. было впервые заявлено, что Устав ООН применим и *имеет важное значение для поддержания мира и стабильности в киберпространстве*. Кроме того, в докладе отмечалось, что на поведение государств в киберпространстве и их юрисдикцию над ИКТ-инфраструктурой распространяются международные нормы и принципы, вытекающие из принципа государственного суверенитета.

Эти выводы Группы получили подтверждение и дальнейшее развитие в Докладе 2015 г. Кроме того, участникам ГПЭ удалось согласовать ряд мнений касательно вопроса о применимости международного права к киберпространству. Вкратце эти мнения включают:

- признание суверенитета государств над ИКТ-инфраструктурой в пределах их территории;
- необходимость соблюдения ряда международно-правовых принципов в киберпространстве (государственный суверенитет, суверенное равенство, мирное разрешение споров, невмешательство во внутренние дела);
- признание за государствами возможности принятия неуточненных мер в соответствии с Уставом ООН в контексте киберпространства;
- упоминание в контексте киберпространства ряда принципов (гуманности, необходимости, пропорциональности и индивидуализации);
- призыв отказаться от использования посредников (proxy actors) для противоправных действий в киберпространстве и от предоставления им своей территории;

- ответственность государств за противоправные действия в киберпространстве в случае, когда обвинения обоснованы и проведена надлежащая атрибуция таких действий.

Несмотря на свою безусловную важность, некоторые меры из этого списка все же можно назвать второстепенными, производными от первоочередных задач. Например, атрибуция кибератак с вовлечением государств имеет практический смысл только в том случае, когда определены и понятны возможные ответные меры в отношении автора противоправных действий в киберпространстве. Аналогично, целесообразность и сама возможность запрета на использование посредников для противоправных действий в киберпространстве определяется прежде всего тем, как международное сообщество будет квалифицировать действия с их участием, какие международно-правовые последствия эти действия будут создавать для причастных к ним государств (и самих посредников), и, опять же, какой диапазон ответных мер будет открыт для пострадавшей стороны в соответствии с общепринятой интерпретацией международного права.

Перенося эти тезисы на конкретный пример, вернемся к хорошо известной ситуации со *Stuxnet*. На сегодня мнение экспертного сообщества, подкрепленное техническим анализом кода червя, данными журналистского расследования Дэвида Сангера и заявлениями Эдварда Сноудена, почти не оставляет места для сомнений в том, что за созданием *Stuxnet* и его применением против объекта в Натанзе стоят американские и израильские спецслужбы. Представим, что уже в 2010 г. Ирану за счет привлечения внешних специалистов по информационной безопасности и организации трансграничного расследования инцидента удалось бы добыть технические свидетельства причастности АНБ и Моссада к операции по кибersаботажу иранских атомных объектов. Безусловно, в случае со *Stuxnet* речь идет о задаче исключительной сложности, однако сегодня атрибуция даже сложных целевых атак все же возможна при условии своевременных действий, сочетающих различные методы и техники. Но что Иран смог бы сделать с полученной информацией? И как международное сообщество в лице, например, Совета Безопасности ООН либо Генассамблеи ООН могло бы квалифицировать действия США и Израиля, даже получив от Ирана убедительные доказательства их причастности?

Этот же вопрос поднимали в своей статье, опубликованной в конце 2014 г., А. В. Крутских, известный в некоторых кругах как *киберцарь*, и один из ведущих отечественных экспертов по международной информационной безопасности (МИБ) А. А. Стрельцов. Кроме того, кейс *Stuxnet* рассматривается в *Таллинском руководстве* по применению международного права в условиях конфликта в киберпространстве CCD COE. Характерно, что ведущие эксперты и дипломаты России и стран НАТО не смогли дать ответа на этот вопрос — это невозможно до тех пор, пока не прояснена интерпретация ключевых понятий международного права применительно к киберпространству. Базовой *точкой отсчета* с точки зрения понятийного аппарата современного международного права, в свою очередь, является Устав ООН — наряду с конвенциями и другими актами, составляющими корпус международного гуманитарного права (jus in bello) и права вооруженного конфликта (jus ad bellum).

О каких конкретно понятиях идет речь? Их практически идентичный перечень приводят и российские авторы упомянутой статьи в журнале *Международная Жизнь*

и авторы Таллинского руководства. Выделим из этого перечня три наиболее важных понятия:

- угроза силой или применение силы (в соответствии со Статьей 2 (4) Устава ООН);
- акт агрессии (в соответствии со Статьей 39 Устава ООН);
- вооруженное нападение (в соответствии со Статьей 51 Устава ООН).

Важным *подспорьем* в вопросе о том, насколько вообще уместно применение этих понятий к действиям в киберпространстве, является Консультативное заключение Международного Суда ООН о законности применения или угрозы применения ядерного оружия в вооруженных конфликтах, 1996. В пункте 39 данного документа утверждается, что действие норм, прописанных в Статье 2 (4), Статье 42, Статье 51 и в целом в Главе VII Устава ООН, включая право государств на самооборону, не ограничено действиями с использованием какого-либо конкретного вида оружия. Таким образом, можно предположить, что с точки зрения Международного Суда ООН действие этих статей распространяется и на те ситуации в киберпространстве, когда ИКТ используются в качестве оружия. Однако здесь возникает новый терминологический вопрос: в каких случаях можно говорить об использовании оружия в киберпространстве. А. А. Стрельцов и А. В. Крутских указывают на разработанную терминологию *информационного оружия* и *информационной войны*, принятую как в доктринальных документах РФ, так и в международных договорах, таких как Екатеринбургское соглашение глав государств ШОС от 16 июня 2009 г. Однако за пределами ШОС, в том числе на площадке ГПЭ ООН, эти определения пока не используются.

В совокупности три приведенных выше понятия служат отправной точкой для того, чтобы так или иначе квалифицировать те или иные действия государств и посредников в киберпространстве, имеющие серьезные последствия (или создающие возможность для наступления таковых) для международной безопасности и/или международного мира. Возможность квалификации того или иного действия в киберпространстве также дает ответ на принципиальный вопрос о том, порождает ли такое действие у затронутого им государства право на самооборону в соответствии со Статьей 51 Устава ООН. В примере со *Stuxnet* основной вопрос звучит так: в случае наличия доказательств причастности США и Израиля к разработке и применению *Stuxnet* против иранских объектов следует ли считать эти действия применением силы, актом агрессии либо вооруженным нападением по смыслу соответствующих статей Устава ООН, и может ли Иран воспользоваться своим правом на самооборону? Ответ неизвестен именно в силу отсутствия общепринятой интерпретации Устава ООН для киберпространства.

В Таллинском руководстве предпринимается попытка выработать такую квалификацию, но в вопросе о *Stuxnet* группа экспертов не пришла к консенсусу. Согласно преобладающему мнению, кейс *Stuxnet* все же не может быть приравнен к применению силы, так как он не соответствует некоторым критериям, принятым экспертами CCD COE для квалификации действий в киберпространстве как применение силы. Перечень из 8 критериев приведен в правиле 11 Таллинского руководства, которое как раз посвящено определению понятия *применение силы* в киберпространстве. Ключевым критерием выступает серьезность последствий действия, которые могут проявляться в физических разрушениях инфраструктуры и иных

объектов, либо в человеческих жертвах, которые непосредственно повлекло действие в киберпространстве. Также используется ряд *качественных* критериев:

- мгновенный, незамедлительный характер действия;
- прямая, непосредственная связь между действием и последствиями;
- степень вторжения в чужое информационное пространство/ИКТ-инфраструктуру;
- измеримость последствий действия;
- военный характер действий;
- степень прямого вовлечения государства в кибероперацию/иное действие;
- наличие либо отсутствие прямого запрета на подобные действия в актах международного права.

В соответствии с этими критериями, даже если бы удалось доказать вовлечение США в создание и использование Stuxnet против Ирана, признать эту операцию использованием силы экспертам CCD COE помешал прежде всего тот факт, что ход и последствия были сильно растянуты во времени (как минимум 2008–2010 гг.). Кроме того, неизвестно, является ли с точки зрения экспертов Таллинского центра вывод из строя каскада центрифуг для обогащения урана в Натанзе достаточно серьезным разрушением для квалификации его как применения силы.

Следует заметить, что авторы Таллинского руководства взялись решать двойную по сложности задачу, так как понятие *применения силы* по смысле Статьи 2 (4) и вне контекста киберпространства не имеет точного определения. Что не менее важно, за прошедшие с момента принятия Устава ООН десятилетия не до конца прояснен вопрос о соотношении между собой понятий *применения силы*, *агрессии* и *вооруженного нападения*. Одной из ключевых ссылок в этом вопросе, которая также приводится в Таллинском руководстве, является решение Международного суда ООН от 27 июня 1986 г. по делу *О военной и военизированной деятельности в Никарагуа и против Никарагуа*, ответчиком по которому выступали США. Во-первых, в решении отмечается, что вооружение и подготовка США антиправительственных повстанческих группировок (контрас) представляет собой акт применения силы или ее угрозы в отношении Никарагуа.

Несмотря на то что это решение никак не связано с кибероперациями, оно достаточно важно в контексте сегодняшних задач, стоящих перед ГПЭ ООН и перед международным сообществом в целом. Во-первых, это означает, что применение силы не ограничивается прямым использованием вооруженных сил государства и может включать иные действия (вооружение, тренировка и пр.). Этот вывод актуален для киберпространства, так как кибероперации чаще всего весьма затруднительно рассматривать в качестве прямого использования национальных ВС. Кроме того, решение Международного Суда открывает возможность для квалификации как применения силы действий посредников (в данном случае отряды контрас), что также актуально для киберпространства.

Также решение МС ООН 1986 г. указывает на необходимость отграничения понятия *применения силы* от понятия *вооруженного нападения*: последнее включает *не все*, а лишь *наиболее серьезные* случаи применения силы. Этот принцип, очевидно, распространяется и на квалификацию кибероперациий с точки зрения

международного права. Вместе с тем ни текст решения, ни последующие документы Международного Суда ООН не сообщают четких критериев, которые позволили бы однозначно разграничить *применение силы* с *вооруженным нападением*. Соответственно, эта проблема будет автоматически переноситься и на квалификацию различных кибероперaций.

Наконец, не проясненным в рамках решения 1986 г. остается соотношение как применения силы, так и вооруженного нападения с понятием агрессии по смыслу Статьи 39 Устава ООН. При этом вне контекста соотношения с другими терминами из Устава ООН как раз понятию агрессии присуща наибольшая ясность. Определению агрессии посвящена отдельная одноименная резолюция Генассамблеи ООН № 3314 от 4 декабря 1974 года. В Статье 3 резолюции приводится перечень из семи видов действий, подпадающих под понятие агрессии. В резолюции отмечается, что список не является исчерпывающим и может быть пополнен решением Совбеза ООН. В настоящее время эта опция приобретает растущую актуальность, так как документ, принятый 41 год назад, по понятным причинам не говорит ничего о действиях с использованием ИКТ и агрессии в контексте киберпространства. Подробный анализ Резолюции производит в своей недавней работе коллектив авторов Минобороны РФ. При этом военные эксперты МО РФ продвигают идею не обновления текста резолюции, а его адаптированного прочтения, которое охватывало бы операции в киберпространстве, потенциально подпадающие под понятие агрессии. В частности предлагается рассматривать использование одним государством прокси-серверов на территории второго для атак на третье как действие, подпадающие под пункт *f)* Статьи 3 Резолюции (предоставление государством своей территории для совершения актов агрессии в отношении третьего государства). Также рассматривается интерпретация применительно к действиям хакерских групп-посредников пункта *g)* (засылка государством или от имени государства вооруженных банд, групп, иррегулярных сил или наемников, осуществляющих применение вооруженной силы).

Однако авторы работы признают, что ключевым недостатком Резолюции ГА ООН является отсутствие у нее обязывающей силы. Следовательно, заложенное в ней определение агрессии, даже при наличии его консенсусной интерпретации применительно к кибероперациям, вряд ли сможет служить прочной основой международно-правового режима в этой сфере. В этой связи любопытная опция предлагалась тем же авторским коллективом МО РФ ранее: инкорпорировать определение агрессии, адаптированное к киберпространству, в Римский Статут Международного уголовного суда (МУС). В 2011 г. на конференции по обзору Римского Статута МУС была принята резолюция о включении в Статут понятия *преступление агрессии*, взятого из Резолюции № 3314 ГА ООН. Но фактическое осуществление юрисдикции МУС по этому преступлению станет возможно только в случае принятия соответствующего решения на следующей обзорной конференции по Римскому Статуту МУС, проведение которой запланировано на январь 2017 г. На данный момент существует вероятность того, что принятие решения может быть отложено и на более дальнюю перспективу. С одной стороны, это дает возможность начать и развить широкую международную дискуссию об адаптации текста Резолюции № 3314 (и параллельно понятия *преступление агрессии* в Римском Статуте МУС) к кибероперациям. В том числе вероятной площадкой для такой дискуссии видится как раз ГПЭ ООН, следующий, пятый созыв которой должен начать свою

работу в 2016 г. С другой стороны, даже в случае достижения компромисса по этому вопросу в рамках ГПЭ ООН временные перспективы вступления в силу обязательного определения агрессии, адаптированного к кибероперациям, — в рамках юрисдикции МУС или в ином формате — пока неясны.

В свете рассмотренных выше терминологических коллизий важен вопрос о том, возьмется ли следующий созыв ГПЭ ООН решать их. Участники группы, включая российских дипломатов, неоднократно делали акцент на том, что мандат Группы не включает глубокую ревизию норм международного права с целью их адаптации к киберпространству — задача ГПЭ состоит в выработке более общих и практических норм поведения в этой сфере. Однако логика подсказывает, что полностью скинуть с себя эту функцию Группе не удастся по нескольким причинам. Во-первых, дальнейшее расширение и даже простое поддержание консенсуса между членами Группы невозможны без общего понимания ключевых терминов, на которые опираются выработанные Группой нормы поведения. В том числе речь идет и о терминах из Устава ООН.

Во-вторых, ставки растут: чем дольше Группа избегает тяжелой и кропотливой работы по глубинной интерпретации основополагающих норм международного права применительно к киберпространству, тем больше шансов на то, что на практике военно-политический курс ведущих держав в сфере кибероперациий будет опираться на видение международного права, сформулированное в рамках других площадок либо выработанное самостоятельно и вообще ни с кем не согласованное.

Отчасти этот процесс уже происходит. Опыт и выводы, полученные в ходе работы над Таллинским руководством, несмотря на его сугубо экспертный статус, уже находят отражение в реальной политике НАТО. В сентябре 2014 г. в ходе саммита НАТО в Уэльсе прошел обзор Углубленной доктрины кибероборонь Организации. По его итогам было принято политическое решение о том, что право членов НАТО на коллективную оборону, заложенное в Статье 5 Вашингтонского договора, распространяется и на те случаи, когда государство — член НАТО становится жертвой нападения в киберпространстве. Отныне кибератака на страну — члена НАТО, повлекшая гибель людей или масштабное разрушение инфраструктуры, и, по мнению Организации, совершенная напрямую государством или его посредниками, может повлечь вооруженный ответ НАТО с использованием всего доступного ей военного потенциала, не ограничиваясь киберпространством. При этом вопрос об атрибуции кибератаки, способной запустить механизм коллективной обороны, будет решаться военным командованием НАТО по ситуации в каждом конкретном случае. Потенциальные риски такого подхода хорошо иллюстрируются примером 2007 г., когда Эстония, ставшая жертвой мощной волны кибератак в разгар так называемого *кризиса Бронзового солдата,* запросила руководство НАТО о возможности применения Статьи 5. При этом в качестве агрессора рассматривалась РФ, которую Эстония обвинила в организации и осуществлении кибератак, несмотря на отсутствие надежных доказательств. Повторись такая ситуация сегодня, с учетом новой доктрины кибероборонь НАТО речь могла бы идти о потенциальной эскалации кризиса между Россией и НАТО.

Стоит отдельно отметить развитие взглядов США на международно-правовую сторону кибероперациий. В июне 2015 г. было опубликовано свежее издание Руководства Министерства обороны США по праву войны (DoD Law of War Manual).

Публикация содержит отдельную главу, посвященную кибероперациям, где среди прочего четко прописаны критерии и условия, при которых кибероперация квалифицируется как незаконное применение силы по смыслу Статьи 2 (4) Устава ООН. В Руководстве приводятся три примера таких операций:

- кибероперация, которая вызывает мелтдаун реактора АЭС;
- кибероперация, которая вызывает открытие дамбы ГЭС в густонаселенной местности, ведущее к человеческим жертвам;
- кибероперация, которая нарушает работу авиадиспетчерских служб, что в свою очередь ведет к авиакатастрофе.

Дополнительно в документе упоминаются и иные примеры кибероперций, которые могут быть признаны актами применения силы, включая операции, нарушающие работу систем военной логистики и в результате препятствующие планированию военных операций и управлению войсками.

Несмотря на то что Руководство не является источником права и не имеет никакой юридической силы, его положения служат практической инструкцией для служащих Вооруженных сил США, включая, например, такие структуры, как Объединенное киберкомандование ВС США.

Для международного сообщества риск разноскоростной, нескоординированной деятельности различных государств и региональных альянсов по выработке интерпретации международного права применительно к киберпространству состоит в том, что в отсутствие общей площадки *окно возможностей* для выработки общего подхода или хотя бы эффективной гармонизации существующих подходов достаточно быстро закроется. В результате мы рискуем оказаться в ситуации, когда множество государственных игроков участвуют в трансграничных кибероперациях по всему миру, руководствуясь лишь собственными либо узкогрупповыми представлениями о границах допустимого в этой сфере. Нетрудно предположить, что такая международно-правовая анархия, помноженная на трансграничный характер почти любой операции в киберпространстве, сможет очень быстро спровоцировать международные кризисы и даже вооруженные конфликты. Особенно опасным и угрожающим в этом свете выглядит тот факт, что реакция государств на недружественные действия в киберпространстве при отсутствии прозрачного и общепринятого международно-правового механизма разрешения разногласий может совсем необязательно ограничиваться киберпространством. На практике это будет означать растущий риск эскалации кризисов в киберпространстве до конфликтов с использованием кинетических вооружений.

На сегодняшний день ГПЭ ООН выглядит единственной достаточно широкой, авторитетной и компромиссной площадкой для того, чтобы попытаться все же приступить к выработке общепринятой консенсусной интерпретации Устава ООН и других ключевых норм международного права применительно к киберпространству и таким образом предотвратить описанный выше сценарий. Остается надеяться, что расширение мандата Группы в рамках ее пятого созыва в 2016 г. будет предусматривать работу над этой задачей. *Если не мы, то кто же?*

АНАТОЛИЙ СТРЕЛЬЦОВ: На мой взгляд, проблема стоит несколько шире, чем просто применение международного права в киберпространстве. Прежде все-

го надо ответить на вопрос, что особенного в применении международного права вообще? В отличие от права национального, это система норм и принципов, не просто регулирующих отношения между субъектами, в данном случае государствами, но система норм и принципов, которая применяется каждым государством самостоятельно. Правоприменителями выступают политические лидеры государств.

Если мы занимаемся борьбой с компьютерной преступностью в рамках национального законодательства, коллеги из Следственного комитета приносят в суд имеющиеся доказательства и говорят: «Вот заключение эксперта, напали такие-то личности, ущерб причинен такой-то». Когда речь идет о международном праве, картина меняется. Хрестоматийный пример — дело о проливе Корфу (Дело Международного Суда ООН 1947–49 гг.). Албания разрешила Югославии заминировать свои территориальные воды, а Англия решила продемонстрировать, что обладает достаточной силой, чтобы игнорировать нежелание Албании пропускать по этим водам международные корабли. В результате два британских эсминца наскочили на мины, 45 человек погибли и 42 получили ранения. Когда этот инцидент рассматривался в Международном Суде, основным доказательством служили свидетельства международных наблюдателей, по словам которых Албания вела за проливом непрерывное наблюдение. Без согласия Албании заминировать эти воды было нельзя. Никаких предупредительных табличек или других обозначений, которые говорили бы о том, что воды заминированы, не было. Таким образом, Албания создала ситуацию, в которой корабли, идущие в соответствии с нормами международного морского права, получили ущерб. По решению Международного Суда к Албании, соответственно, были применены санкции.

Есть общее мнение государств — членов ООН о том, что положения международного гуманитарного права применимы ко всем видам боевых действий. В связи с этим возникает вопрос: что такое боевые действия и средства, с помощью которых осуществляется насилие? В настоящее время в отношении Российской Федерации введены санкции. Насилие ли это? Да, экономическое. Это не вооруженное насилие, не военные действия. Разница в том, что военные действия осуществляются вооруженными силами с помощью оружия. Вспомним определение оружия — это устройство или механизм, предназначенный для поражения живой силы и техники. А что такое кибератака? Это злонамеренное использование информационных технологий, то есть процессов и методов обработки и передачи информации. Так могут ли методы обработки и передачи информации быть оружием?

К сожалению, практически любое слово, написанное в международных договорах, являющихся источником международного гуманитарного права, будучи рассмотрено в той плоскости, о которой мы говорим, становится достаточно проблемным, начиная с базовых определений. Что такое *театр военных действий* в киберпространстве, что такое *нейтральные государства*, где пролегают их границы, да и вообще, где находятся границы государств? Что такое международно-правовая ответственность государств? Хороший пример: в 2001 г. было решение Генассамблеи ООН по конвенции об ответственности государства за международно-противоправное деяние. Однако не надо забывать, что эта конвенция решением ГА ООН была принята к сведению и не более того, и с тех пор каждые три года представляется Генеральной Ассамблее и возвращается на доработку. Но при этом понятие *приписанной ответственности* гуляет по юридической литературе. Кто приписы-

вает ответственность? Каждое государство самостоятельно, потому что оно является правоприменителем в этой сфере.

Много споров сейчас ведется насчет того, что считать достаточным доказательством нападения в киберпространстве? Учитывая, что киберпространство — это пространство IP-адресов и доменных имен, и практически все, что можно отследить по бэктрекингу, всегда можно подделать, поскольку данные находятся в компетенции операторов, провайдеров, а каждый оператор находится в юрисдикции своего государства, то проблема достоверности доказательств кибернападения остается нерешенной.

Еще один важный вопрос — что такое оружие в киберпространстве. По сути, это использование информационных технологий для причинения ущерба, но в какой момент технология становится оружием? Для решения этой проблемы была предложена концепция *неявного оружия*. За основу был взят прецедент трагедии 11 сентября 2001 г. в США, в связи с которой Совет Безопасности ООН принял два решения, в которых согласился с тем, что средством вооруженного нападения не обязательно является оружие. Такая концепция не дает ответов на все вопросы, поставленные выше, но помогает классифицировать злонамеренное использование информационных технологий как разновидность вооруженной атаки или вооруженного нападения. Самый простой случай — хакерская атака. Простой, потому что возможности хакеров ограничены: бюджетом, количеством людей, которые могут быть привлечены к работе, и, следовательно, результаты, которых можно достичь с помощью злонамеренного применения технологий, тоже ограничены. Самым опасным субъектом враждебного использования информационных технологий является государство. Ведь таких возможностей и ресурсов, какие есть у государств, нет больше ни у кого. С этой точки зрения для нас небезразлично, кто осуществляет атаку. Ведь одно государство может сымитировать атаку с территории другого, чтобы возник конфликт, и совершенно непонятно, как классифицировать эти ситуации.

Применимость международного права имеет два аспекта. Первый — возможность правоприменителя использовать существующие нормы, чтобы регулировать свое поведение или реагировать на использование информационных технологий в качестве оружия. Второй — единообразное понимание ситуации, в которой осуществляется правоприменение. В Уставе ООН есть положения, касающиеся применения силы, но до сих пор нет ответа, могут ли информационные технологии рассматриваться в качестве силы. Я считаю, что в ряде случаев это возможно, например в тех случаях, когда речь идет о *неявном оружии*. Но отмечу, что *сила* в Уставе ООН рассматривается как вооруженная сила, а экономическая сила как сила уже не рассматривается. Получается, что, если использовать эту концепцию, дорабатывать Устав ООН и другие источники международного права нужно будет по минимуму.

Значительно сложнее вопрос о применении международного гуманитарного права. Он был поднят, и Мария Станиславовна правильно отразила эти важные проблемы, но я хотел бы еще подчеркнуть вопрос о суверенитете. Все международные отношения строятся на понятии суверенитета, а оно привязано к территории. Можно говорить о суверенитете в воздушном пространстве. Государственная граница в этом случае — это некая воображаемая линия, которая уходит вертикально

вверх от географической границы, закрепленной на карте международными договорами. Договоры, которые определяют государственную границу, рассматриваются как источник международного права при разрешении спорных вопросов. Международное морское право определяет, как закрепляется граница территориального моря, на которое распространяется государственный суверенитет.

В области определения государственной границы киберпространства ничего подобного нет. Впрочем, не совсем так считают наши американские коллеги, которые полагают, что к данному случаю может быть применен подход, предложенный в *Таллинском руководстве.* Авторы Руководства предлагают привязывать объекты киберпространства к территории страны. Но для увязывания IP-адресов объектов киберпространства с национальной территорией необходимы данные, которые есть, насколько я знаю, только у Корпорации по управлению доменными именами и IP-адресами (ICANN). Эта организация присваивает адреса и ведет учет распределения адресного пространства, сотрудничая с несколькими другими аффилированными организациями. У ICANN есть реальная возможность осуществлять контроль, но это американская компания. Возникает вопрос, как остальные государства будут реализовывать свои суверенные права, которые им приписывают, приписывая также ответственность за то, что они не предотвратили злонамеренное использование информационных технологий со своей территории? Ведь на это государство может ответить: где моя ответственность, где я подписался под этим, где проходит граница?

Недавно мы совместно с коллегами из ICANN проводили научно-исследовательскую работу, изучали вопросы обеспечения безопасности функционирования Интернета, дискутировали с американскими коллегами о том, существуют ли политические риски того, что Интернет может быть использован для нарушения суверенных прав государств? Американцы согласились с тем, что такие риски существуют.

В 2003 и 2005 гг. проходили Всемирные встречи на высшем уровне по вопросам информационного общества, в ходе которых китайские коллеги предложили интернационализировать управление Интернетом. С тех пор прошло больше десяти лет, но мы до сих пор не можем договориться, зачем это делать и в чем должна заключаться суть интернационализации. На мой взгляд, единственная цель интернационализации Интернета состоит в том, чтобы предотвратить ограничение функционирования Интернета в одной стране по политическому решению руководства другой страны. Возможно, необходимо создать под эгидой Совета Безопасности ООН организацию, которая принимала бы такие решения на основании норм международного права вместо частной организации, находящейся под юрисдикцией того или иного государства. Для нас это важно. Мы не готовы делегировать это право США. У нас есть основания не доверять им, но оттого что мы не вполне доверяем американским коллегам, мы не перестаем быть членами международного сообщества. Поэтому проблему надо решать на многосторонней основе.

Возможно, было бы целесообразно создать международную организацию, которая бы занималась решением задач объективизации и атрибуции опасных для международной безопасности случаев злонамеренного использования информационных технологий. Если это делать в международном масштабе, а также выве-

сти операторов определенного уровня из-под национальной юрисдикции и отдать их под юрисдикцию международную, это поможет решить проблему. Пример такой организации — Международный орган по морскому дну, существующий в рамках международного морского права. Действительно, не видно, что делает государство на дне морском, но есть организация, которая пытается урегулировать возникающие в этой области проблемы.

Первым шагом, на мой взгляд, должна стать выработка международных правил поведения, хотя бы необязательных. В конце концов все принципы международного права до некоторой степени носят декларативный характер. В этом плане правила поведения в киберпространстве не будут сильно отличаться от остальных принципов. Группа правительственных экспертов ООН по международной информационной безопасности, которая закончила работу в 2015 г., уникальна потому, что впервые эксперты согласились с тем, что можно и нужно подумать над тем, что можно было бы положить в основу дальнейшего обсуждения регулирования поведения государств в киберпространстве.

Вторым шагом могло бы стать обсуждение того, как трактовать и отражать в международных договорах злонамеренное использование информационных технологий в киберпространстве против территориальной целостности и политической независимости других государств. Потому что наиболее действенным источником международного права является прежде всего международный договор.

АНДРЕЙ КОЗИК: Полагаю эту тему очень актуальной. Хочу отметить, что кроме нарастающей статистики применения кибервзаимодействия государств растет обсуждение проблемы в академических кругах.

Действительно, создано несколько площадок для межгосударственного диалога. Группа правительственных экспертов (далее — GGE), о которой уже шла речь, — одна из них. Однако GGE, в работе которой мне посчастливилось принимать участие, — это в меньшей степени юридический, скорее, политический форум. Любые решения, которые он принимает, хороши тем, что принимаются они на основе консенсуса. Но судить о применимости международного права на основании решений GGE я бы не стал. В лучшем случае, только лишь о политической составляющей вопроса. Что касается моего опыта работы в группе, то мне показалось, что наиболее настороженно, хотя и по различным основаниям, к применению международного права отнеслись делегации Китая и России. В работе группы и в итоговых документах чувствуется эта настороженность. Даже там, где применение международного права очевидно, — государства пытаются смягчить формулировки, опасаясь, видимо, быть связанными своей позицией в будущем.

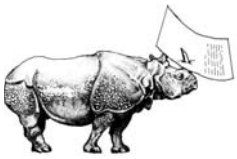
Однако право — это не политика. Оно консервативно, и норма, разработанная 50 лет назад, во время отсутствия предмета обсуждения, вполне может применяться сегодня. Так, ничто не помешало Международному суду ООН в Консультативном заключении о правомерности использования ядерного оружия сослаться на оговорку Мартенса, ставшей юридической нормой задолго до изобретения ядерной бомбы. Поэтому все те общественные отношения, которые уже урегулированы международным правом, продолжают ему подчиняться — не важно, с приставкой они *кибер-* или нет. При этом, что действительно важно, следует иметь в виду, что появляются и принципиально новые общественные отношения, которые раньше правом либо не регулировались, либо применение к ним суще-

ствующих норм приводит к конфликту самих норм в системе. Например, сложным вопросом является то, что в современной компьютерной сети информация, проходя путь от одного компьютера к другому, проходит по территории многих государств. Это нетипичная для международного права ситуация. В такой ситуации несут ли ответственность государства, если знают, что это вредоносный код? Каков предел их ответственности? Если государство желает действовать добросовестно, какими действиями ограничивается его поведение? Должно ли оно в ущерб своим интересам предпринять что-либо и т. д.? Здесь также возникают вопросы правомерности прослушивания телефонов лидеров государств и вообще электронного шпионажа.

Поскольку для многих государств неукоснительное применение норм международного права является приоритетом, были запущены академические проекты, призванные оценить применимость международного права к конкретным правоотношениям. Самым успешным и известным таким проектом является Таллинское руководство, созданное под руководством американского профессора Шмита международной группой экспертов. В настоящее время готовится вторая версия документа. Я имею удовольствие быть экспертом рабочей группы. Могу сказать, что это чисто академическая работа. Все нормы принимаются группой консенсусом, что бывает непросто. Группа объединяет экспертов со всего мира — от Австралии и Канады до Беларуси и Таиланда. Итоговый документ планируется подготовить в 2016 г.

Почему у европейцев и американцев находятся ресурсы для организации таких крупных научных проектов? Дело в том, что здесь есть понятные цели. Во-первых, и об этом не надо забывать, это престиж страны или организации, которая такое исследование проводит и публикует. То же Таллинское руководство пишется таким образом, чтобы любой прочитавший практик смог его немедленно применить. Оно издается ведущим академическим издательством и, как следствие, попадает в ведущие библиотеки мира, в министерства обороны, иностранных дел и другие профильные органы. Во-вторых, это влияние на практику государств. У нас масса примеров, когда академическая или общественная работа привела к созданию серьезных международных документов и изменению практики — вспомнить ту же Оттавскую конвенцию о запрещении противопехотных мин и проблематику химического оружия.

Для таких стран, как Россия, и таких организаций, как ОДКБ, на мой взгляд, создание подобных проектов жизненно важно. К сожалению, у нас традиционно мало внимания уделяется академической составляющей, а постсоветская наука международного права по прежнему обособлена от всего мира. Боюсь, что пока мы, вместо того чтобы создавать свои проекты и приглашать в них иностранных специалистов, будем критиковать чужие, так все и останется. Не думаю, что это конструктивно. Поэтому, на мой взгляд, долгосрочным устойчивым способом развития является создание и поддержание международных научных проектов. Это принесет ощутимую пользу и доктрине международного права, и нашим странам.



Алексей Лукацкий

КИБЕРБЕЗОПАСНОСТЬ ЯДЕРНЫХ ОБЪЕКТОВ

ВВЕДЕНИЕ

Говоря о безопасности ядерных установок, первое, что вспоминается, — это японская Фукусима и советский Чернобыль. При упоминании безопасности ядерных материалов приходят на ум истории с их кражами и голливудские боевики (например, пятый *Крепкий орешек*). Понятие *ядерная безопасность* прочно ассоциируется с ее физической составляющей. Именно ее обеспечению в настоящее время уделяется значительное внимание как на уровне государств, в которых осуществляется деятельность в области использования атомной энергии, так и на уровне международных организаций. Безопасность ядерных объектов является залогом стабильного развития программ, связанных с использованием атомной энергии в различных отраслях науки и экономики, например в генерации электроэнергии, медицине, судостроении, а также залогом энергетической безопасности регионов, где доля атомной энергетики в энергобалансе велика.

Обеспечение безопасности ядерных объектов является комплексной задачей и включает в себя множество аспектов. Для ее решения на ядерных объектах создаются различные системы защиты, каждая из которых предназначена для предотвращения угроз безопасности определенной природы. Примерами таких систем являются системы ядерной и радиационной безопасности, система учета и контроля ядерных материалов и система физической защиты ядерных материалов и установок — системы физической ядерной безопасности, а также система кибербезопасности.

Состав и структура каждой из систем обеспечения безопасности зависят от целей создания системы, а именно в предотвращении угроз конкретной природы в отношении конкретных объектов. При этом для реализации комплексного подхода к безопасности при проектировании каждой из систем необходимо учитывать влияние других угроз на достижение целей проектируемой системы.

В данной статье мы остановимся на системе кибербезопасности ядерных объектов. Здесь под системой обеспечения безопасности мы понимаем совокупность соответствующего оборудования и программного обеспечения, комплекса организационных и технических мер, а также персонала, реализующего эти меры. Актуальность развития и постоянного совершенствования систем кибербезопасности ядерных объектов связана с растущей ролью компьютерных технологий

и систем в управлении технологическим процессами ядерного объекта, обращении с информацией, значимой для безопасности ядерного объекта, и в управлении другими системами безопасности. Также безусловным индикатором необходимости развития и совершенствования систем кибербезопасности ядерных объектов является известные случаи кибератак на ядерные объекты. Дальнейшее обсуждение посвящено примерам кибератак, совершенных в отношении ядерных объектов, классификации киберугроз, а также обзору опыта РФ, США и МАГАТЭ в разработке нормативных документов и рекомендаций в области кибербезопасности, в том числе документов и рекомендаций, связанных с кибербезопасностью систем управления технологически процессами ядерных объектов и систем безопасности ядерных объектов.

ТАКСОНОМИЯ КИБЕРУГРОЗ

На сегодняшний день не существует общепринятой классификации кибератак (киберугроз) не только на объекты атомной энергетики, но и более общей. С одной стороны, это осложняет процесс моделирования киберугроз, а с другой — развязывает исследователям руки, позволяя использовать любую удобную для целей исследования модель. В частности, как нам кажется, очень удобной может быть модель, построенная на базе трех ключевых параметров любой угрозы:

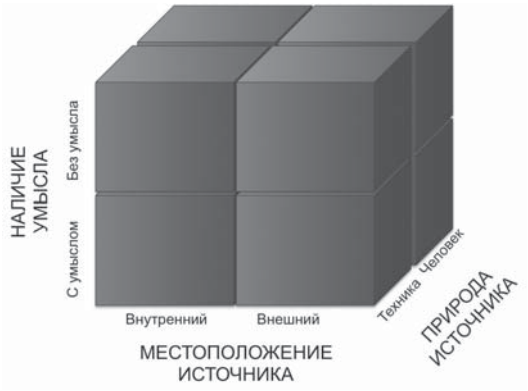
- местоположение источника ее возникновения;
- природа источника;
- наличие умысла.

Если проанализировать первый фактор классификации, то самым простым было бы разделить источник на внутренний и внешний. Специалисты по физической ядерной безопасности давно и активно занимаются противодействием *внутренним нарушителям*. Тому, как принимать персонал на работу, как выявлять нарушителей, как формировать культуру безопасности на ядерных объектах, снижающую опасность инсайдеров, посвящено немало рекомендаций, разработанных МАГАТЭ, и требований отдельных государств. С появлением интернета и подключением отдельных обслуживающих ядерные объекты процессов к всемирной сети (например, появилась электронная почта, из интернета скачиваются обновления от производителей оборудования и программного обеспечения, системы мониторинга и диагностики зачастую работают в Сети) стала нарастать и угроза внешнего вмешательства в работу ядерных объектов.

Источники киберугроз могут иметь как техногенную, так и антропогенную природу. Иными словами, нарушение одного из трех важнейших свойств информации и информационных систем ядерных объектов (доступность, целостность и конфиденциальность) может произойти как по причине воздействия человека на отдельные элементы ядерной инфраструктуры, так и по причине воздействия программного или аппаратного обеспечения. При этом разработчик может и не принимать непосредственного участия в негативном воздействии, либо не предполагать такого воздействия, либо готовить свою *акцию* для другого объекта.

Наконец, третьим измерением таксономии кибератак на ядерные объекты мы бы выделили наличие умысла. Очевидно, от наличия злого умысла при совершении

разрушающего или нарушающего работу ядерного объекта воздействия зависят методы, используемые источником атак (человеком или программой). При этом отсутствие злого умысла не должно быть основанием для исключения из рассмотрения возникающих в результате кибератаки проблем. Ведь нет разницы, ядерная установка прекратила свою работу по причине направленной на нее кибератаки или по причине вредоносного кода, случайно проникшего на USB-носителе, который принес с собой сотрудник подрядной организации, обслуживающей инфраструктуру установки.



Объединяя все вместе, мы получаем следующую классификацию киберугроз для ядерных объектов, которую легко изобразить в виде куба. Измерения куба отражают три ключевых параметра описания угрозы — местоположение источника, его природу и наличие умысла.

Разумеется, возможна еще большая детализация данной классификации и введение дополнительные параметров. Например, можно учесть объект воздействия — системы управления технологическими процессами (АСУ ТП), *завязанные* на работу с радиоактивными материалами, системы физической ядерной безопасности, нарушение работы которых может привести к диверсиям или хищениям ядерных материалов, или сопутствующие системы, воздействие на которые может привести к утечкам информации о работе атомного объекта. Можно учесть вид ущерба (утечка радиации, кража ядерных материалов, останов реактора и т. п.). Но такая детализация усложнит задачу и не требуется для целей данной статьи.

ИЗВЕСТНЫЕ ИНЦИДЕНТЫ НА ЯДЕРНЫХ ОБЪЕКТАХ

Адекватная статистика и тем более детальная информация по инцидентам кибербезопасности на критически важных, и тем более ядерных объектах отсутствует, а данные, которые есть в открытом доступе, не могут служить основанием для проведения глубокого анализа причин возникновения инцидентов, атрибуции их авторов и определения способов и методов реализации. Однако, несмотря на нехватку данных, можно составить список основных подтвержденных инцидентов кибербезопасности, произошедших в разное время в разных странах мира. К их числу можно отнести:

- АЭС Sellafield, Великобритания, 1991 г.;
- Игналинская АЭС, Литва, 1992 г.;
- АЭС Бредвелл, Великобритания, 1999 г.;
- АЭС David Besse, США, 2003 г.;

- АЭС, Япония, 2005 г.;
- АЭС Browns Ferry, США, 2006 г.;
- АЭС Hatch, США, 2008 г.;
- АЭС в Майами, США, 2008 г.;
- АЭС Areva, Франция, 2011 г.;
- АЭС San Onofre, США, 2012 г.;
- АЭС Susquehanna, США, 2012 г.;
- АЭС Monju, Япония, 2014 г.;
- АЭС KHNP, Южная Корея, 2014 г..

Все указанные инциденты хорошо ложатся в предложенную мной классификацию. Например, самая последняя из известных атак на атомный объект южнокорейской корпорации KHNP (занимает 5-е место в мире по выработке атомной энергии) произошла в декабре 2014 г. В рамках данной атаки пока не установленные (или публично не названные) злоумышленники направили партнерам и бывшим сотрудникам АЭС по электронной почте письмо, содержащее вредоносный код. Открытие данного письма привело к заражению компьютера и утечке данных, касающихся ядерных объектов KHNP. Второй стадией атаки стал взлом веб-сайта, на котором располагалось сообщество бывших сотрудников KHNP. В результате использования украденной учетной записи бывшего сотрудника была добыта очередная порция материалов, касающихся частной жизни действующих сотрудников корпорации KHNP. Наконец, на третьей стадии злоумышленники, воспользовавшись полученными сведениями, направили действующим сотрудникам атомных объектов KHNP специально подготовленные письма, которые должны были вызвать доверие и тем самым повысить шансы на успешное заражение компьютеров во внутренней сети KHNP. К счастью, на этом этапе инцидент был остановлен и ущерба ядерным объектам и циркулирующей на них информации нанесено не было. Данный инцидент имел внешнюю природу, исходил от человека (или группы лиц) и очевидно имел злой умысел.

Второй пример, который также хорошо ложится в предлагаемую классификацию, — это инцидент, произошедший в 2003 г. на атомной электростанции David Besse в Огайо (США). Внутренняя сеть компании, обслуживающей АЭС в Огайо, была заражена червем Slammer, который заражал сервера с программным обеспечением MS SQL Server 2000. В процессе проведения регламентных работ и в нарушение всех установленных на АЭС политик безопасности сотрудник обслуживающей организации установил прямое соединение между АЭС и сетью своей компании, чем не преминул воспользоваться вредоносный код, попавший внутрь сети АЭС David Besse. Неконтролируемое распространение червя привело к перегрузке сети и невозможности компьютеров в ней общаться друг с другом. В итоге система отображения параметров безопасности (SPDS) была недоступна в течение 6 часов 9 минут. Согласно предложенной классификации данный инцидент является внутренним, совершенным программой и без злого умысла.

Схожий инцидент произошел во Флориде в 2008 г. Инженер, обслуживающий обычную электростанцию в западном Майами, в обход всех правил отключил

основную и резервную системы противоаварийной защиты. В результате последующего сбоя из строя было выведено оборудование подстанции, а система противоаварийной автоматики не смогла его предотвратить. В итоге пострадало свыше 680 тыс. потребителей, оставшихся без электричества. Несколько компаний, продающих электроэнергию, потеряли контроль над своими энергосетями. В том числе пострадала атомная станция Turkey Point на юге Майами. В отличие от предыдущего, данный инцидент произошел по вине человека, но по-прежнему оставался внутренним и без злого умысла.

Нельзя сбрасывать со счетов внутренних нарушителей, действующих со злым умыслом, как это было в 1992 г. в Литве, когда программист Игналинской АЭС загрузил вредоносный код в автоматизированную систему, отвечающую за работу одной из подсистем реактора. Данный факт был своевременно обнаружен, для проведения всестороннего расследования АЭС была остановлена. Аналогичная ситуация, когда внутренний нарушитель действовал со злым умыслом, произошла в 1999 г. на АЭС в Бредвелле (Великобритания). В инциденте участвовал сотрудник службы безопасности атомной электростанции.

Наконец, последним примером, который мне хотелось бы упомянуть, является нашумевший *Stuxnet*, который был разработан спецслужбами США и Израиля специально для атаки на ядерные объекты Ирана. Данный вирус, занесенный извне в изолированную от внешнего мира систему управления заводом по обогащению урана в иранском городе Натанз, вывел из строя около тысячи центрифуг, что привело к существенному снижению объема производства обогащения урана, используемого в ядерной программе Ирана. Данный хорошо изученный пример отличается от вышеприведенных инцидентов тем, что это первый в истории случай, когда мы имеем дело с злоумышленным воздействием на ядерную инфраструктуру извне, которое привело к желаемому результату, продемонстрировав не только возможность, но и всю серьезность кибератак на атомные, да и на вообще на критически важные объекты. Более того, *Stuxnet* стал первым примером вредоносного кода, разработанного специально для атаки на атомный объект. В случае с внешней атакой на АЭС в Южной Корее, описанной выше, злоумышленники использовали традиционные методы заражения компьютеров, применяемые в обычных корпоративных и ведомственных сетях. В Иране же действовала специализированная вредоносная программа, аналогов которой с тех пор обнаружено не было (или нам о них пока неизвестно). Однако, нельзя говорить, что такое повторить невозможно. В 2014 г. было зафиксировано несколько заражений вредоносной программой *HAVEX*, которая, как и *Stuxnet*, была ориентирована на атаки именно на промышленные сети. В частности, *HAVEX* собирал данные, передаваемые с помощью промышленного протокола OPC, которые затем пересылались владельцам *HAVEX*. С какой целью проводилась эта разведка и как будут использоваться собранные данные о работе многих промышленных сетей (а то, что она будет использована, не вызывает сомнений), до сих пор непонятно.

ОБЗОР ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ НА ЯДЕРНЫХ ОБЪЕКТАХ

Информационные и автоматизированные системы, которые могут подвергнуться внешним или внутренним, техническим или человеческим, случайным или злоу-

мышленным атакам, могут использоваться в совершенно различных процессах на ядерных объектах — для обогащения, транспортировки ядерных материалов и радиоактивных отходов, выработки электроэнергии, производства ядерного топлива, хранения облученных ядерных материалов и радиоактивных отходов. Такое разнообразие защищаемых процессов и систем требует комплексного подхода к их безопасности, который на протяжении последних лет активно продвигается МАГАТЭ, а также прописан в нормативных документах регуляторов в области атомной энергетики ряда стран (например, США). Речь идет о программе кибербезопасности, которая включает в себя целый комплекс технических и организационных мер, повышающих защищенность и снижающих риски нанесения ущерба ядерным объектам. В обучающем курсе МАГАТЭ по компьютерной и информационной безопасности четко зафиксирована мысль, что не существует ни волшебного решения, ни оборудования, ни программного обеспечения, которые могут сделать организацию защищенной. Безопасность сегодня не гарантирует безопасность завтра. Поэтому список защитных мер, прописанных, например, в RG 5.71 американского NRC, или в американском же NEI 08–09, или в нормативных документах российского Росэнергоатома или ФСТЭК, насчитывает около двух сотен пунктов, планомерная и дифференцированная реализация которых позволяет надеяться, что ни информации, ни автоматизированным системам ядерных объектов, а через них и самим объектам, ядерным материалам и радиоактивным отходам, ядерному топливу не будет нанесен вред.

В частности, если дистанцироваться от конкретного нормативного акта (будь то NSS 17 МАГАТЭ, *Общие положения* Росэнергоатома, 31-й приказ ФСТЭК или руководящий документ NRC RG 5.71, о которых еще будет сказано ниже), все защитные меры могут быть разделены на 5 блоков, каждый из которых решает свой спектр задач кибербезопасности:

- идентификация активов и рисков;
- защита от угроз;
- обнаружение угроз;
- реагирование на угрозы;
- восстановление после реализации угрозы.

Каждый из пяти блоков может быть детализирован. Например, первый блок может включать в себя такие защитные меры, как управление защищаемыми активами и оценка рисков. *Защитный* блок включает в себя следующий набор мероприятий:

- контроль доступа;
- обучение и повышение осведомленности;
- защита данных;
- процедуры и процессы защиты информации и информационных систем;
- поддержка защитных мер.

Оставшиеся блоки включают в себя непрерывный мониторинг безопасности, обнаружение атак и аномалий, планирование процесса реагирования на инциденты, сбор доказательств, атрибуция кибератак, коммуникации с заинтересованны-

ми сторонами, анализ инцидента и *разбор полетов*, улучшение системы защиты, восстановление после сбоев и инцидентов и ряд других защитных мер.

Ядерные объекты исторически были изолированными и отделенными от интернета, а информационные системы на них были закрытыми, построенными по проприетарным технологиям и протоколам. Поэтому до недавнего времени никаких особых требований по кибербезопасности таких объектов не предъявлялось; основные мероприятия касались ядерной безопасности. По мере проникновения процессов информатизации на изолированные объекты ситуация начала меняться, а опасность киберугроз возрастать. Поэтому начиная с середины первой декады XXI века нормативные акты, регулирующие вопросы безопасности ядерных объектов, стали включать тематику кибербезопасности. Сначала это было просто упоминание необходимости защиты информации без какой-либо детализации. Более того, даже эти общие требования мало учитывали специфику защищаемого объекта, на котором надо не защитить информацию, а обеспечить бесперебойность функционирования технологических процессов. Однако с течением времени ситуация начала меняться в лучшую сторону, и сейчас многие государства разрабатывают и внедряют собственные программы обеспечения кибербезопасности ядерноых объектов.

МАГАТЭ

Когда МАГАТЭ начинало свою деятельность в области безопасности, оно фокусировалось на вопросах физической защиты ядерных объектов, материалов и радиоактивных отходов. Среди прочего, МАГАТЭ выпускало различные руководящие документы по тем или иным вопросам ядерной безопасности, объединенные в серию изданий МАГАТЭ по физической ядерной безопасности (Nuclear Security Series, NSS). В рамках данной серии были выпущены руководства по формированию культуры безопасности, борьбе с внутренними нарушителями, формированием проектных угроз и множеству других вопросов. Однако до 2009 г. среди этих документов не было ни одного, посвященного вопросам кибербезопасности.

Эта тема понемногу просачивалась в различные документы, но целостного взгляда на нее не было. Например, в NSS № 20 по основам физической ядерной безопасности (*Nuclear Security Fundamentals*) вкратце упоминается тема информационной безопасности и устанавливаются требования по:

- обеспечению конфиденциальности чувствительной информации и защиты активов, обрабатывающих чувствительную информацию;
- обеспечению адекватной защиты при обмене чувствительной информацией;
- обеспечению кибербезопасности в рамках общей атомной безопасности.

В пятой версии рекомендаций по физической безопасности ядерных материалов и ядерных установок (*Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*) появился раздел 4.10, в котором было установлено требование по защите компьютерных систем ядерных объектов от компрометации (например, кибератак, манипуляций и фальсификаций).

Однако комплексно к данной теме МАГАТЭ стало подходить, когда была сформирована программа по информационной и компьютерной безопасности (*Information*

and Computer Security Program), цель которой — предоставить государствам и ядерным объектам необходимые ресурсы, которые могут понадобиться при разработке и внедрении собственных программ по информационной и компьютерной безопасности, повышающих общий уровень обеспечения безопасности ядерных объектов. Фокусируется данная программа на трех темах, имеющих свое преломление в области информационных и телекоммуникационных технологий:

- неавторизованное уничтожение ядерных или иных радиоактивных материалов;
- диверсия против ядерных материалов или ядерных объектов;
- кража чувствительной информации по ядерной тематике.

Ресурсы, предоставляемые МАГАТЭ в рамках данной программы, включают:

- технические руководства;
- форумы по обмену технической информацией;
- региональные обучающие мероприятия;
- поддержку в проведении региональных и международных учений;
- экспертизу при реагировании на инциденты.

В части разработки технических руководств в серии изданий МАГАТЭ по физической ядерной безопасности в 2011 г. был разработан документ под номером 17 *Компьютерная безопасность на ядерных объектах* (*Computer Security at Nuclear Facilities*). Работа над ним была непростой и длилась целых 8 лет — первые наработки по нему появились еще в 2003 г., задолго до того, как в других государствах вплотную подступились к этой тематике. Переведен этот документ был на 6 рабочих языков Агентства.

На этом работа не остановилась, и в феврале 2015 г. был опубликован еще один документ, NSS 23-G *Безопасность информации по ядерной тематике* (*Security of Nuclear Information*), посвященный реализации принципа конфиденциальности и иных аспектов информационной безопасности (целостности и доступности) в сфере безопасности ядерных объектов. Данный документ по сути перекинул мост между существующими государственными и индустриальными требованиями по кибербезопасности и их применимостью в ядерной отрасли.

Еще два документа уже подготовлены и должны быть опубликованы ближе к концу 2015 г.:

- NST 037 *Обеспечение оценки защищенности на ядерных объектах* (*Conducting Computer Security Assessments for Nuclear Facilities*);
- NST 038 *Планирование реагирования на инциденты для событий компьютерной безопасности* (*Incident Response Planning for Computer Security Events*).

Наконец, последний документ, NST 036 *Меры компьютерной безопасности для контрольно-измерительных приборов и систем управления ядерных установок* (*Computer Security Controls to for Instrumentation and Control Systems at Nuclear Facilities*) разработан и разослан на согласование всем членам МАГАТЭ. Его публикация запланирована на 2016 г.

Также в разработке в Департаменте ядерной безопасности МАГАТЭ находятся еще два документа:

- NST 045 *Компьютерная безопасность для физической ядерной безопасности* (*Computer Security for Nuclear Security*). Данный документ должен пересмотреть и уточнить положения NSS 17;
- NST 047 *Методы компьютерной безопасности для ядерных объектов* (*Computer Security Methods for Nuclear Facilities*).

В разное время заявлялось о планах разработки еще ряда документов, но в настоящий момент об их судьбе авторам ничего неизвестно:

- *Развитие нормативно-правовой базы для обеспечения компьютерной безопасности ядерных объектов (Developing a Regulatory Framework for Computer Security for Nuclear Facilities)*;
- *Проведение учений по реагированию на инциденты в области компьютерной безопасности ядерных объектов и объектов, на которых используются радиоактивные материалы (Computer Security Incident Response Exercises for Nuclear/Radiological Facilities)*;
- *Обеспечение кибербезопасности при закупках (Ensuring Cyber Security in Procurement Processes)*;
- *Оценка угроз в области кибербезопасности (Cyber Threat Assessment)*.

При этом МАГАТЭ не забывает и про другие свои рекомендации, внося в них изменения, касающиеся вопросов кибербезопасности. Например, с 2012 г. начинается активный учет вопросов кибербезопасности при определении проектных угроз (Design Basis Threat), которые раньше не учитывались в рамках публикации NSS 10 *Разработка, использование и поддержка процесса моделирования проектных угроз* (*Development, Use and Maintenance of a DBT*).

В июне 2015 г. в Вене прошла конференция МАГАТЭ, целиком посвященная вопросам кибербезопасности ядерных объектов. По сути, это было первое мероприятие такого масштаба (около трехсот докладов), на котором представители разных стран делились своим опытом в области кибербезопасности. Можно предположить, что это мероприятие послужит толчком к развитию данного направления в национальном законодательстве стран-участниц МАГАТЭ.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

Исторически вопросы защиты информации в России регулировались Федеральной службой по техническому и экспортному контролю (ФСТЭК), которая унаследовала от своей предшественницы, Гостехкомиссии России, право устанавливать соответствующие требования. Они были установлены как для сведений, составляющих государственную тайну, так и для конфиденциальной информации, обрабатываемой в различных автоматизированных и информационных системах. При этом основной акцент российским регулятором делался именно на сохранности защищаемой информации, то есть на конфиденциальности. В 1992 г., а именно тогда появились первые несекретные требования по защите информации, никто не задумывался о таких свойствах информационных систем, как доступность

и целостность, которые имеют первоочередное значение для ядерных и любых других объектов, на которых функционируют автоматизированные системы управления технологическими процессами (АСУ ТП), в том числе и в ущерб конфиденциальности.

Так продолжалось более двадцати лет. Организации, имеющие отношение к ядерной отрасли, сначала самостоятельно, а позже через соответствующий орган управления использования атомной энергии, *Росатом*, также использовали требования ФСТЭК в качестве руководства к действию. И хотя данные требования исходили из совершенно иной парадигмы, мало применимой к атомным объектам, это не мешало применять к ним принципы защиты обычных ведомственных и корпоративных сетей.

Так, приказом Федерального агентства по атомной энергии от 4 августа 2006 г. № 395 была разработана и утверждена Типовая инструкция по защите информации в автоматизированных системах предприятий и организаций Федерального агентства по атомной энергии. Спустя 5 лет был утвержден приказ ОАО *Концерн Росэнергоатом* от 9 февраля 2011 г. № 119 *О мерах по исключению неконтролируемого доступа к ПТС АСУ ТП*.

В конце 2012 г. когда ФСТЭК решила разработать новые требования по защите информации и информационных систем, лучше соответствующие текущему уровню развития информационных технологий. Такой приказ, получивший название *Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах* (Приказ № 17), был утвержден 11 февраля 2013 г. Спустя месяц был утвержден схожий приказ ФСТЭК (Приказ № 21), ориентированный на защиту информационных систем, содержащих персональные данные граждан. Эти документы мало чем отличались по своей идеологии и списку защитных мер, которые оператор информационной системы волен был выбирать самостоятельно. Во главу угла была поставлена конфиденциальности информации, но при этом впервые в официальном документе регулятора нашли свое отражение требования обеспечения целостности и доступности защищаемой системы и циркулирующей в ней информации.

Спустя год, 14 марта 2014 г. был утвержден еще один приказ ФСТЭК (Приказ № 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*. Схожий по набору защитных мер с 17-м и 21-м приказами, новый документ был ориентирован на защиту АСУ ТП, в том числе на ядерных объектах. При этом в качестве основной задачи этот приказ постулировал необходимость обеспечения бесперебойного функционирования технологических процессов. Доступность и целостность были поставлены во главу угла.

Помимо множества несомненных достоинств у 31-го приказа есть и недостаток, причем перевешивающий все его достоинства. Юридическая сила этого приказа неочевидна. Дело в том, что он разрабатывался по прямому распоряжению Президента России и не опирается ни на один федеральный закон, который был делал этот приказ обязательным к применению всеми организациями, которые пере-

числены в его введении. Подготовленный в 2013 г. законопроект *О безопасности критической информационной инфраструктуры* так пока и не принят.

В таком правовом вакууме за дело взялся концерн *Росэнергоатом*, который в январе 2014 г. выпустил обязательный при обеспечении безопасности атомных электростанций документ под названием *Общие положения по обеспечению безопасности информации автоматизированных систем контроля и управления технологическим процессом на АЭС*. Данный документ опирался не на 31-й приказ ФСТЭК, а на 17-й, имеющий ряд недостатков, связанных с тем, что акцент делается на защите информации, а не на технологических процессах и системах управления и контроля.

В 2015 г. концерн *Росэнергоатом* планировал принять еще два обязательных документа *Системы контроля и управления, средства автоматизации АЭС. Защита информации от несанкционированного доступа и воздействий. Требования информационной безопасности при монтаже, наладке и эксплуатации АСУ ТП* и *Системы контроля и управления, средства автоматизации АЭС. Защита информации от несанкционированного доступа и воздействий. Требования информационной безопасности при проектировании, конструировании и изготовлении АСУ ТП*, которые схожи по своей идеологии с 31-м приказом ФСТЭК.

Общие положения, утвержденные *Росэнергоатомом* в 2014 г., определяют общие принципы, критерии и требования в области обеспечения кибербезопасности АСУ ТП АЭС и предполагают разработку необходимых мер и действий (организационных мероприятий и технических решений) по обеспечению информационной безопасности и координации требований по кибербезопасности АСУ ТП применительно к отдельным элементам и системам контроля и управления, а также АСУ ТП в целом. Такая разработка более детальных технических требований к обеспечению информационной безопасности АСУ ТП АЭС начата и позволит конкретизировать специально разрабатываемые технические требования к процедурам проверки комплектующих, разработки, изготовления и испытаний ПТС систем контроля и управления АЭС и технические требования к монтажу, наладке и эксплуатации (включая внесение изменений, техническое обслуживание и ремонты) ПТС систем контроля и управления АЭС.

В целом, надо признать, что текущие требования, разработанные ФСТЭК или *Росэнергоатомом,* являются, с одной стороны, обязательными к применению, а с другой, достаточно техническими, мало учитывающими управленческие и организационные вопросы обеспечения информационной безопасности, упомянутые в документах МАГАТЭ. С другой стороны, никто не мешает применять документы МАГАТЭ в России, которые только дополнят упомянутые выше требования ФСТЭК и *Росэнергоатома*.

США

В США вопросы гражданского применения ядерных материалов регулирует NRC, который так же, как и МАГАТЭ, как и *Росатом*, на первых порах основное внимание уделял традиционным вопросам физической ядерной безопасности ядерных установок, материалов и радиоактивных отходов. Например, среди документов выпущенных NRC, есть такие:

- Регулирующее руководство 5.66 *Авторизация доступа персонала на атомные электростанции* (*Personnel Access Authorization for Nuclear Power Plants*),
- Регулирующее руководство 5.77 *Программа нейтрализации воздействия внутренней угрозы* (*Insider Mitigation Program*),

которые имеют свои аналоги в свыше чем 100 странах — членах МАГАТЭ.

Однако с начала 2000-х гг. NRC начинает учитывать вопросы кибербезопасности в своей деятельности. В 2001 г. был опубликован бюллетень с рекомендацией допускать к обеспечению кибербезопасности на атомных объектах только те организации, которые имеют соответствующую лицензию. В 2002 г. эта рекомендация превращается в обязательный приказ (NRC Order EA-02-026 *Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants*). Кстати, лицензирование деятельности в области защиты информации, — это то, что объединяет США и Россию; в России третьим лицам также требуется получить специальное разрешение на предоставление услуг в области защиты информации. Правда, в России такое требование распространяется на услуги любой организации во всех отраслях экономики, в отличие от США, где это оно ограничено только критическими отраслями, включая атомную энергетику.

В 2004 г. NRC выпускает еще один документ, посвященный самооценке АЭС в области кибербезопасности (NUREG/CR-6847 *Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants*). Спустя год Институт по атомной энергетике США (NEI) выпускает руководство по построению программы информационной безопасности на атомных электростанциях (NEI 04-04 *Cyber Security Program for Power Reactors*). По сути, именно с этого документа начинается планомерное включение темы с приставкой *кибер* в документы американского регулятора NRC. Однако само руководство NEI 04-04 так и не было согласовано с регулятором, который начал самостоятельно готовить документы по информационной безопасности. NEI же позже выпустило второй документ, получивший поддержку NRC и названный *План кибербезопасности для ядерных реакторов* (NEI 08-09 *Cyber Security Plan for Nuclear Power Reactors*).

В 2007 и 2009 гг. соответственно NRC выпускает документы в смежных темах — обновленное руководство по выбору программного обеспечения для контрольно-измерительных систем (*Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems*, NRC BTP 7-14) и *Руководство по защите компьютеров, коммуникаций и сетей* (*Protection Of Digital Computer and Communication Systems And Networks*, 10 CFR 73.54).

В 2008 г. NRC начинает разработку проекта всеобъемлющего документа по кибербезопасности ядерных объектов. Проект этого документа (DG-5022) получил много отзывов и комментариев и уже в 2010 г. превратился в основополагающий и обязательный руководящий документ для всех подрядчиков ядерной отрасли США. Это RG 5.71 *Программа кибербезопасности для ядерных объектов* (*Cyber Security Programs for Nuclear Facilities*). Данное руководство базировалось на уже существующих в США и принятых Национальным институтом стандартизации (NIST) специальных публикациях SP00-53 и SP800-82, описывающих защитные меры, которые должны быть реализованы в государственных информационных системах. RG 5.71 транслировал эти требования на атомную энергетику. По сути,

Россия пошла тем же путем, когда *Росэнергоатом* и ФСТЭК взяли за основу своих документов по защите критических инфраструктур и, в частности, АЭС уже имеющиеся документы, учтя в них специфику отрасли.

Если сравнивать RG 5.71 с предыдущими документами (NIST и NEI), то соотношение будет следующим:

- NIST SP800-53 rev.4 содержит 237 защитных мер (против 198 в предыдущей версии): 91 техническую, 97 операционных и 49 управленческих;
- NEI 08-09 R6 содержит уже 139 защитных мер, из них 71 техническую, 61 операционную и 7 управленческих;
- NRC RG 5.71 содержит 147 защитных мер, из них 71 техническую, 67 операционных и 9 управленческих.

Именно RG 5.71 является сегодня обязательным документом по кибербезопасности атомных объектов в США, наряду с другими документами выпущенными NRC по другим вопросам ядерной безопасности.

ЗАКЛЮЧЕНИЕ

К счастью, известные и упомянутые выше инциденты не привели ни к хищению ядерных материалов, ни к облучению людей, ни к радиационному загрязнению окружающей среды. Значит ли это, что таких последствий не может быть в принципе? Увы, с уверенностью утверждать это мы не можем. С учетом процессов информатизации, которые наблюдаются в ядерной отрасли многих стран мира, вероятность кибератак на информационные системы не является нулевой.

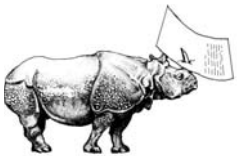
Как правильно написано в стандарте по кибербезопасности североамериканской электроэнергетической корпорации NERC, цель ее киберпрограммы «гарантировать, что автоматизированные системы и коммуникационные сети, необходимые для надежной поставки электроэнергии в стране, **разумно** защищены от атак из различных вероятных источников угроз, а также поддерживают жизнеспособность и эффективность такой защиты». Аналогичная задача может и должна решаться для ядерных объектов, что достигается комплексным внедрением различных защитных мер, организационных и технических, управленческих и юридических, применяемых в правильное время и в правильном месте и только после всестороннего изучения объекта защиты и рисков, которые с ним связаны.

В последние несколько лет при разработке проектных угроз (design of basic threats) ядерным объектам многие государства и МАГАТЭ стали всерьез рассматривать кибер-природу совершения противоправных или случайных действий в отношении ядерных установок или ядерных материалов. Также положено начало формированию нормативной и методической базы и единых подходов к обеспечению кибербезопасности, как части мер по обеспечению безопасности ядерных объектов. В связи с относительной новизной проблемы говорить о том, что существует какие-то правильные или неправильные подходы, работающие или неработающие защитные меры для ядерных объектов не приходится.

Обратившись к России, хочется отметить, что у нас сделан хороший задел в части обеспечения информационной безопасности атомных электростанций, находя-

щихся в ведении *Росэнергоатома*. Однако ядерные объекты не ограничены только епархией *Росэнергоатома* или даже *Росатома*. Есть и такие, которые находятся под эгидой минпромторга (например, какой-нибудь завод битумных материалов, который производит кокс, нефтепродукты и ядерные материалы). И особых требований по информационной безопасности для таких объектов у минпромторга нет. Одна из проблем, присутствующих при формировании нормативных требований в области ядерной кибербезопасности — разобщенность регуляторов. Необходима координация действий разных ведомств, которые бы объединили свои усилия в части регулирования вопросов кибербезопасности критических инфраструктур в целом и ядерных объектов в частности. Пока это недостижимая мечта. Видимо, русская поговорка *пока гром не грянет, мужик не перекрестится* как нельзя лучше подходит к описанию этой ситуации.

Необходимы дальнейшие исследования, направленные на оценку эффективности и недостатков тех защитных мер и подходов, которые описаны в документах МАГАТЭ, РФ и США, которые обсуждались в статье, а также на оценку практики применения самих документов и их полноты и достаточности. На основе полученных результатов могут быть разработаны инструменты оценки достаточности мер, предпринимаемых на уровне конкретного государства и его ядерных объектов для обеспечения кибербезопасности, а также рекомендации по коррекции выявленных недостатков. Наличие таких инструментов будет, помимо прочих, полезно странам, только начинающим разработку своих ядерных программ. 



Ван Гоюй[1]

НЕДОСТАТКИ ДПРОК: РЕАЛЬНЫЕ ИЛИ МНИМЫЕ? ВОЗМОЖНЫЕ ПУТИ РЕШЕНИЯ ПРОБЛЕМЫ КОНТРОЛЯ НАД ВООРУЖЕНИЯМИ В КОСМОСЕ

ВВЕДЕНИЕ

Космос бесконечно далек от нас, чего нельзя сказать о кризисе в космической сфере. Он может разразиться внезапно, а его последствия будут роковыми и необратимыми. Космическое пространство становится все более густонаселенным, усиливается конкуренция, множатся споры. В обществе растут опасения (особенно после выхода фильма *Гравитация*) в связи с тем, что в ближайшие десять лет угрозы существованию космических программ могут возрасти в силу естественных или техногенных причин[2], что, в свою очередь, может привести к дальнейшей милитаризации космического пространства[3]. К тому же действующие нормы космического права не могут регулировать все сложные вопросы, связанные с новыми космическими технологиями и новыми видами космической деятельности, и не отвечают всем имеющимся потребностям.

Контроль над развертыванием вооружений в космосе и космический мусор принято считать наиболее серьезными угрозами безопасности космической деятельности, стоящими перед международным сообществом.

Что касается контроля и регулирования в сфере космической безопасности, то по вопросу предотвращения гонки вооружений в космическом пространстве (ПГВК) согласия и тем более договоренностей достигнуто гораздо меньше, чем в решении проблемы космического мусора. При этом наиболее существенные проблемы, которые возникают в сфере защиты от космического мусора, носят технический характер, в то время как наиболее острые проблемы в области ПГВК относятся к разряду политических и юридических.

Деятельность по ПГВК в значительной степени опирается на статью IV Договора о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела (ДК), в которой, однако, устанавливается лишь ограниченный контроль над вооружениями, а также вводится принцип мирного использования космоса. Она не запрещает размещение в космосе обычных вооружений, а создание военных баз, сооружений и укреплений, испытания любых типов оружия и проведение военных маневров запрещаются лишь на *небесных телах*; иными словами, использование для этих целей

околоземной орбиты и орбит небесных тел считается допустимым. Кроме того, статья IV ДК не запрещает использование лазеров и испытание противоспутниковых систем.

Помимо несовершенства действующей нормативно-правовой базы серьезную сложность с точки зрения ПГВК представляют такие новые темы, как самооборона в космосе, активное удаление космического мусора и кибербезопасность космической деятельности. Они преподносятся как основание, оправдание или предлог для размещения оружия, применения силы или угрозы силой в космическом пространстве. При этом следует учесть, что грань между нападением и обороной, равно как и между военными и невоенными целями, становится все более размытой. Кроме того, необходимо принять во внимание и особенности процесса разработки регулятивной базы в этой сфере.

В последние годы, особенно после 2007 г., все чаще звучат призывы установить новые нормы, регулирующие космическую деятельность, которые способствовали бы обеспечению безопасности, надежности и долгосрочной устойчивости космической деятельности. Ряд инициатив о выработке новых норм в этой области уже обсуждался на нескольких международных площадках. Одной из таких инициатив был проект Договора о предотвращении размещения оружия в космическом пространстве, применения силы или угрозы силой в отношении космических объектов (ДПРОК). Проект был впервые представлен Китаем и Россией на Конференции по разоружению (КР) в 2008 г.

ДПРОК

10 июня 2014 г., спустя две недели после того, как в конце мая в Люксембурге завершился третий раунд консультаций открытого состава по разработке международного кодекса поведения для космической деятельности (МКПКД), проводимых по инициативе Европейского Союза, Россия и Китай представили на КР новую версию проекта ДПРОК[4].

Выбор момента для внесения нового варианта проекта позволяет предположить, что для России и Китая этот шаг был продиктован не столько желанием ускорить разработку документа, сколько стремлением вдохнуть жизнь в Конференцию по разоружению, и, используя *мягкую силу,* сохранить свое влияние на страны третьего мира в составе ООН, а также отвлечь внимание от МКПКД и в целом от попыток Группы правительственных экспертов использовать меры по обеспечению транспарентности и укреплению доверия для решения проблем безопасности в космическом пространстве[5]. Кроме того, новый проект предоставляет Европе историческую возможность вернуть свое лидерство в вопросах разработки правил в области космической деятельности, целью которой является поддержание безопасности и стабильности в космическом пространстве, иными словами, сохранение экологически чистого космоса, что является залогом охраны окружающей среды на нашей планете.

Однако ряд стран не поддержал новый проект ДПРОК по самым разным причинам. Делегация США заявила, что ДПРОК «не отвечает необходимым критериям, ... документ не предусматривает эффективный режим проверки и контроля за соблюдением, не учитываются противоспутниковые системы наземного бази-

рования, представляющие наиболее серьезную и непосредственную угрозу». Составители документа утверждают, что большинство негативных комментариев по ДПРОК являются субъективными или предвзятыми и требуют дальнейшей тщательной проверки.

Отдельные лица и делегации, в особенности делегация США, указывали, что в рамках ДПРОК, даже с учетом последних поправок, не рассматривается целый ряд вопросов. Большинство критиков проекта выделяют три темы: не учитывается проблема испытаний противоспутниковых систем (ПСС) наземного базирования, нет механизма контроля и положений, касающихся космического мусора.

ПРОБЛЕМА ИСПЫТАНИЙ ПСС НАЗЕМНОГО БАЗИРОВАНИЯ

Один из экспертов, прокомментировавших новый проект, отметил, что ДПРОК не получил широкого одобрения прежде всего потому, что в нем не рассматриваются ПСС прямого запуска. По мнению эксперта, проект запрещает лишь коорбитальные противоспутниковые системы, совершенно не учитывая более опасные системы наземного базирования, целью которых могут стать объекты в космическом пространстве, что продемонстрировало испытание китайской противоспутниковой системы в 2007 г.[6].

Во-первых, противоспутниковые системы действительно представляют серьезную угрозу безопасности космической деятельности, особенно с учетом того, что в результате их применения образуется космический мусор. В связи с этим можно отметить, что аргумент, приведенный выше, отражает реальную обеспокоенность относительно защиты космического пространства, особенно с позиции представителей частного сектора. Однако с точки зрения логики утверждение о том, что противоспутниковые системы наземного базирования несут более серьезную опасность, представляется неверным. Космический мусор опасен вне зависимости от способа его образования — не важно, появился он в результате действия систем наземного или орбитального базирования. Кроме того, прямо скажем, ДПРОК, пусть и не учитывающий проблему испытаний противоспутниковых систем, лучше, чем правовой вакуум. Учитывая эти соображения, указанный довод против ДПРОК представляется неубедительным. В конце концов, кому плохо от того, что Россия и Китай сами вызываются ограничить свой военный потенциал в космосе, подписав соответствующий договор?

В чем же реальная причина такой разницы в позициях по этому вопросу? Все дело в том, что стратегическое соперничество между США и Россией/Китаем на земле переносится в космическое пространство.

Здесь следует отметить две проблемы. Во-первых, необходимо учитывать, что размещение оружия в космическом пространстве и испытания ПСС являются инструментами защиты национальных интересов и средствами стратегического сдерживания. Во-вторых, возникает вопрос, до какого момента они могут использоваться в таком качестве и каковы будут результаты тщательного, всеобъемлющего анализа их эффективности в долгосрочной перспективе.

Учитывая, что китайской стороной было проведено несколько тайных испытаний противоспутниковых систем, о чем не так давно стало известно из заявлений

министерства обороны и Госдепа США, Китай вовсе не собирается ограничить применение этих систем, распространив на них действие ДПРОК.

Что касается испытаний ПСС, то и США, и Россия до 2007 г.[7] провели десятки таких испытаний, поскольку «на заре освоения космоса противоспутниковое оружие, пожалуй, являлось единственным способом получить контроль над космическим пространством»[8]. Первопроходцы всегда стремятся не подпускать слишком близко тех, кто следует за ними, желая навсегда закрепить за собой достигнутые преимущества. Поэтому начиная с 2007 г. США выступают с резкой критикой испытаний ПСС, проводимых Китаем, несмотря на то что эти испытания не привели к образованию космического мусора.

Кроме того, испытание 2007 г. поставило Китай в беспрецедентно сложное с дипломатической точки зрения положение. Все прошлые достижения Китая в космической сфере и его вклад в освоение космического пространства были почти позабыты, и на страну обрушился шквал осуждения со всех концов света — из США, Европы, развивающихся стран, со стороны международных организаций, частного сектора и научных кругов. С тех пор о Китае закрепилось представление как о безответственном государстве, которое представляет серьезную угрозу космической безопасности, и поэтому должно постоянно находиться под пристальным вниманием международной общественности. Осуждающие комментарии слышны со всех сторон, и за каждым из них стоят свои мотивы и цели. Единодушие критиков Китая играет на руку США, позволяя им отвлечь внимание мировой общественности от усилий, цель которых — не допустить размещения оружия в космическом пространстве. Вместо этого США на каждом заседании по контролю над вооружениями заявляют о необходимости принять новые правила, запрещающие использование ПСС. В прошлом США также сталкивались с аналогичным давлением, вызванным противоречием между необходимостью наращивания оборонительных и наступательных потенциалов и потребностями международного сообщества в демилитаризации космоса.

Кроме того, отсутствие решения по данной проблеме ослабляет стратегическое преимущество Китая в его геополитическом соперничестве с Японией, Индией и другими соседними государствами, и — что еще хуже — Китай может потерять поддержку развивающихся стран в космической сфере. Таким образом, в настоящее время Китай оказался перед дипломатической дилеммой. При этом Китаю хотелось бы, чтобы в космической сфере (как и в других направлениях его политики) его воспринимали как ответственного игрока, который руководствуется международными стандартами[9].

С другой стороны, Китай серьезно заинтересован в развитии противоспутниковых технологий, учитывая его стратегическое соперничество с США. С конца 90-х гг. сохраняются проблемы в отношениях Китая и США в космической сфере, которые обусловлены сложностями в двусторонних отношениях государств. Враждебный настрой по отношению к коммунистическому Китаю, сохраняющийся в политике США, а также необходимость обеспечивать защиту чувствительных технологий в сочетании с позицией самопровозглашенного лидера в космическом пространстве обусловливают негативное отношение Соединенных Штатов к китайской космической программе. США рассматривают Китай как наиболее вероятного претендента на оспаривание их господства в космической сфере. Например,

в рамках одного из военных учений, которые проводились США в 2001 г., именно Китай выступал в качестве предполагаемого противника[10]. Поэтому, по мнению высшего руководства Китая, страна должна «разрабатывать современные системы вооружений для ведения боевых действий в космосе»[11]. Таким образом, Китай стал новым участником старой игры под названием *гонка вооружений в космосе*.

Учитывая все вышесказанное, в ближайшее время убедить США и Китай изменить свои позиции по вопросу о противоспутниковых системах будет непросто.

Что касается предотвращения гонки вооружений в космическом пространстве (ПГВКП), политика США в космической сфере всегда уделяла большое внимание планам по созданию системы ПРО космического базирования и противоспутникового оружия. В этих областях США обладают наиболее развитыми технологиями. С одной стороны, для России и Китая нежелательно любое нападение из космоса, хотя с другой стороны они могут надеяться, что им удастся замедлить деятельность США по размещению оружия в космическом пространстве. Это поможет им выиграть время и наверстать отставание.

Очевидно, что и размещение оружия в космическом пространстве, и использование ПСС создали бы угрозу международной безопасности и спровоцировали столь нежелательную гонку вооружений в космическом пространстве. Однако на данном этапе вряд ли реалистично надеяться, что удастся запретить один или оба этих вида деятельности с помощью договора, выработанного в результате политических переговоров.

Было бы полезно рассмотреть возможность разработки не имеющего юридически обязывающей силы кодекса поведения, в котором говорилось бы как о предотвращении размещения оружия в космическом пространстве, так и о не использовании ПСС в случае, если это ведет к образованию долгоживущего космического мусора.

Что касается осуществимости этой идеи, Китаю, возможно, будет труднее принять ее, чем США: до настоящего времени Китай так и не признал, что в 2007 г. он проводил испытания ПСС, поэтому в этом отношении потребуется приложить большие усилия; Китаю необходимы позитивные изменения, которые помогли бы восстановить равновесие среди космических держав и позволили бы ему внести свой вклад в обеспечение международной космической безопасности. Соединенным Штатам, возможно, будет легче согласиться на этот компромисс. Во-первых, учитывая, что США обладают наиболее передовыми технологиями, а остальные государства имеют ограниченные возможности для контроля, Соединенные Штаты могли бы размещать оружие в космическом пространстве, когда и где пожелают, и никто не смог бы их в этом уличить. Даже в случае утечки информации США смогут отрицать все обвинения и продолжать преследовать свои национальные интересы. Такие примеры уже были — США и ранее нарушали международное право, не говоря уже о нормах, регулирующих поведение в космосе, которые не являются юридически обязывающими.

Однако не следует недооценивать эффективность не имеющих юридически обязывающей силы международных инструментов. Не являясь юридически обязывающим, они, тем не менее, налагают политические обязательства. Иными словами, любое государство понимает, что нарушая эти правила, оно рискует своим авто-

ритетом и репутацией, сохранение которых в наше время является одной из наиболее важных стратегических задач каждого государства, в особенности сверхдержав.

Кроме того, как установил политолог Дж. Рагги, для соглашения о сотрудничестве важно не только количество участников, но и создание определенной *социальной среды* между ними. Поэтому любые международные документы и даже дискуссия, предшествующая их принятию, способствуют формированию такой *социальной среды*, которая будет способствовать демилитаризации космоса[12].

Другим аргументом, приведенным делегацией США, было то, что в краткосрочной перспективе более *мягкие* правила оказываются эффективнее юридически обязывающих соглашений о контроле над вооружениями. Это стало еще одной причиной, по которой США восприняли китайско-российское предложение в штыки. Однако это не значит, что если договор превратится в кодекс, США поддержат это предложение. Например, в своем выступлении на Конференции по разоружению помощник государственного секретаря США Ф. Роуз упомянул необязывающие договоренности по таким вопросам, как предупреждение образования космического мусора, обмен информацией, негативное воздействие радиочастотных помех и т. д., но даже вскользь не затронул проблему размещения оружия в космическом пространстве. В системе аргументации США это является слабым местом.

К большому сожалению, ни Китай, ни Россия не указали на это несоответствие и не воспользовались преимуществом, которое дает избирательный подход американской стороны, чтобы загнать ее в политический цугцванг.

Представляя проект договора в 2014 г., Китай и Россия снабдили текст пояснительной запиской, в которой излагалась их изначальная точка зрения. В ней говорилось: «Мы считаем, что юридически обязывающий запрет на размещение оружия в космическом пространстве является одним из важнейших инструментов укрепления глобальной стабильности и равной и неделимой безопасности для всех».

Авторам кажется, что Китай и Россия не должны слишком настаивать на необходимости или важности юридически обязывающего ДПРОК, или, точнее, не должны создавать у партнеров ощущения, что они на нем настаивают. В противном случае у них останется слишком мало возможностей для отстаивания своего мнения. На данном этапе чрезвычайно сложно достичь консенсуса даже по кодексам, которые носят добровольный характер, не говоря уже о юридически обязывающих документах.

КОНТРОЛЬ

Выступая на Конференции по разоружению, посол Китая Ху Сяоди отметил, что «на данный момент правовой инструмент, регулирующий поведение в космосе, мог бы быть создан без механизма контроля. В дальнейшем, по мере развития науки и технологий, когда наступит подходящий момент, можно будет вернуться к обсуждению вопроса о механизме контроля».

Кроме того, четыре договора, регулирующие деятельность в космическом пространстве, — Договор по космосу 1967 г., Соглашение о спасании 1968 г., Конвенция о международной ответственности за ущерб, причиненный космическими

объектами, 1972 г. и Конвенция о регистрации объектов, запускаемых в космическое пространство, 1975 г. — внесли неоценимый вклад в глобальное регулирование в этой области, хотя ни в одном из них не был прописан механизм контроля.

Поэтому утверждение, что ДПРОК не будет исполняться, поскольку в нем не предусмотрены методы контроля, опирается скорее на политические мотивы, а не реальные технологические проблемы.

КОСМИЧЕСКИЙ МУСОР

По мнению делегации США, проект договора также не учитывает такую существенную проблему, как космический мусор, который в долгосрочной перспективе представляет угрозу устойчивости космической деятельности, особенно находящийся на низкой околоземной орбите. Как заявила американская сторона, проблема космического мусора не упоминается в предлагаемом проекте договора, несмотря на то что она представляет гораздо большую угрозу, чем размещение оружия в космическом пространстве. Маловероятно, что в ближайшее время какое-либо из государств сможет приступить к размещению в космическом пространстве оружия, в том числе оружия массового уничтожения, в то время как накопившийся космический мусор уже мешает нормальной работе космических объектов. Проблема усугубляется реальной угрозой со стороны мощных противоспутниковых систем прямого наведения, предназначенных для непосредственного уничтожения целей. ДПРОК должен признать серьезность проблемы космического мусора, причиной возникновения которого является использование ПСС прямого запуска, однако составители текущего проекта договора предпочли обойти этот вопрос вниманием, указывает делегация США.

Как следует из аргументации американской стороны, гонка вооружений в космическом пространстве — вопрос отдаленной перспективы, а проблема космического мусора требует немедленного решения, следовательно, в ДПРОК нет необходимости, поскольку в нем не рассматривается вопрос о космическом мусоре.

На деле же все обстоит совсем иначе.

Во-первых, ДПРОК не задумывался как всеобъемлющий договор, охватывающий все важные вопросы в космической области; также не ставится задача заменить им существующий Договор по космосу.

Во-вторых, Конференция по разоружению является платформой для обсуждения вопросов использования космического пространства в военных целях или военной деятельности в космическом пространстве. Проблема космического мусора имеет два измерения, поскольку она связана как с гражданской, так и с военной деятельностью в космическом пространстве. На данном этапе не следует поднимать вопрос о космическом мусоре в рамках Конференции по разоружению. То есть ограничения по рассмотрению этого вопроса связаны с форматом Конференции, а не с самим ДПРОК. Фактически, отсюда логически вытекает еще один важный вопрос, требующий обсуждения, — реформа нормативной базы ООН в области космоса. В долгосрочной перспективе следует постепенно объединять обсуждение вопросов гражданской и военной космической деятельности. Это не означает, что предназначенные для обсуждения этих вопросов площадки, такие

как КОПУОС и Конференция по разоружению, должны быть объединены. Однако обсуждение норм, регулирующих деятельность в космосе, должно включать все ее виды. Учитывая возможное двойное назначение многих видов деятельности в космическом пространстве, более разумно, а также полезно с точки зрения регулирования было бы разработать нормы двойного назначения, вместо того, чтобы искусственным образом разделять платформы на те, которые предназначены для обсуждения вопросов использования космического пространства в мирных целях, и те, которые служат для решения вопросов, связанных с его военным использованием.

Кроме того, проблемы космического мусора уже обсуждаются на самых различных площадках, таких как КОПУОС, МКП и Межучрежденческий координационный комитет по космическому мусору. Это не означает, что проблема космического мусора не может или не должна подниматься в рамках Конференции по разоружению. Это лишь означает, что отсутствие положений о космическом мусоре не может считаться существенным недостатком ДПРОК.

ОПРЕДЕЛЕНИЯ

Среди недостатков проекта его противники указывают также на отсутствие упоминаний оружия радиоэлектронного подавления, такого как лазеры, которое может быть использовано, чтобы временно или окончательно вывести из строя спутник[13].

С проблемой космического мусора тесно связан вопрос его активного удаления. Средства, разработанные для ликвидации космического мусора, технически могут быть использованы для нарушения функционирования чужих спутников. В связи с этим существует мнение, что «ДПРОК усугубит эту проблему, поскольку любое государство-участник, недовольное деятельностью другого государства участника по удалению космического мусора, сможет на законном основании потребовать ее прекращения, заявив, что используемые системы на самом деле являются *космическим оружием*... ДПРОК не учитывает такую возможность; это вызывает обеспокоенность и заставляет еще больше сомневаться в легитимности проекта договора»[14].

Авторы документа признают, что на данном этапе вряд ли возможно на международном уровне согласовать определение понятия *космическое оружие* и установить, какие виды оружия следует относить к этой категории, однако этот вопрос может рассматриваться как в рамках ДПРОК, так и отдельно от него. Не следует ставить участие в ДПРОК или его выполнение в зависимость от включения этого вопроса в договор.

С одной стороны, в большинстве случаев цели работы по активному удалению космического мусора отличаются от целей, с которыми применяется космическое оружие. Космическое оружие используется для нанесения ущерба, уничтожения, повреждения или нарушения нормального функционирования космического объекта[15]. Однако активное удаление космического мусора является одной из мер по снижению негативного воздействия космического мусора, и его целью является *расчистка* космического пространства, поскольку принято считать, что мер по предупреждению образования космического мусора недостаточно, чтобы в долгосрочной перспективе поддерживать чистоту космического пространства.

Таким образом, если государство уничтожает нефункционирующий космический объект, находящийся в его юрисдикции и под его контролем, такие действия не могут рассматриваться как размещение или использование оружия в космическом пространстве в том смысле, в котором это определение используется в ДПРОК.

Даже в случае злоупотреблений в ходе активного удаления космического мусора — например, если какое-либо государство уничтожит действующий космический объект другого государства без его согласия, пострадавшая сторона сможет потребовать от нарушителя объяснений, при условии что оба государства являются участниками ДПРОК[16]. В этом случае нарушителю предстоит доказать, что его деятельность по активному удалению космического мусора не является случаем применения космического оружия.

С другой стороны, проблемы, возникающие в связи с активным удалением космического мусора, должны решаться в рамках соответствующего международного механизма, а не договора о контроле над вооружениями в космосе. Настороженное отношение к деятельности других государств по активному удалению космического мусора или любой другой аналогичной деятельности всегда будет сохраняться, если эти государства воспринимаются как противники или соперники, вне зависимости от того, вступит ДПРОК в силу или нет. Любое государство сможет и без ДПРОК выразить свое несогласие с деятельностью другого государства по активному удалению космического мусора или с уничтожением космического объекта, находящегося в его юрисдикции и под его контролем, в соответствии с действующими нормами международного права.

Таким образом, вопрос не в том, следует ли рассматривать проблему активного удаления космического мусора в рамках ДПРОК, а в том, как создать международный механизм, который бы регулировал активное удаление космического мусора. На заседании Рабочей группы КОПУОС по долгосрочной устойчивости космической деятельности российская делегация представила проект руководства в области активного удаления космического мусора. В разделе *Соблюдение критериев для осуществления операций по активному удалению орбитальных объектов*[17] говорится: «Общее понимание должно состоять в том, что любые операции по активному удалению:

- исключают принудительное техническое воздействие на указанное выше имущество в космическом пространстве в отсутствие надлежащим образом подтвержденного согласия государства (включая государство регистрации), международной организации и/или юридического лица, интересы которых затронуты, и полномочий, предоставленных ими в ясно выраженной форме;
- не могут иметь своим результатом любое нарушение функций по осуществлению юрисдикции и/или контроля в отношении такого иностранного имущества»[18].

Постановка вопроса об активном удалении космического мусора или его обсуждение на базе других платформ, таких как КОПУОС и МККМ, будет способствовать рассмотрению или выполнению ДПРОК. Поэтому технологии двойного назначения не будут и не могут считаться препятствием, мешающим всеобъемлющему

одобрению ДПРОК, даже несмотря на сложности, связанные с поиском адекватного определения космического оружия.

Кроме того, следует отметить, что недостаточно четкая формулировка определений вряд ли вызвала бы столько критики, если бы ДПРОК не предлагался как юридически обязывающий документ. Возможно, Китаю и России следует пересмотреть свою позицию относительно юридической силы проекта договора. Возможно, следовало бы придать ему добровольный характер, тогда даже после утверждения документа его недостатки можно было бы свободно обсуждать как открытые вопросы. Иными словами, такие проблемы, как недостаточно четко сформулированные определения или споры относительно того, что включается в понятие *оружие*, не будут восприниматься как существенные недостатки, если речь идет о своде правил, имеющих рекомендательный характер, в то время как наличие их в тексте юридически обязывающего договора будет вызывать серьезные разногласия.

ЗАКЛЮЧЕНИЕ И КОММЕНТАРИИ

Переговоры по ДПРОК зашли в тупик не из-за несовершенства самого документа, а, скорее, из-за столкновения политических интересов.

Что касается дальнейших шагов в сфере контроля над вооружениями в космическом пространстве, следует сделать ставку на самодисциплину. В данном случае это означает, что каждое государство должно в односторонне порядке отказаться от размещения оружия в космическом пространстве. Речь не идет ни о компромиссе, ни об отказе от наилучшей стратегии. По сути, в долгосрочной перспективе наилучшая стратегия — это космическое разоружение, даже осуществляемое отдельными государствами в одностороннем порядке. Поэтому чрезвычайно важно провести анализ эффективности таких шагов в долгосрочной перспективе. Если мы не хотим, чтобы космическое пространство стало новой ареной противостояния, всем государствам следует отвлечься от разногласий и спросов насчет предотвращения гонки вооружений в космическом пространстве (тем более что в ближайшем будущем маловероятно, что удастся в них продвинуться) и сосредоточиться на односторонних заявлениях, жестах и действиях, которые подтверждали бы мирные намерения государств в космосе[19].

Едва ли ПСС и размещение оружия в космическом пространстве смогут обеспечить стратегическое сдерживание в космосе, хотя бы потому, что сложно представить себе космический *Перл-Харбор* без массированного ракетного нападения или мощного электромагнитного импульсного удара, а в этом случае потери для атакующей стороны будут самые серьезные. Более того, подготовку такого нападения и запуск ракет невозможно осуществить незаметно, развертывание займет несколько дней, а пусковые установки будут поставлены под угрозу уничтожения сразу после пуска первой ракеты[20]. В качестве контрмеры государства, которые могут стать объектом такого нападения, стали бы максимально повышать защищенность своих спутников и снижать зависимость от отдельных космических летательных аппаратов, чтобы минимизировать возможный ущерб[21]. Размещение космических систем обороны и наступления может обеспечить господство в космосе лишь на короткий срок, поэтому такая деятельность при отсутствии самодисци-

плины представляется недальновидной[22]. Таким образом, можно утверждать, что потенциал сдерживания противоспутниковых систем и другого оружия, размещаемого в космическом пространстве, явно преувеличен.

Международному сообществу необходимо принять превентивные меры и подписать новый международный юридический документ по ПРОК, чтобы не допустить гонки вооружений в космическом пространстве, задействовав при этом как юридически обязывающие механизмы, так и добровольные механизмы. Именно это должно стать общей целью международного сообщества.

Примечания

1 Данная работа отражает личное мнение автора, которое может не совпадать с точкой зрения правительства Китая.

2 Отчет Группы правительственных экспертов по мерам транспарентности и укрепления доверия в космической деятельности, A/68/189, 2013.07.19, параграф 6.

3 Г. Ван. Урегулирование кризиса в космическом пространстве: Совместный подход для Европы и Китая, Отчет о научно-исследовательской работе Академии Института Chatham House, готовится к публикации.

4 Текст доступен по ссылке: http://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/t1165762.shtml.

5 Г. Ирстен. Процесс консультаций по разработке международного кодекса поведения для космической деятельности завершен (Gabriella Irsten, The consultation process for the International Code of Conduct for Outer Space Activities ends), ссылка: http://us3.campaign-archive1.com/?u=c9787c74933a00a9066ba32d5&id=30168cfe11&e=c416a13f52 (на английском языке).

6 М. Листнер, Р. Раджагопалан. ДПРОК-2014: новый проект со старыми и новыми проблемами (Michael Listner and Rajeswari Pillai Rajagopalan, The 2014 the PPWT: a new draft but with the same and different problems), ссылка: http://www.thespacereview.com/article/2575/1 (на английском языке).

7 С 1958 по 2005 гг. США провели 33 испытания противоспутниковых средств, а Россия — 20. См. К. Клейтон, С. Чунь. Защищая космос: Противоспутниковое оружие США и космические вооружения, (Clayton K S Chun, Defending Space: US Anti-Satellite Warfare and Space Weaponry), изд-во «Osprey Publishing», 2006 год, стр. 53–54.

8 М. Шихан. Международная политика в космической сфере (Michael Sheehan, The International Politics of Space), изд-во «Routledge», 2007 г., стр. 120.

9 Р. Деллиос. Космическая программа Китая: стратегический и политический анализ (Rosita Dellios, China's space programme: a strategic and political analysis), издание Culture Mandala, часть 7, № 1 (декабрь 2005 г.), стр. 6.

10 М. Шихан. Международная политика в космической сфере (Michael Sheehan, The International Politics of Space), изд-во Routledge, 2007 г., стр. 165.

11 См. М. Шихан. Международная политика в космической сфере (Michael Sheehan, The International Politics of Space), изд-во Routledge, 2007 г., стр. 164–165.

12 См. Дж. Рагги. Международный ответ технологиям: концепции и тенденции (John Gerard Ruggie, International Responses to Technology: Concepts and Trends), издание International Organization, том 29, № 3, 1975 г., стр. 559–60. Цитируется по публикации Дж. Молтца *Политика космической безопасности* (James Clay Moltz, The Politics of Space Security),, изд-во Stanford University Press, 2011 г., стр. 328.

13 М. Листнер, Р. Раджагопалан. ДПРОК-2014: новый проект со старыми и новыми проблемами (Michael Listner and Rajeswari Pillai Rajagopalan, The 2014 the PPWT: a new draft but with the same and different problems), http://www.thespacereview.com/article/2575/1 (на английском языке).

14 Там же.

15 Согласно пункту (b) Статьи I ДПРОК (вариант 2014 г.), под *космическим оружием* понимается «любой объект в космическом пространстве или его часть, которые были созданы или переоборудованы для уничтожения, повреждения или нарушения нормального функционирования объектов в космическом пространстве, а также на поверхности Земли или в ее воздушном пространстве».

16 Согласно Статье VII ДПРОК, PPWT (вариант 2014 г.), «Любое государство-участник, которое имеет основание полагать, что другое государство-участник не исполняет свои обязательства в соответствии с настоящим Договором, может потребовать у этого государства-участника объяснений по этому вопросу».

17 A/AC.105/C.1/2014/CRP.17, стр. 6.

18 Там же, стр. 7.

19 См. Я. Робинсон. Роль мер по обеспечению транспарентности и укреплению доверия в повышении космической безопасности, доклад Европейского института космической политики, Вена, 2010 г., 9, стр 54.

20 Там же, стр. 340.

21 Дж. Молтц. Политика космической безопасности (James Clay Moltz, The Politics of Space Security), изд-во Stanford University Press, 2011 г., стр. 339.

22 Там же.

15 Согласно пункту (b) Статьи I ДПРОК (вариант 2014 г.), под *космическим оружием* понимается «любой объект в космическом пространстве или его часть, которые были созданы или переоборудованы для уничтожения, повреждения или нарушения нормального функционирования объектов в космическом пространстве, а также на поверхности Земли или в ее воздушном пространстве».

16 Согласно Статье VII ДПРОК, PPWT (вариант 2014 г.), «Любое государство-участник, которое имеет основание полагать, что другое государство-участник не исполняет свои обязательства в соответствии с настоящим Договором, может потребовать у этого государства-участника объяснений по этому вопросу».

17 A/AC.105/C.1/2014/CRP.17, стр. 6.

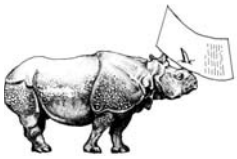
18 Там же, стр. 7.

19 См. Я. Робинсон. Роль мер по обеспечению транспарентности и укреплению доверия в повышении космической безопасности, доклад Европейского института космической политики, Вена, 2010 г., 9, стр 54.

20 Там же, стр. 340.

21 Дж. Молтц. Политика космической безопасности (James Clay Moltz, The Politics of Space Security), изд-во Stanford University Press, 2011 г., стр. 339.

22 Там же.



Михаил Мостовюк

ИСТОЧНИКИ ФИНАНСИРОВАНИЯ ТЕРРОРИСТИЧЕСКОЙ ОРГАНИЗАЦИИ *ИСЛАМСКОЕ ГОСУДАРСТВО*

В свете событий последних недель внимание мировой общественности и средств массовой информации приковано к военной операции, развернутой воздушно-космическими силами России и коалицией, ведомой США, против террористической организации *Исламское государство* (ИГ). Вступление в активные боевые действия российской авиации и террористические акты, совершенные в отношении российского авиалайнера в небе над Синаем, взрывы и захват заложников во Франции и Тунисе, ответственность за которые взяло на себя ИГ, придали серьезный импульс военной операции, начатой еще в августе 2014 г.

Исламское государство — особенная террористическая организация. Заявляя о себе как о *государстве* ислама, она стремится к расширению подконтрольной ей территории, занимается обустройством инфраструктуры, обеспечивает широкое администрирование захваченных объектов и населенных пунктов. На сегодняшний день ИГ — самая богатая террористическая организация мира. Ее доходы выросли с 1 млн долл. США в день в конце 2008 г. до 3 млн долл. США в день в 2014 г.

Как любая крупная организация, *Исламское государство* планирует и принимает годовой бюджет, к подготовке которого привлекаются специалисты высокого уровня. Часть из них составляют иракцы, работавшие в этой сфере раньше, часть — добровольцы со всего мира, имеющие соответствующий опыт и знания.

Боевики-исламисты составляют наемную армию, численность которой оценивается в 30 тыс. человек. Рядовой *воин ислама* получает в месяц около 400 долл. США не считая премиальных за успешное выполнение военных операций. Таким образом, сумма ежемесячного вознаграждения боевика больше, чем правительство Ирака может предложить большинству своих служащих[1]. В масштабах всей террористической организации ежемесячные затраты на содержание *вооруженных сил* оцениваются в 12 млн долл. США.

По сведениям европейских аналитиков (на октябрь 2015 г.), ежегодный доход *Исламского государства* составляет порядка 2,5 млрд долл. США, что сопоставимо с бюджетом небольшой европейской страны[2]. Это говорит о том, что в экономическом смысле организация вполне самодостаточна, а наличие у нее подконтрольной территории позволяет ставить эксперименты по созданию квазигосударства со многими традиционно присущими государству атрибутами. Наличие существенных доходов позволяет выплачивать вознаграждение воюющим на стороне ИГ боевикам и компенсации семьям убитых в боях, нести расходы, связанные с управлением подконтрольными территориями и захваченными объектами инфраструктуры, а также вести пропагандистскую деятельность.

Военные удары, наносимые российской авиацией и коалицией во главе с США по захваченным террористами территориям, имеют вполне определенную цель — ликвидировать инфраструктуру террористической организации и, следовательно, снизить ее финансовые возможности. Сокращение источников финансирования снижает потенциал *Исламского государства* по целому ряду направлений деятельности: пополнению числа боевиков, продолжению территориальной экспансии, расширению пропаганды.

Анализу источников финансовых средств террористической организации в последние два года уделялось достаточно внимания. Соответствующие документы готовились и в рамках деятельности Совета безопасности ООН[3], и в рамках ФАТФ, опубликовавшей тематический отчет[4], в котором детально классифицированы источники доходов *Исламского государства*.

Согласно сведениям ФАТФ, финансовые источники можно разделить на следующие группы:

- прибыль, получаемая от оккупации территории: грабеж населения, контроль банков, нефтяных месторождений и нефтеперерабатывающих заводов, хищение экономических активов, налогообложение товаров и наличных средств, провозимых транзитом через подконтрольную ИГ территорию;
- похищение людей с целью выкупа;
- пожертвования;
- привлечение денежных средств с использованием информационно-коммуникационных технологий, в том числе социальных сетей;
- использование доходов или имущества вступающих в *Исламское государство* боевиков.

В совокупности перечисленные источники террористической сети позволяют ей получать регулярную прибыль, несмотря на то что их приоритетность различна и зависит от оперативной обстановки и возникновения новых факторов.

Первая группа доходов связана с контролем захваченных территорий. Она наиболее важна для *Исламского государства* в силу широкого охвата осуществляемой деятельности и уровня получаемых доходов.

Можно выделить несколько направлений данной деятельности:

а) **Доходы от переработки и продажи углеводородов — нефти и нефтепродуктов, а также природного газа.** Это крупнейшая статья доходов *Исламского государства*. Осознавая стабильность данного источника прибыли, боевики стремятся к сохранению и повышению эффективности использования существующей инфраструктуры нефтеперерабатывающей и газодобывающей сферы. Добыча нефти и ее переработка позволяет боевикам обеспечивать как собственные потребности в топливе, так и отправлять ее для продажи или обмена на местных или региональных рынках, в том числе в страны, с которыми они воюют. Тяжелая битумная нефть продается в среднем по 26–35 долл. США за баррель (в отдельных случаях цена может опускаться до 10 долл.) местным торговцам, через границу в Ирак или нефтеперерабатывающим заводам, финансируемым турецкими, ливанскими и иракскими бизнесменами. Посредники могут перепродавать приобретенную у боевиков нефть по цене в два и более раз выше.

Основной объем нефти *Исламское государство* добывает на подконтрольных сирийских территориях (контролируется 60% добычи нефти в Сирии и семь крупных месторождений в Ираке), где в среднем за сутки получают до 40 тыс. баррелей.

По сведениям турецких дипломатических источников, количество конфискованной нефти вдоль турецко-сирийской границы выросло в четыре раза по сравнению с 2011 г.[5]

Осенью 2015 г. была распространена информация о том, что большую часть нефти ИГ вывозит через территорию Иракского Курдистана и Турции. При этом коалиция, ведомая США, располагала возможностями для борьбы с нефтяной контрабандой ИГ, но не предприняла для этого достаточных усилий[6].

Авиаудары российских воздушно-космических сил и действия международной антитеррористической коалиции во главе с США в значительной степени направлены на разрушение добывающей и перерабатывающей инфраструктуры нефтепромысла и создают глобальные предпосылки для существенного сокращения этого источника дохода террористов. Их результатами уже сейчас стало снижение прибыли от незаконного экспорта нефти и нефтепродуктов в Турцию, Иорданию и Курдский автономный район Ирака[7].

Как отмечается в докладе ФАТФ, авиаудары коалиции, ведомой США (на момент подготовки доклада российская операция еще не началась), вынуждают *Исламское государство* обращаться к примитивным технологиям нефтепереработки, например сжиганию нефти в карьерах, что приво-

дит к значительному снижению объемов поставок нефтепродуктов и существенно ухудшает их качество. Несмотря на это, данный источник доходов является основным для террористической организации. Он приносит исламистам более 1 млрд долл. США в год, из которых порядка 600 млн приходится на продажу нефти, а 350 млн — на продажу газа.

б) **Продажа антикварных ценностей и памятников старины.**

На оккупированных боевиками *Исламского государства* территориях находится свыше 4,5 тыс. археологических памятников, многие из которых являются объектами всемирного наследия ЮНЕСКО. Подавляющее их большинство расположено в разрушенных войной регионах, что способствует их хищению в крупных размерах. Генеральный директор ЮНЕСКО И. Бокова заявила о *промышленных масштабах* нелегальных раскопок[8].

Главари ИГ наладили два основных способа получения прибыли от продажи памятников культуры — их прямую продажу и взимание сборов с контрабандистов, провозящих артефакты через контролируемую боевиками территорию. Отсутствие доступа к захваченным объектам не позволяет в полной мере оценить масштабы ущерба и доходы от этого вида преступного промысла. Однако косвенные оценки, в первую очередь отчетность правоохранительных органов, позволяют говорить о том, что средняя стоимость вывозимых предметов составляет от нескольких сотен до нескольких десятков тысяч долларов США, в особых случаях — до нескольких миллионов долларов США. Данная сфера деятельности приносит террористической организации порядка 100–200 млн долл. США в год.

в) **незаконное налогообложение местного населения** (как минимум восьми миллионов человек), ведущееся под видом оказания формальных услуг или *государственной* защиты. Занимаясь различными формами вымогательства и грабежей в виде сбора *налогов* на личный транспорт, на проезд в общественном транспорте, на посещение школьных занятий, террористы получают до 400 млн долл. США в год.

г) **контроль банков и банковской деятельности** на оккупированной террористам территории Ирака и Сирии.

Все наличные средства, хранящиеся в государственных банках, находятся под полным контролем *Исламского государства*. Только при ограблении в июне 2014 г. нескольких банков в иракском Мосуле были похищены средства на сумму 430 млн долл. США[9].

Что касается частных банков, то их клиенты имеют право снимать наличные деньги со своих счетов при условии уплаты налога в пользу исламистов в размере 5% от суммы снятия.

В целом, данный источник деятельности приносит террористической сети до 1,6 млрд долл. США.[10]

д) **торговля людьми**. Преимущественно представляет собой сделки по продаже девушек *для брака* или сексуального рабства. На каждую рабы-

ню установлена определенная цена, которая зависит от возраста девушки и ряда других факторов. В прейскурантах проводимых аукционов самыми высокими являются цены на детей в возрасте от одного года до девяти лет — порядка 165 долл. США. Дети постарше, включая подростков в возрасте до 20 лет, *продаются* на специализированных рынках по цене, эквивалентной 125 долл. США. Рабыни в преклонном возрасте обходятся в 40 долл. США. В ряде случаев женщины, попавшие в рабство, могут быть выкуплены родственниками. Различные источники определяют сумму выкупа примерно в 3 тыс. долларов США за человека.

е) **доходы, получаемые от аграрного сектора**, разнообразны по своим видам. Присутствует традиционный рэкет, замаскированный под пожертвования денежных средств или части возделываемого урожая в пользу ИГ, причем плата зависит от размера земельного надела, а не от урожая. Процветает конфискация сельскохозяйственной техники и полей, сдаваемых в дальнейшем в аренду самим же фермерам. Захваченная сельскохозяйственная техника активно продается в Сирию, где у местных властей зачастую нет других поставщиков.

Контроль над складированием зерна в зернохранилища и его распределением позволяет боевикам определять цены на зерновые в прилегающих регионах. Непосредственный захват зернохранилищ и контроль над их последующим функционированием позволяют боевикам выгодно легально продавать зерно, а условия его хранения не позволяют определить фермеров, которым оно первоначально принадлежало. Кроме того, у исламистов есть договоры на скупку урожая у сельскохозяйственных предприятий, что гарантирует сохранение их статуса главного поставщика продовольствия на контролируемой территории, не зависящего от внешних поставок.

По данным тематического доклада, представленного в апреле 2015 г. Конгрессу США, продажа урожая на черном рынке по цене в два раза ниже среднерыночной ежегодно приносит боевикам более 200 млн долл. США.[11] Продовольственная и сельскохозяйственная организация (ФАО) ООН объясняет, что высокий уровень доходов в этой сфере обусловлен тем, что ИГ контролирует часть Ирака, на которую приходится более 40% всех иракских земель, выделенных под культивацию пшеницы.

ж) **доходы от добычи природных ресурсов** связаны с использованием расположенных на захваченных боевиками территориях рудников и промышленных предприятий по переработке ресурсов. Под контролем *Исламского государства* находятся фосфатный и соляной рудники, завод по переработке фосфатов в серную и фосфорную кислоту, пять крупных цементных заводов, несколько заводов по производству серы. Только продажи фосфатов позволяет ИГ пополнять свои доходы минимум на 50 млн долл. США в год. Поставки серной и фосфорной кислот могут ежегодно приносить порядка 300 млн долл. США.

з) **доходы от налогообложения товаров, провозимых транзитом** через подконтрольную боевикам территорию. Несмотря на существенное падение торгового оборота на территориях, оккупированных террористической организацией, отдельные виды товаров все же продолжают поступать в оборот. ИГ облагает налогами все товары, проходящие транзитом через его территорию. Дорожный налог в размере 200 долл. США введен в северном Ираке, а таможенный налог в размере 800 долл. США взимается с грузовиков, въезжающих в Ирак через границу с Сирией и Иорданией.

и) **доходы от отъема заработной платы государственных служащих Ирака**. Несмотря на прекращение прямых выплат иракским госслужащим, работающим на контролируемых *Исламским государством* территориях, а также действующий запрет на безналичный перевод средств для этих целей, госслужащие получают свою зарплату в финансовых организациях в неподконтрольных боевикам провинциях. Однако при возвращении в регион проживания они выплачивают боевикам налог, составляющий до 50% от полученной суммы. По данным ФАТФ со ссылкой на американские источники, размер выплат госслужащим составляет несколько миллиардов долларов США, следовательно, ежегодный получаемый доход ИГ можно оценить в сотни миллионов долларов.

Второй группой доходов *Исламского государства*, не связанной напрямую с контролем захваченных территорий, является похищение людей с целью выкупа. Количество похищенных ИГ людей исчисляется сотнями. Часть из них похищается целенаправленно для выкупа, часть — с целью устрашения, например для массовых казней, видеозаписи которых с лета 2014 г. широко распространены в интернете. В ряде случаев боевики *Исламского государства* перекупают заложников у умеренных мятежников. По данным ФАТФ, приблизительная ежегодная доходность подобного промысла составляет от 20 до 45 млн долл. США. Точнее оценить прибыль боевиков невозможно, поскольку большинство сделок в этой сфере не афишируются или проводятся через посредников, которые не заинтересованы в разглашении своих имен.

Третьей группой доходов являются пожертвования в пользу *Исламского государства* от физических лиц или при посредничестве некоммерческих организаций. Сопоставление этого источника дохода с другими, например с выручкой от продажи нефти, показывает, что внешние пожертвования не имеют существенного веса в структуре прибыли, получаемой террористической организацией. Вместе с тем, на фоне перманентных рисков снижения иных поступлений данный вид прибыли остается достаточно стабильным. К числу стран, граждане которых спонсируют *Исламское государство*, традиционно относят его соседей, страны, находящиеся в непосредственной близости от захваченных ИГ территорий, — Саудовскую Аравию, Кувейт, Катар, Ливию, Турцию, а также Пакистан и Афганистан, где группировка пользуется общественной поддержкой.

Согласно оценкам, представленным в упомянутом выше докладе *Islamic State Financing and U. S. Policy Approach*, в период 2013–2014 гг. *Исламское государство* получило около 40 млн долл. США от доноров из Саудовской Аравии, Катара, Кувейта и ОАЭ. Нагнетая и дестабилизируя обстановку в регионе, каждая из этих стран борется за лидерство на Востоке.

На сегодняшний день отмечается некоторое снижение количества пожертвований из стран Персидского залива, поскольку их правительства начали воспринимать присутствие террористической организации на прилегающей территории как угрозу своей территориальной безопасности. Заявления о наличии у ИГ государственного финансирования звучат и на высшем уровне. В ходе саммита *Группы 20* в Анталье в ноябре 2015 г. президент России В. Путин отметил, что финансирование *Исламского государства* осуществляется из 40 стран, в том числе и из стран *двадцатки*. Только российскими спецслужбами зафиксированы финансовые операции в поддержку ИГ на сумму 300 млн руб. [12]

Четвертой группой доходов *Исламского государства* является привлечение денежных средств с использованием информационно-коммуникационных технологий, в том числе социальных сетей. ИГ активно использует современные информационные технологии как для информирования о своей деятельности, так и для привлечения финансовых средств. Открыт медиацентр *Al-Itisam Establishment for Media Production*, который активно распространяет пропаганду *Исламского государства* через социальные сети, в том числе ведя аккаунты группировки в социальных сетях. С помощью этих аккаунтов организуются пиар-кампании, использующие технологии вовлечения широких масс пользователей соцсетей, например *Twitter-шторм*. Такая деятельность позволяет террористической организации не только оперативно информировать мир о своих *успехах*, но и конвертировать потенциальную поддержку радикально настроенных лиц в фактические финансовые активы.

Одним из широко используемых инструментов сбора средств в интересах ИГ является краудфандинг (массовый сбор добровольных пожертвований через интернет), сопровождаемый полноценными маркетинговыми кампаниями. Задокументированы случаи, когда через социальные сети производился прямой сбор средств на поддержку боевиков-террористов, при этом доноры могли незамедлительно получить ответ о расходовании внесенных средств в виде фотографий боевиков с приобретенным оружием, снаряжением и амуницией.

К более завуалированным инструментам сбора средств относятся интернет-магазины, где можно приобрести товары с высокой наценкой, переводимой в дальнейшем в криптовалюту и направляемую на поддержку боевиков, или тематические форумы по вопросам ислама, где доступ к разделам, посвященным сбору денежных средств для ИГ, доступен лишь после регистрации пользователя или получения специального кода доступа. Содержимое этих разделов не индексируется поисковыми системами.

Вопросам использования боевиками информационно-коммуникационных технологий, в том числе механизмов краудфандинга, посвящен утвержденный в октябре 2015 г. отчет ФАТФ о новых *нетрадиционных* источниках финансирования ИГ[13].

Распространение вышеупомянутых схем позволяет радикально настроенным гражданам, ранее не имевшим возможности оказать пособническую помощь террористическим организациям и не связанным с ними, направлять денежные средства террористам. Кроме того, в силу дифференцированности и отсутствия отличительных признаков таких финансовых транзакций их анализ представляет сложность даже для спецслужб.

Пятой группой доходов *Исламского государства* является использование доходов или имущества вступающих в организацию боевиков. Удельный вес этого источника доходов сравнительно невелик, поскольку пополняющие организацию боевики представляют большую ценность именно в качестве людского ресурса. Вместе с тем, средства, привозимые ими с собой, также идут на финансирование ИГ.

Средства эти могут принадлежать лично боевику или быть собраны диаспорами или радикально настроенными знакомыми. Это могут быть как легальные доходы, так и доходы от различного рода преступной деятельности. Российские и европейские аналитики отмечают, что будущие *воины ислама* перед поездкой стараются продать свое недвижимое имущество, получить заведомо невозвратные потребительские кредиты на небольшие суммы, открыть банковские счета для использования лимита овердрафта при снятии наличных, осуществить мошеннические действия с различными видами социальных пособий[14].

По сведениям ФАТФ, к началу 2015 г. по крайней мере 19 тыс. боевиков из более 90 стран уехали в Сирию и Ирак, чтобы присоединиться к ИГ. Большинство из них вывезли денежные суммы от нескольких сотен до нескольких тысяч долларов США.

Вопрос сохранения стабильных источников финансирования для *Исламского государства* является ключевым. Вследствие роста координации действий мирового сообщества против ИГ боевики вынуждены изыскивать новые источники доходов или адаптировать старые к новым условиям. Так, например, фиксируются факты нелегальной торговли человеческими органами и тканями, контрабанды хлопка, отмечены случаи массовой конфискации денежных средств у населения. Для обеспечения стабильности финансирования террористической организации ее лидеры сформировали резервный фонд в размере 2,3 млрд долл. США.

Россия продолжает усиливать противодействие финансированию *Исламского государства* как на международных площадках, так и в двустороннем формате.

В феврале 2015 г. по инициативе России Совет Безопасности ООН принял резолюцию 2199, нацеленную на пресечение финансовых доходов терро-

ристов, действующих в Сирии, Ираке и других странах Ближнего Востока[15]. В документе закрепляется запрет на любую торговлю нефтью и нефтепродуктами с *Исламским государством* и *Джабхат ан-Нусрой,* такие действия квалифицируются как оказание финансовой поддержки террористам, что является основанием для введения против физических и юридических лиц, вовлеченных в эту преступную активность, адресных санкций по линии Совета Безопасности ООН.

Вместе с тем, по мнению российской стороны, выполнение указанной резолюции осуществляется рядом государств недостаточно эффективно. Предложения о создании мониторингового механизма выполнения резолюции 2199 неоднократно блокировались в Совете Безопасности ООН *западниками*. Этим обусловлена новая инициатива России в виде проекта резолюции, распространенной среди постоянных членов Совета Безопасности ООН, требующей от государств принятия конкретных мер, направленных на достижение задач, определенных в резолюции 2199, а также включающей положение о координации усилий по поимке виновных в терактах с властями Сирии.

Успешные шаги по сокращению постоянных источников доходов *Исламского государства* в значительной степени обусловлены сочетанием скоординированных военных действий, в том числе авиаударов по захваченным боевиками территориям и объектам, и общих усилий участников мирового сообщества по созданию инструментария, позволяющего выявлять и пресекать каналы легализации преступно полученных финансовых средств, обеспечивающих регулярную подпитку террористического движения.

Примечания

1 https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-its-money/

2 http://www.lefigaro.fr/economie/le-scan-eco/dessous-chiffres/2015/11/19/29006-20151119ARTFIG00006-petrole-taxes-donations-trafics-d-humains-comment-daech-se-finance.php

3 Доклад Мониторинговой группы Комитетов Совета Безопасности ООН 1267/1989. http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2014_815.pdf

4 Финансирование террористической организации Исламское государство Ирака и Леванта. Отчет ФАТФ. *Финансовая безопасность*, 2015 г., № 8.

5 ИГ наполняет казну за счет преступной экономики в Сирии и Ираке. The Wall Street Journal. http://www.inopressa.ru/article/28aug2014/wsj/isis.html

6 10 фактов о финансировании ИГ. http://www.vestifinance.ru/articles/63842/print

7 Брифинг Минобороны России: «ВС РФ в борьбе с международным терроризмом. Новые данные». http://function.mil.ru/for_media/press_conferences/detail.htm?id=12070767@morfPressConferenceNew

8 Места археологических раскопок в Сирии подверглись разграблению. http://www.interfax.ru/world/467082

9 Mosul Seized: Jihadis Loot $429m from City's Central Bank to Make Isis World's Richest Terror Force. http://www.ibtimes.co.uk/mosul-seized-jihadis-loot-429m-citys-central-bank-make-isis-worlds-richest-terror-force-1452190

10 http://www.theguardian.com/world/2014/jun/15/iraq-isis-arrest-jihadists-wealth-power

11 Islamic State Financing and U.S. Policy Approach. https://www.fas.org/sgp/crs/terror/R43980.pdf

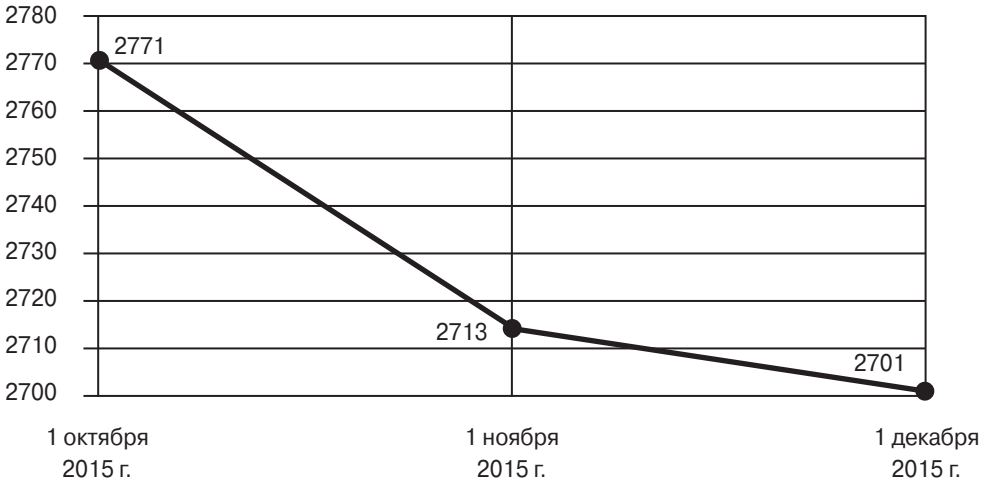
12 Росфинмониторинг: 3,5 тыс. россиян направляли деньги террористам. http://izvestia.ru/news/596157#ixzz3sLqyx7Aw

13 http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

14 Росфинмониторинг: 3,5 тыс. россиян направляли деньги террористам. http://izvestia.ru/news/596157#ixzz3sLqyx7Aw

15 http://www.cbr.ru/today/anti_legalisation/un/2199.pdf

График 1. **Индекс международной безопасности *iSi* в октябре-декабре 2015 г.**



Осенью — в начале зимы 2015 г. Индекс международной безопасности падал, поскольку росли мировые угрозы. На 1 ноября показатель Индекса *iSi* составил **2713** пунктов, что на 58 единиц ниже значения на 1 октября. Резкое снижение показателя связано с дальнейшей эскалацией ситуации в Сирии, терактом на российском пассажирском авиалайнере над Синайским полуостровом и ростом напряженности на севере Афганистана. 1 декабря показатель *iSi* упал еще на 12 пунктов и составил **2701.** Причина тому — теракты в Париже, Мали, Ливане, Нигерии, Ираке, а также резкое обострение отношений Москвы и Анкары из-за российского военного самолета, сбитого турецкими ВВС.

БЛИЖНИЙ ВОСТОК И АФРИКА

Ситуация на Ближнем Востоке и Африке остается главной угрозой региональной и международной безопасности. Борьба против террористической группировки ИГ в регионе пока не дала эффективных результатов.

Война в **Сирии** и вступление в конфликт России на стороне Б. Асада — главный фактор, влиявший на показатели Индекса iSi. Российская авиация за два месяца операции нанесла около 17 авиаударов по сирийским городам Сальма, Гмам, Кесладшук и Бахса, где, по мнению Кремля, располагались повстанческие отряды исламистов. 7 октября российские корабли Каспийской флотилии провели 26 пусков крылатых ракет по целям в Сирии. 9 октября боевики ИГ начали наступление на второй по величине сирийский город Алеппо. В контрнаступлении на Алеппо сирийские правительственные войска поддерживались российской авиацией, иранскими подразделениями и группировкой *Хезболла*. 21 октября президент Б. Асад встретился в Москве с В. Путиным и заручился его поддержкой. США, Евросоюз и их союзники в странах Персидского Залива обвинили Россию в бомбардировке объектов сирийской умеренной оппозиции и гражданского населения. Турция обвинила Россию в нарушении своего воздушного пространства. Военные ведомства Москвы и Вашингтона в октябре провели несколько видеоконференций и обсудили безопасность полетов авиации двух стран в ходе сирийской операции.

Созданная в сентябре 2014 г. коалиция во главе с США продолжила авиаудары по позициям ИГ в Сирии и **Ираке**. 16 октября курды отбили у ИГ город Синджар на северо-западе Ирака. В результате военно-воздушных ударов России и коалиции под руководством США удалось сдержать продвижение ИГ, но полной победы одержать не удалось. Предложение России создать единую коалицию по борьбе с терроризмом на Ближнем Востоке и Северной Африке под эгидой ООН пока не нашло поддержки на Западе.

23 октября в Вене прошла встреча глав МИД России, США, Саудовской Аравии и Турции по ситуации в Сирии. Стороны обсудили возможность присоединения к переговорному процессу Египта, стран Персидского Залива, Лиги арабских государств, Организации исламского сотрудничества и Ирана. 30 октября переговоры в Вене продолжились в оговоренном ранее расширенном составе. Результатом стал план из девяти пунктов, предусматривающий формирование переходного

Андрей Кортунов, генеральный директор Российского совета по международным делам — по телефону из Москвы:

Восстановление многостороннего политического диалога по сирийскому урегулированию — одно из немногих событий осени, которое внушает оптимизм. Важно, что мировое сообщество осознает необходимость дипломатическими методами решать украинский кризис, о чем свидетельствует запущенный новый раунд минских консультаций. Не исключено, что в ходе очередных консультаций по Украине удастся сблизить позиции сторон или даже привести их к общему знаменателю.

Позитивный сценарий развития международных отношений в 2016 г. реализуется, если великие державы и ключевые страны Ближнего Востока смогут поставить общие интересы выше частных разногласий и конъюнктурных соображений руководства отдельных стран. Такой сценарий позволит не только урегулировать сирийский конфликт, но, не исключено, начать работу по созданию новой системы безопасности для всего Ближнего Востока. Конструктивный сдвиг ближневосточной ситуации и преломление здесь опасных тенденций позитивно повлияет на урегулирование кризиса на Украине, в Восточной Азии, Северной Африке.

В 2016 г. внимание американцев будет приковано к начавшейся президентской избирательной кампании и внутренним проблемам, поэтому ожидать серьезных позитивных прорывов не следует. Достижением станет хотя бы восстановление привычного формата российско-американского диалога по стратегическим региональным и глобальным проблемам. Восстановление контактов и линий коммуникаций, в значительной степени замороженных в 2015 г., создаст основу для работы со следующей Администрацией США, которая придет к власти в начале 2017 г.

Константин фон Эггерт (Россия), член Королевского института международных отношений, журналист — по телефону из Москвы:

Уровень безопасности в мире ухудшился. Причины тому — возросший градус конфронтации вокруг Сирии между Россией и союзниками по НАТО, очередная волна дестабилизации на востоке Украины, теракты в Париже, дестабилизация европейского континента из-за серьезной угрозы радикального ислама и временной неспособности абсорбировать поток мигрантов с Ближнего Востока.

Продолжающийся российско-украинский конфликт — главный негативный фактор на постсоветском пространстве. Выполнение минских соглашений желательно, но максимум, на что стоит рассчитывать, — это на продление срока его реализации.

Вовлечение России в сирийский конфликт влияет на пространство СНГ. В Кремле рассчитывают, что немногочисленные союзники в постсоветских странах увидят серьезность намерений Москвы и осознают, что с ней стоит дружить. Демонстрируется, что друзья России, как Б. Асад, получают от нее военную и политическую помощь. Но страны СНГ воспринимают ситуацию иначе. Для России применение вооруженной силы — не экстраординарное событие, а нечто в порядке вещей — считают они. В постсоветских странах это будет иметь далеко не позитивный отклик.

Длительность российской военной операции в Сирии будет зависеть от ее внутриполитического эффекта на российское общество. Уничтожение гражданского самолета над Синаем, история со сбитым Турцией российским военным самолетом Су-24 очевидно связаны с участием Москвы в сирийском конфликте и являются факторами неконтролируемой эскалации конфликта. Как российское общество будет воспринимать эскалацию, если жертвы среди военнослужащих страны станут заметными, сложно прогнозировать. Но для среднего россиянина конфликт на Украине — это одно, а конфликт в Сирии, которая далеко, — другое. Полагаю, в Кремле будут рассматривать сирийскую ситуацию с точки зрения внутренней политики. Если конфликт не будет грозить массовыми жертвами среди российских солдат, то Россия предпочтет остаться в Сирии до 2017 г., чтобы было как минимум о чем говорить с новой Администрацией США.

Проблему ИГ не удастся решить без крупномасштабной сухопутной операции в Сирии. Поскольку найдется не много желающих поучаствовать в ней, то на Ближнем Востоке, в частности в Сирии, обстановка продолжит ухудшаться.

Вынужденное взаимодействие между Россией и США по Сирии сохранится в новом году, но улучшения двусторонних отношений не произойдет. Отсутствие доверия между Москвой и Вашингтоном достигло такого уровня, что сложно представить позитивные подвижки.

2016 — последний год Администрации Б. Обамы. Все, кто хотел ослабить американское влияние и добиться каких-то преимуществ, активизируют свои усилия, пока у власти в США слабая и неуверенная Администрация.

Единственным позитивом в новом году может стать движение к трансатлантической торговле.

правительства и проведение всеобщих выборов с последующей конституционной реформой.

16 ноября состоялся второй раунд венских переговоров по сирийскому урегулированию в расширенном составе. Стороны приблизились к согласию относительно того, какие оппозиционные группировки в Сирии можно считать умеренными. В основе *дорожной карты* будущего сирийского урегулирования лежит договоренность между властями и оппозицией Сирии начать переговоры ориентировочно 1 января 2016 г., установить режим прекращения огня и начать формировать переходное правительство. Не удалось договориться о судьбе Б. Асада в будущем обустройстве страны. Вашингтон требует его отставки, Россия настаивает на праве сирийцев самостоятельно определять власть.

31 октября над **Синайским полуостровом** потерпел крушение российский пассажирский самолет А321–231 компании *Когалымавиа*, выполнявший рейс по маршруту Шарм-эш-Шейх — Санкт-Петербург. Находившиеся на борту 220 человек погибли. Боевики ИГ взяли на себя ответственность за крушение самолета. 17 ноября российские власти признали теракт. Граждане России и некоторых европейских стран были эвакуированы с курортов Египта.

20 ноября в **Мали** боевики лояльной *Аль-Каиде* исламистской группировки *Аль-Мурабитун* напали на отель и взяли в заложники 170 человек. В результате штурма здания отеля малийскими силовиками большинство заложников удалось освободить. Жертвами теракта стали 19 человек.

Теракты были совершены также в Ливане, Нигерии, Ираке, Турции.

25 ноября турецкие ВВС сбили российский бомбардировщик Су-24 на границе с Сирией, обосновав это нарушением воздушного пространства страны. Россия в ответ ввела экономические санкции против Турции. Отношения двух стран резко обострились.

В **Турции** после неудавшейся попытки сформировать правящую коалицию после июньских выборов, где *Партия справедливости и развития* потеряла парламентское большинство, 1 ноября состоялись внеочередные парламентские выборы. Партия Т. Р. Эрдогана вернула себе большинство в парламенте.

15 ноября в Турции прошел саммит *Группы 20*, где помимо вопросов экономического развития лидеры стран-участниц большое внимание уделили борьбе с международным терроризмом.

В **Йемен** 17 ноября вернулся из изгнания в Саудовскую Аравию президент М. Хади. 2 декабря боевики *Аль-Каиды* захватили два города на юге Йемена — Джаар и Зинджибар. Осенью МИД Йемена подтвердил наземное вторжение войск Саудовской Аравии и ОАЭ. Блокада моря и военные действия привели к гуманитарному кризису — в стране не хватает еды, медикаментов, товаров первой необходимости.

В октябре — ноябре резко ухудшились отношения **Израиля** и **Палестины** в связи с чередой нападений на израильтян в районах Западного берега и Восточного Иерусалима; погибли 19 человек, более 200 ранены. Напряженной сохранялась обстановка вокруг святых мест Иерусалима: палестинцы напали на иудейскую святыню — гробницу Иосифа в районе города Наблус, израильская сторона применила непропорциональную силу, усилились подстрекательства к насилию

Мустафа Фетоури (Ливия), независимый аналитик и журналист — по электронной почте из Парижа:

В Ливии при посредничестве ООН сформировано правительство национального единства. Несмотря на существующие в его рядах противоречия, есть надежда на стабилизацию ситуации в разрушенной силами НАТО стране. Если правительство сможет начать полноценную работу, это станет позитивным достижением. Ожидать улучшения ситуации в Ливии можно в случае, если новым властям предоставят больше свободы действий и независимости.

Несмотря на недавние теракты, Тунис смог выйти на путь демократического развития. Принята конституция, сформировано правительство, избран президент. Достижения Туниса были отмечены двумя психологически важными наградами — Нобелевской премией мира, врученной Квартету национального диалога Туниса*, и премией Международной кризисной группы.*

Египет смог провести легитимные парламентские выборы. Новые законодательные органы страны в условия растущей угрозы терроризма должны провести процесс национального примирения и стать образцом преобразований для других арабских стран, которые всегда видели в Каире пример для подражания.

Россия вступила в конфликт в Сирии, чтобы не допустить повторения ливийского сценария. Решение даже несколько запоздало. Пролилось много крови, прежде чем Москва, наконец, вступила в борьбу против терроризма на Ближнем Востоке. Российское участие в сирийском урегулировании выявляет две важные тенденции. Первая — Россия и сегодня в состоянии противостоять агрессии и защищать свои интересы и интересы союзников в регионе. Вторая — Москва не ждет разрешения великих держав, чтобы начать участвовать в борьбе с общим врагом — международным терроризмом.

В 2016 г. безопасность на Ближнем Востоке и в Северной Африке улучшится в случае, если не произойдет дезинтеграции Сирии и сохранится федеративная система, гарантирующая территориальную целостность страны. Победу над ИГ не удастся одержать без наземной операции. Израильско-палестинские противоречия не разрешатся, пока Тель-Авив не освободит оккупированные территории Палестины на Западном берегу и Иерусалим.

Равновесие международной системы возможно при соблюдении принципа невмешательства крупных держав и НАТО в дела небольших государств. Россия должна быть шире представлена на мировой арене для достижения глобального равновесия.

Николай Злобин (США), президент Центра глобальных интересов — по телефону из Вашингтона:

Состояние безопасности в США осенью не изменилось. Падение российского самолета над Синаем, теракты в Париже и Мали повлияли на безопасность страны, но особой паники не наблюдалось, поскольку американцы живут в режиме борьбы с терроризмом еще с терактов одиннадцатого сентября. Раздающиеся в интернете угрозы радикалов устроить теракты в американских городах психологически воздействуют на общественные настроения, но реальная ситуация под контролем.

Парижские теракты показали, что негативный эффект от сливов Э. Сноудена оказался сильнее, чем полагали. Незаконные или полузаконные программы по наблюдению, опережающему слежению, прослушиванию подозрительных людей пришлось заморозить. Специалисты спецслужб полагают, что если бы не это, то можно было бы отследить подготовку терактов в Париже.

Европейский кризис с ближневосточными беженцами оказывает на США косвенное влияние. Американцы пока не видят прямой связи между беженцами и террористами, хотя осознают, что такие угрозы существуют. Миграционный кризис в Евросоюзе волнует Вашингтон в контексте собственных интересов на европейском континенте и обеспечения безопасности союзников.

Позитивом осени стало усиление роли американцев и европейцев в военной операции в Сирии. Вовлечение России в сирийский конфликт, что бы ни говорили на Западе, сыграло конструктивную роль. Террористическая активность благодаря участию Москвы в сирийской операции снизилась. Можно спорить, целесообразно ли уничтожать террористов бомбардировками, но активизацию операции следует воспринимать позитивно.

В 2016 г. события в мире будут развиваться по негативному сценарию. Главной угрозой станет активизация терроризма во многих регионах мира. Теракты последнего времени носят в основном спонтанный характер и происходят там, где их удобно организовать. Террористы не всегда связаны в большую сеть, поэтому их сложно отследить. Борьба с терроризмом усилится, но политические противоречия между крупными державами помешают фундаментальному объединению против этого зла. При всем желании спецслужб сотрудничать в передаче чувствительной информации руководство многих стран будет сдерживать эти намерения, руководствуясь политическими причинами.

в социальных сетях. 15 ноября по инициативе Иордании состоялось экстренное совещание Совбеза ООН по деэскалации арабо-израильского конфликта. 11 ноября Б. Нетаньяху и Б. Обама на встрече в США обсудили подписание соглашения в области безопасности, по которому американцы предоставят Израилю военную помощь в размере 50 млрд долл. США 18 ноября Б. Нетаньяху разморозил резонансный строительный проект в одном из спорных районов Иерусалима. 24 ноября Дж. Керри посетил Израиль и Палестину, где обсудил возможные варианты снижения напряженности. 29 ноября Тель-Авив приостановил дипломатические контакты с Евросоюзом по вопросу урегулирования конфликта с Палестиной.

В **Ливии** в начале октября сформировано правительство национального единства. 17 ноября новым спецпредставителем ООН по Ливии назначен немецкий дипломат М. Коблер. В стране продолжились бои между сторонниками сформированного правительства и боевиками ИГ и *Аль-Каиды*.

В **Нигерии** шли бои армии с боевиками *Боко харам*, присягнувшим ранее на верность ИГ.

АФГАНИСТАН–ПАКИСТАН

В октябре афганская армия при поддержке американских военных вернула контроль над городом Кундуз на севере Афганистана, но бои с талибами и боевиками, именующими себя ИГ, продолжились. Под контролем экстремистов оказались район Тала-ва-Барфак в провинции Баглан и Хваджа Гхар в провинции Тахар. США заявили, что сохранят военное присутствие в Афганистане до 2017 г. из-за неспособности афганской армии самостоятельно контролировать страну. 8 октября Минобороны России обнародовало данные о наличии на севере Афганистана ряда тренировочных центров боевиков ИГ, что представляет угрозу соседним странам Центральной Азии. Информацию об обострении ситуации на границах Таджикистана, Узбекистана и Туркменистана с Афганистаном официально подтвердила лишь таджикская сторона.

16 ноября территории Пакистана и Афганистана подверглись обоюдному минометному обстрелу; отношения стран обострились из-за взаимных обвинений в поддержке террористических группировок. 1 декабря президент Афганистана А. Гани и премьер-министр Пакистана Н. Шариф договорились возобновить совместные переговоры с движением *Талибан*.

2 декабря на встрече министров стран НАТО в Брюсселе была достигнута договоренность о продолжении военного присутствия в Афганистане в 2016 г.

23 октября на севере Афганистана в результате землетрясения погибли более 115 человек.

ЕВРОПЕЙСКИЙ СОЮЗ–США

13 ноября в **Париже** была совершена серия терактов. Одновременно были атакованы футбольный стадион, концертный зал *Bataclan*, ресторан и бар. Погибли 129 человек, более 350 получили ранения. Во Франции было объявлено чрезвычайное положение. Ответственность за теракты взяли на себя боевики ИГ. Ф. Олланд после парижских терактов заявил о необходимости широкой между-

Фарход Толипов (Узбекистан), директор негосударственного научно-образовательного учреждения *Караван знаний* — по электронной почте из Ташкента:

Уровень международной безопасности снизился в связи с обострением ситуации на Ближнем Востоке и терактами, прокатившимися в европейских и африканских странах. Эхо ближневосточных событий и проводимой военной операции России в Сирии докатилось до Центральной Азии. После того как Россия использовала Каспийскую флотилию для операции в Сирии, напряженность возникла и в районе Каспия. Милитаризация Каспия вызывает тревогу в центральноазиатских странах.

В соседнем с регионом Афганистане ситуация оставалась напряженной из-за раскола в рядах движения Талибан *и его конфликтом с* Исламским движением Узбекистана, *присягнувшим ИГ.*

Позитивным событием периода стало начало массированной военной кампании против ИГ. Создание международной коалиции нанесло мощный удар по ИГ и остановило его экспансию. Но существование двух коалиций против одного врага указывает на наличие у участников иных целей, помимо борьбы с терроризмом, что делает кампанию малоэффективной.

Зимой 2016 г. ситуация в мире будет находиться в состоянии flux *из-за вспыхнувшего российско-турецкого конфликта.*

Абдулазиз Сагер (Саудовская Аравия), председатель Исследовательского центра Залива — по электронной почте из Дубая:

Конфликты на Ближнем Востоке негативно воздействуют на безопасность стран, расположенных за пределами региона. Проблема беженцев в Европе, растущая террористическая угроза в мире — все это результат разрастания ближневосточного кризиса. Боевики ИГ заявили о намерении расширить театр боестолкновений далеко за пределы Сирии. Усилились атаки ИГ в Ливане, Турции, на Синайском полуострове, в Саудовской Аравии, Йемене. Вовлечение России в войну в Сирии на стороне режима Б. Асада привело к трагическим событиям. Решение Франции после терактов в Париже расширить военную кампанию против ИГ еще больше обострит ситуацию. Начало венской дискуссии не сулит дипломатического прорыва по сирийскому урегулированию, пока США, Россия и другие державы не сформируют коалицию. Пока мировое сообщество не поймет, что феномен ИГ не имеет чисто военного решения, проблема не сдвинется с мертвой точки.

Позитивным трендом осени стали успехи возглавляемой Саудовской Аравией коалиции в Йемене. Эти подвижки сулят возможность политического решения йеменского конфликта в среднесрочной перспективе.

Дайан Джаятеллека (Шри-Ланка), посол, профессор, университет Коломбо — по электронной почте из Коломбо:

Терроризм снова оказался на передовой глобальной, региональной и национальной безопасности. Уничтожение российского авиалайнера над Синаем, теракты в Париже и Мали — самые негативные события осени. Растущая угроза ИГ в Африке и Европе усугубляет ощущение растущей угрозы, формирует осадное мышление и усиливает поляризацию в обществе.

После речи В. Путина на 70-й Генеральной Ассамблее ООН, а также шока от парижских терактов возникло понимание, что необходимо объединить усилия мирового сообщества в борьбе с терроризмом и что усилия только западной коалиции в борьбе с ИГ бесперспективны. Российское предложение о создании широкой антитеррористической коалиции, включающей Запад, Россию, страны Ближнего Востока и Африки, приобретает все больше сторонников, так как выглядит наиболее эффективным методом ведения антитеррористической борьбы.

Создание широкой постпарижской коалиции должно стать главной целью мирового сообщества зимой 2016 г. Активная позиция России получит более широкое признание в мире, что будет способствовать формированию многополярных тенденций и здорового геополитического баланса на Ближнем Востоке и в мире.

народной коалиции при участии России и США для уничтожения ИГ. Переговоры с потенциальными участниками коалиции продолжились.

В **Черногории** в октябре — ноябре имели место протесты с требованием отставки премьер-министра М. Джукановича. 2 декабря Черногория получила приглашение вступить в НАТО. Процедура вступления продлится полтора года. Россия, выступавшая против расширения Альянса и вступления в него Подгорицы, заявила о негативном влиянии события на отношения РФ и НАТО.

5 октября в **США** завершились переговоры о создании Транстихоокеанского партнерства (ТТП), которые велись с 2005 г. Страны, представляющие треть мирового ВВП, в том числе США, Австралия, Канада, Япония, Малайзия, Мексика, Чили, Вьетнам, создают зону свободной торговли. В ТТП будут действовать нулевые пошлины, единые правила оборота интеллектуальной собственности и соглашение по валютной политике.

ПОСТСОВЕТСКОЕ ПРОСТРАНСТВО

Президент России В. Путин 16 октября на саммите СНГ в Казахстане заявил, что на стороне ИГ воюют от 5 до 7 тысяч выходцев из России и стран СНГ. В связи с ростом потенциальных угроз для стран Центральной Азии на саммите СНГ в Казахстане 15 октября была создана группировка погранслужб для реагирования на кризисные ситуации. Президент Таджикистана Эмомали Рахмон подтвердил, что на 60% протяженности таджико-афганской границы идут бои с афганскими радикальными группировками. Туркменистан отверг предположения казахских властей о растущей угрозе на туркмено-афганской границе; при этом в середине октября глава МИД Туркмении Р. Мередов посетил США и обсудил вопросы безопасности. Узбекистан усилил меры безопасности на узбекско-афганской границе.

28 октября премьер-министр Японии завершил первый визит в страны Центральной Азии. Итогом встречи стало решение Токио направить на развитие региона 25 млрд долл. США.

С 29 октября по 3 ноября Госсекретарь США Дж. Керри впервые за семилетнее пребывание демократов у власти посетил государства Центральной Азии, где обсудил угрозы региональной безопасности в связи с активизацией исламистских террористов в Афганистане и пообещал американскую помощь в поддержании стабильности в регионе. В рамках визита Керри в регион был создан новый формат диалога между Центральной Азией и США *С5+1.*

Ситуация на Украине. После встречи 6 октября глав государств *нормандской четверки* — России, Украины, Франции и Германии — представители ДНР и ЛНР согласились перенести местные выборы при условии выполнения Киевом политической части соглашения *Минск-2.* В конце октября Киев и руководство ДНР обвинили друг друга в нарушении перемирия и пригрозили возобновить силовую операцию. 6 ноября в Берлине прошла встреча глав МИД стран *нормандской четверки*. Стороны обсудили вопрос разминирования территории Донбасса и подтвердили, что минские соглашения будут действовать до полного выполнения. 25 ноября на Украине прошли местные выборы, отдельные районы Донецкой и Луганской областей не приняли в них участие. Главным итогом голосования стало ослабление позиций партии П. Порошенко.

Евгений Бужинский (Россия), председатель совета ПИР-Центра, генерал-лейтенант (запаса) — по телефону из Москвы:

Обострение обстановки в Сирии и террористические атаки против России и Франции значительно снизили уровень безопасности в мире. Наиболее негативными событиями осени стали подрыв российского гражданского лайнера над Синаем, теракты в Париже и атака турецких ВВС на российский фронтовой бомбардировщик из состава авиагруппы в Сирии. Агрессия со стороны Анкары резко обострила российско-турецкие двусторонние отношения. Дальнейшие события будут зависеть от усилий Франции по созданию широкой коалиции по борьбе с ИГ и возможной эскалации или деэскалации российско-турецкого конфликта. Будет ли Россия вводить в действие комплексный план свертывания двусторонних торгово-экономических отношений и реализует ли механизм поражения воздушных целей в районе российской авиабазы в Сирии — все это определит состояние региональной безопасности зимой 2016 г.

Дополнительным негативным фактором стало дальнейшее ухудшение российско-украинских отношений в сфере экономики, в частности взаимный запрет полетов гражданской авиации, энергетическая, транспортная и торговая блокада Крыма, прекращение поставок российского угля для украинских ТЭЦ. Кроме того, к марту 2016 г. должна быть выполнена политическая часть минских договоренностей и проведены местные выборы в ДНР и ЛНР. Если развитие событий по обозначенным направлениям будет развиваться в положительном ключе, уровень безопасности повысится, если нет — понизится.

С натяжкой к положительным событиям осени можно отнести венские переговоры в расширенном составе по вопросу сирийского урегулирования и возобновление российско-американского неформального диалога. Несколько заявлений западноевропейских лидеров свидетельствуют, что в Европе находит понимание российская позиция по Сирии и по выполнению минских договоренностей по Украине. На Западе понимают, что Киев также должен пройти свою часть пути по имплементации этих договоренностей.

Евгений Сатановский (Россия), президент Института Ближнего Востока — по электронной почте из Москвы:

Участие воздушно-космических сил России в военной операции в Сирии позитивно повлияло на ближневосточный климат безопасности. В 2016 г. интенсификация действий Москвы против террористических группировок и их спонсоров еще более улучшит состояние безопасности в регионе.

Наиболее негативным событием осени 2015 г. стал теракт против российского пассажирского лайнера на Синае. Эксперты Института Ближнего Востока возлагают вину за этот теракт на Катар и персонально на главу катарского внешнеполитического ведомства Х. аль-Атыйю.

Другое негативное событие периода — действия Турции и президента Т. Р. Эрдогана, спровоцировавшие поток мигрантов и беженцев в Евросоюз с территории Турции через Балканы.

Халил Каравели (Турция — Швеция), руководитель проекта по Турции Института по изучению Центральной Азии и Кавказа при университете Джонса Хопкинса — по электронной почте из Стокгольма:

Парламентские выборы в Турции летом 2015 г. вселили надежду, что правлению авторитарной Партии справедливости и развития приходит конец. Но провалившиеся переговоры по созданию правящей коалиции, тактика насилия и устрашения правящего режима привели к внеочередным парламентским выборам в ноябре. Они вернули Т. Р. Эрдогану парламентское большинство.

Главную угрозу региональной безопасности создает ситуация в Сирии. Угроза терактов возросла не только на Ближнем Востоке, но и в Европе. Единственным позитивным событием на фоне наблюдаемого в регионе хаоса можно назвать ядерную сделку с Ираном. Что происходило бы сейчас, если бы угроза ядерного распространения была актуальна по Ирану, — страшно представить.

Стоит надеяться, что США, ЕС, Россия, союзники этих стран на Ближнем Востоке все же смогут создать единую коалицию для борьбы с ИГ и терроризмом. Но реальность показывает, что поводов для надежд нет.

20 ноября в Херсонской области произошел подрыв опор ЛЭП, по которым электричество поставляется в **Крым**. 22 ноября Крым полностью отключился от поставок электроэнергии с Украины. П. Порошенко инициировал остановить грузовое сообщение с полуостровом.

В **Молдавии** в октябре — декабре продолжились антиправительственные демонстрации; протестующие выступили с требованием провести референдум для прямых выборов президента и изменения конституции страны.

В **Белоруссии** 12 октября состоялись президентские выборы, победу одержал А. Лукашенко. Евросоюз приостановил санкции в отношении Белоруссии.

В **Азербайджане** 1 ноября прошли парламентские выборы, завершившиеся победой пропрезидентской правящей партии. На протяжении осени на линии соприкосновения вооруженных сил Азербайджана и Нагорного Карабаха имели место столкновения военных.

19 октября в **Канаде** прошли парламентские выборы. Победу одержала Лейбористская партия. Новым премьер-министром страны стал Ж. Трюдо.

7 ноября лидеры **Китая** и **Тайваня** Си Цзиньпин и Ма Инцзю провели в Сингапуре первую встречу с момента окончания гражданской войны.

17 ноября на **Филиппинах** прошел очередной саммит АТЭС. Итогом мероприятия стала декларация о намерении создать зону свободной торговли в регионе.

22 ноября в **Аргентине** состоялись президентские выборы. Победу одержал кандидат от оппозиции М. Макри.

Галия Ибрагимова

ГЛАЗАМИ ЛИБЕРАЛА: ВРЕМЯ ТУРБУЛЕНТНОСТИ

Though this be madness, yet there is method in't[1].

Этот обзор предназначен главным образом для российской аудитории, что предопределило его тематику: он сфокусирован на событиях, представляющих особый, остроактуальный интерес для Российской Федерации. К ним относятся гражданская война в Сирии, перспективы нынешней холодной войны между Россией и Западом, развитие ситуации в Украине и миграционный кризис в Европе. Эта тематика, естественно, охватывает лишь часть, причем, возможно, далеко не самую важную, сложного переплетения разнонаправленных процессов, определяющих мировую политику. В частности, в обзоре не затрагивается продолжающееся, хотя и низкими темпами, снижение цен на нефть; осложнение экономической ситуации в Китае и достигнутое в октябре 2015 г. соглашение о создании Транстихоокеанского партнерства, крупнейшей интеграционной группировки, на которую приходится почти 40% глобального ВВП и около четверти мирового экспорта[2]. В среднесрочной перспективе, а, возможно, и раньше они могут оказаться намного более важными для российской экономики и, следовательно, политики, чем, например, локальный по своим масштабам конфликт в Сирии или практически неизбежное геополитическое переформатирование некоторых регионов Ближнего Востока. Сегодня, однако, когда рухнули планы так называемого

20 ноября в Херсонской области произошел подрыв опор ЛЭП, по которым электричество поставляется в **Крым**. 22 ноября Крым полностью отключился от поставок электроэнергии с Украины. П. Порошенко инициировал остановить грузовое сообщение с полуостровом.

В **Молдавии** в октябре — декабре продолжились антиправительственные демонстрации; протестующие выступили с требованием провести референдум для прямых выборов президента и изменения конституции страны.

В **Белоруссии** 12 октября состоялись президентские выборы, победу одержал А. Лукашенко. Евросоюз приостановил санкции в отношении Белоруссии.

В **Азербайджане** 1 ноября прошли парламентские выборы, завершившиеся победой пропрезидентской правящей партии. На протяжении осени на линии соприкосновения вооруженных сил Азербайджана и Нагорного Карабаха имели место столкновения военных.

19 октября в **Канаде** прошли парламентские выборы. Победу одержала Лейбористская партия. Новым премьер-министром страны стал Ж. Трюдо.

7 ноября лидеры **Китая** и **Тайваня** Си Цзиньпин и Ма Инцзю провели в Сингапуре первую встречу с момента окончания гражданской войны.

17 ноября на **Филиппинах** прошел очередной саммит АТЭС. Итогом мероприятия стала декларация о намерении создать зону свободной торговли в регионе.

22 ноября в **Аргентине** состоялись президентские выборы. Победу одержал кандидат от оппозиции М. Макри.

Галия Ибрагимова

ГЛАЗАМИ ЛИБЕРАЛА: ВРЕМЯ ТУРБУЛЕНТНОСТИ

Though this be madness, yet there is method in't[1].

Этот обзор предназначен главным образом для российской аудитории, что предопределило его тематику: он сфокусирован на событиях, представляющих особый, остроактуальный интерес для Российской Федерации. К ним относятся гражданская война в Сирии, перспективы нынешней холодной войны между Россией и Западом, развитие ситуации в Украине и миграционный кризис в Европе. Эта тематика, естественно, охватывает лишь часть, причем, возможно, далеко не самую важную, сложного переплетения разнонаправленных процессов, определяющих мировую политику. В частности, в обзоре не затрагивается продолжающееся, хотя и низкими темпами, снижение цен на нефть; осложнение экономической ситуации в Китае и достигнутое в октябре 2015 г. соглашение о создании Транстихоокеанского партнерства, крупнейшей интеграционной группировки, на которую приходится почти 40% глобального ВВП и около четверти мирового экспорта[2]. В среднесрочной перспективе, а, возможно, и раньше они могут оказаться намного более важными для российской экономики и, следовательно, политики, чем, например, локальный по своим масштабам конфликт в Сирии или практически неизбежное геополитическое переформатирование некоторых регионов Ближнего Востока. Сегодня, однако, когда рухнули планы так называемого

Пал Дунай (Венгрия), директор Академии ОБСЕ в Бишкеке — по электронной почте из Бишкека:

Состояние безопасности в Европе ухудшилось. Страны Восточной и Центральной Европы, которые обычно упоминались скорее в региональном, нежели глобальном контексте, ощутили на себе последствия тлевших мировых кризисов. В европейской повестке дня доминировали два события: миграционный кризис и ситуация на Украине.

Миграционное давление на Европу — серьезная проблема, обострившаяся в 2015 г. Угрозу миграции в европейский регион рассматривают в привязке к угрозе терроризма и борются с двумя проблемами, как с одной. Фундаментальная ошибка заключается в том, что Конвенция о статусе беженцев 1951 г. основывается на принципе, что получить в Европе убежище могут люди, подвергшиеся гонениям по политическим, расовым, религиозным причинам. Речь не идет о массовых перемещениях граждан по экономическим причинам, и статус беженцев таким переселенцам не полагался. Но когда заключалась Конвенция, Европа не могла предположить, что через полвека миллионы людей из охваченных войнами и хаосом стран — от Сирии до Ливии, Эритреи и Афганистана — смогут на законном основании претендовать на статус беженцев. Юридический механизм не выдержал тяжести сложившейся реальности. По мере того как потоки мигрантов будут поставлены под контроль, европейцам придется поступиться одним из главных демократических принципов — правом свободного передвижения по Европе.

Соглашение Минск-2 *привело к снижению интенсивности боевых действий на юго-востоке Украины. Однако этот документ не совсем объективный, потому что в нем говорится не о широкомасштабном российско-украинском конфликте, а только о внутриукраинском противостоянии. Украинский конфликт может быть разрешен на основе классического сценария — достижением* негативного *мира, где причины конфликта не устранены, но враждебность сторон взята под контроль. Запад вложил немалые средства в экономическую стабилизацию страны, но если Киев не проведет радикальные реформы в 2016 г., Запад откажет в финансировании коррумпированному клептократическому украинскому режиму. Ни Европа, ни США не станут тратить от 30 до 40 млрд долл. США на страну, которая не выполняет взятые на себя обязательства и игнорирует все данные обещания.*

НАТО и Евросоюз проявили готовность к компромиссам и смогли сохранить единство в принятии решений. Были противоречия в вопросе расширения санкций против России, но санкционный режим в целом сохранялся.

Североатлантический Альянс смог сохранить баланс между коллективной обороной и управлением кризисами. Защита стран НАТО, находящихся в непосредственной близости от Москвы, усилилась. В текущем году она особенно потребовалась Эстонии, Латвии, Литве, Польше, Румынии. Эти относительно новые члены Альянса убедились не в номинальных, а в реальных гарантиях безопасности, полагающихся им наравне со старыми *государствами-членами.*

Сержио Дуарте (Бразилия), посол, высокий представитель ООН по вопросам разоружения (2007–2012 гг.) — по электронной почте из Белу-Оризонте:

Уровень безопасности в мире ухудшился. Россия и США, похоже, не смогут договориться о совместной борьбе с терроризмом. Евросоюз не способен действовать более решительно, и от него не следует ожидать ничего, кроме неэффективных воздушных атак по террористам. Между тем, после терактов в Париже взаимодействие Востока и Запада в борьбе с международным терроризмом актуально как никогда.

Несмотря на чудовищные теракты, общественное мнение в Европе и США не может найти баланс между демократией и безопасностью. Чем больше усилий требуется от великих держав в противодействии угрозам, тем меньше сплоченности в их рядах и тем хуже складывающаяся ситуация. Если террористические группировки решат использовать ОМУ, то негативные последствия ощутят на себе все страны мира. Угроза увеличивается по мере того, как великие державы также усиленно вооружаются. Предотвратить распространение вооружений в подобных условиях вряд ли получится.

Латинская Америка остается на периферии конфликтных зон и не ощущает на себе угрозу эскалации терроризма и последствия напряженности между Востоком и Западом. Ситуация в регионе стабильная, и общественное мнение занято, в основном, решением внутренних проблем — бедности, криминала, соблюдения прав человека, защитой экологии.

поворота на Восток и связанные с ним надежды, российская внешняя политика вновь сосредоточивается на западном и ближневосточном направлениях.

ЛОГИКА ТУРБУЛЕНТНОСТИ

Об относительно длительных последствиях инцидента с российским фронтовым бомбардировщиком Су-24, вторгнувшимся в воздушное пространство Турции и сбитым турецким истребителем, говорить пока рано. Но уже ясно, что идея широкой международной антитеррористической коалиции с участием России, которая, предположительно, могла бы создать предпосылки для смягчения ее противостояния с Западом, вызванного событиями в Украине и вокруг нее, оказалась несостоятельной. И самое главное: инцидент с Су-24 подтвердил, что начиная с февраля 2014 г., с первых моментов гибридной войны России против Украины, международные отношения в районах, прилегающих к российским границам, на Ближнем Востоке и в мусульманском мире в целом вошли в *полосу турбулентности*, когда ломаются привычные, выработанные в последние два с лишним десятилетия модели, нормы, стереотипы и механизмы, определяющие взаимоотношения государств. Неизбежное следствие наступившей турбулентности — непредсказуемость международных отношений и растущая вероятность того, что события, сами по себе незначительные, могут стать своего рода триггерами, вызывающими к жизни гораздо более масштабные и, как правило, опасные процессы. Это, в свою очередь, заставляет политических лидеров и правящие элиты ориентироваться не на самый вероятный, но на самый опасный вариант развития событий. А ключевой вопрос *чем же все завершится* остается открытым.

Пятьсот лет тому назад Уильям Шекспир подметил, что в безумии часто есть логика, свой, как он заметил, *method in madness*. В наше время это наблюдение подтверждено психологами и психиатрами. Оно, однако, справедливо не только при лечении душевнобольных, но и при анализе мировой политики. Действительно, на первый взгляд, турбулентность и ее причины воспринимаются как торжество абсурда, как хаотическое нагромождение плохо связанных друг с другом, вышедших из-под контроля иррациональных действий и событий. На деле в этом хаосе просматривается определенная логика. Нынешняя турбулентность порождается сочетанием двух основных факторов: линией российского руководства на переформатирование международных отношений и противостоянием социальных слоев и групп, являющихся движущей силой модернизации, и кругов, пытающихся сохранить традиционные ценности и структуры.

РОССИЯ КАК ФАКТОР СТРАТЕГИЧЕСКОЙ НЕСТАБИЛЬНОСТИ

К стремлению Москвы переформатировать систему международных отношений, сложившуюся после окончания *первой холодной войны*, и, прежде всего, утвердить Россию в качестве одного из ведущих центров современного мира, сопоставимого по своему влиянию с США и Китаем, можно относиться по-разному. Но главное в том, что экономические, научно-технические и политические ресурсы России заведомо недостаточны для достижения этой цели.

В основе этого — слабость российской экономики, которая, как писал в 2012 г. президент Путин, «не гарантирует нам ни стабильности, ни суверенитета, ни достойного благосостояния». Он отмечал «крайне высокую зависимость от импорта потребительских товаров, технологий и сложной продукции; от колебания цен на основные экспортные товары», подчеркивал необходимость экономики, «работающей на современной технологической базе», и предупреждал о недопустимости и неэффективности протекционистских мер, поскольку «чрезмерный протекционизм всегда приводит к застою, низкому качеству и высоким ценам»[3].

Установки высшего политического руководства России остались невыполненными. Кризис, начавшийся в 2013 г., стал закономерным следствием той самой экономической модели, которая, по словам президента Путина, «не гарантировала ни стабильности, ни суверенитета». Геополитические амбиции, заложенные в нынешней внешнеполитической стратегии Кремля, пришли в противоречие с экономическим и технологическим потенциалом страны, несопоставимым с соответствующими возможностями ведущих мировых держав.

Особое значение имеет далеко зашедшее и, возможно, уже непреодолимое отставание России по научно-исследовательским и опытно-конструкторским работам (НИОКР) — ключевом факторе, определяющем перспективы развития экономики и военной мощи. Об этом, в частности, свидетельствует опубликованный в июне 2015 г. *Доклад ЮНЕСКО по науке: на пути к 2030 году*. По данным ЮНЕСКО, основанным на информации, предоставленной правительствами государств-членов, в 2009–2013 гг. российские расходы на НИОКР были примерно в 25 раз ниже, чем совокупные расходы на эти цели трех основных центров того, что принято называть западным миром, — США, ЕС и Японии.

Таблица 1. **Расходы на НИОКР в 2009 и 2013 гг. (млрд долл. США в пересчете по ППС)**[4]

Страны/ объединения	Годы	
	2009	2013
США	406,0	453,5
ЕС	287,0	342,5
Китай	184,2	336,6
Япония	136,9	160,2
Индия	39,4	48,1
Россия	34,6	40,7

Бросается в глаза также, что если в 2013 г. финансирование российских НИОКР увеличилось по сравнению с 2009 г. на шесть млрд долл. США, то Запад в этот период нарастил финансирование науки на 126 млрд долл. США. Есть и другие подтверждения растущего научного и, соответственно, технологического отставания России. Так, в США выдается 120,8 патента на 100 научных публикаций в области нанотехнологий, в Японии — 94,4, в Германии — 25,6, а в России — 1,1[5].

Неспособность России конкурировать в научно-технической сфере с Западом, а в недалеком будущем — и с Китаем, намного обгоняющим Россию и по расходам на НИОКР, и по количеству научных публикаций, дополняет ее хорошо известное отставание от технологически развитых стран как по количественным показателям, так и по качественным параметрам экономики. При этом сланцевая революция, в том числе начавшееся внедрение технологии плазменного импульса вместо гидроразрыва пластов[6], неизбежное появление на мировых рынках иранских нефти и газа, растущее использование сжиженного природного газа, вовлекающее в глобальную энергетику газовые месторождения, находящиеся далеко от основных районов потребления газа, предопределяют дальнейшую деградацию российской экономики, основанной на экспорте углеводородов.

В этих условиях веер стратегических альтернатив, имеющихся в распоряжении российского руководства, крайне узок. По сути дела, их всего две. Первая — сосредоточить имеющиеся ресурсы на форсированном развитии тех направлений НИОКР, по которым Россия сохраняет конкурентоспособность, и на этой основе вписаться в мировую экономическую систему в качестве важного, хотя и не сравнимого по своему влиянию с США и ЕС субъекта, подчинив внешнюю и внутреннюю политику нормам и принципам, утвердившимся в развитой части мира. По причинам, обсуждение которых выходит за рамки этого обзора, для российского руководства такой подход оказался неприемлемым. Это, в свою очередь, подтолкнуло российский истеблишмент к другой альтернативе.

Как писал российский аналитик Владимир Фролов, если раньше российская внешняя политика отстаивала главные принципы международного права и основы миропорядка как самоценности — уважение суверенитета, территориальной целостности, признанных границ, неприменение военной силы, невмешательство во внутренние дела, то сегодня она видит в них инструменты избирательного применения. «Стратегическая цель — ... геополитический паритет с США, понимаемый как право второго ключа России на большинство глобальных и региональных проблем, обязательность обсуждения с РФ всех силовых действий США и даже право вето на них в регионах жизненно важных российских интересов. Идеальное устройство — это возвращение к системе двусторонних консультаций СССР — США конца 1970-х — середины 1980-х гг. по ключевым международным проблемам при полном отсутствии какой-либо взаимозависимости»[7].

Такая стратегия предопределяет опору на единственный ресурс, по которому Россия сопоставима с США и обгоняет все другие страны, то есть на ядерное оружие. Для этого потребовалось восстановить в международных отношениях механизмы, типичные для периода первой холодной войны. Итог очевиден — серьезная дестабилизация стратегической ситуации.

СОПРОТИВЛЕНИЕ МОДЕРНИЗАЦИИ

Другой источник турбулентности в международной политике — столкновение того, что еще двадцать лет тому назад Вацлав Гавел назвал *глобальной цивилизацией*, и теми, кто отстаивает «право поклоняться ... древним богам и следовать старым священным пророчествам»[8]. Действительно, уже давно было отмечено, что глобализация и научно-технический прогресс, как ключевые факторы модернизации, открывают перед государствами, экономическими субъектами, социальными

группами и индивидами новые возможности и одновременно требуют принятия новых ценностей, следования новым нормам и принципам поведения.

Являясь необходимым условием благосостояния и развития, включение в глобализацию приводит к эрозии традиционных групп, структур и идеологий, сопровождается падением их социального статуса и ухудшением экономического положения. В итоге возникает неприятие глобализации и, в целом, модернизации со стороны тех, кто не в состоянии соответствовать новым требованиям, воспринять и реализовать свойственные новым условиям стереотипы и модели. Такая реакция характерна не для наиболее отсталых, погруженных в нищету регионов: последние практически не затронуты модернизацией. Сопротивление ей возникает, прежде всего, в той части мира, которая уже вовлечена в становление транснациональной экономики и глобальных институтов, но не готова к активному участию в них.

Группы и силы, видящие в модернизации угрозу собственным привилегированным позициям, часто добиваются возвращения в международной политике к устаревшим геополитическим парадигмам, основанным на традиционных концепциях баланса сил, сфер влияния, концепта великих держав и абсолютного национального суверенитета. У них часто возникает соблазн направить накапливающееся раздражение масс вовне, нацелить его на те страны и регионы, которые являются символом и источником перемен, прежде всего США. В мусульманском мире к ним относится также Израиль. Такая стратегия часто получает поддержку масс: мифологизированное сознание склонно искать причины собственного неблагополучия в действиях внешних *сил зла*.

В идеологическом плане сопротивление переменам чаще всего выражается в обращении к религиозным и политическим доктринам, идеализирующим прошлое, видящим в происходящих в мире изменениях моральную и социальную деградацию. В целом же, незавершенная модернизация нередко выливается в социальную дезориентацию, раздражение и агрессивность, перерастающие в террористические устремления.

В наибольшей степени эти процессы характерны для мусульманского мира, в том числе для мусульманских общин Европы и Северной Америки, что способствует распространению там радикального ислама. Последний стал идеологической основой противодействия переменам и сохранения традиционных культур, противоборства с либеральным, антропоцентрическим видением мира. *Умеренный* вариант ислама оказался в глазах значительной части населения мусульманских стран — как плохо образованных масс, так и нередко рафинированной верхушки, получившей образование в лучших западных университетах, — неспособным предотвратить размывание традиционного общества под воздействием новых экономических моделей и социальных идей. В свою очередь, радикальный ислам ясно обозначает путь — *священную войну* во имя утверждения истинных ценностей и собственной веры как единственно правильного пути к спасению.

Из этого следует тревожный вывод. По мере вовлечения в глобализацию — а это неизбежный процесс — в мире нарастают силы, пытающиеся ее остановить и с этой целью вступающие в противостояние с постмодернистской цивилизацией Запада. Это противостояние может принять форму *глобальной герильи*, полями

сражений которой будут не только ущелья и плоскогорья стран Юга, но и городские джунгли крупнейших мегаполисов Севера.

«Международный терроризм представляет собой механизм воздействия коалиции немодернизированных (вернее, частично модернизированных) традиционных обществ на мир либеральной цивилизации», — писал российский политолог Игорь Яковенко. — «В этом нет злого умысла со стороны Запада. Динамичные общества по своей природе эффективнее застойных и разлагают традиционный мир. Однако идеологи традиции осмысливают эту закономерность мировой истории как заговор, направленный против традиционного мира. ...Силы, поддерживающие международный терроризм, стремятся дестабилизировать Запад, оторвать от него страны, недавно избравшие либеральный путь, изменить вектор исторического развития» [9].

СИРИЙСКИЙ ТУПИК

Российская военная операция в Сирии, последовавшие за ней гибель российского авиалайнера, террористическая атака в Париже в *черную пятницу* 13 ноября 2015 г., уничтожение Су-24 и острейший кризис в отношениях России с Турцией вновь привлекли всеобщее внимание к гражданской войне в Сирии, исламскому терроризму и в более широком контексте к вопросу о том, что, собственно, происходит на Ближнем Востоке и имеется ли шанс стабилизировать стратегическую обстановку в этом регионе. Происходящие в этой зоне события подробно, день за днем описаны в средствах массовой информации. Важно, однако, выделить несколько устойчивых характеристик сложившейся ситуации. Главное в том, что острейший внутренний конфликт в Сирии не имеет ни военного, ни политического решения. Во многом это предопределено соотношением сил противоборствующих группировок и, в целом, спецификой военно-политической ситуации в этой стране.

СООТНОШЕНИЕ СИЛ

Вооруженные силы режима Асада насчитывали в конце 2014 г. (более поздних данных в открытых публикациях найти не удалось), по разным оценкам, от 150 до 170 тыс. солдат и офицеров [10]. Однако, в полной мере лояльными Б. Асаду и его клану считаются 65–70 тысяч человек, служащих в элитных частях [11]. Наряду с вооруженными силами режим опирается на ополчение, известное как Национальные силы обороны (National Defense Forces), состоящее из отрядов шиитской милиции *шабиха* (в переводе с арабского *призраки*), созданной в 1980-е годы братом Х. Асада из алавитских бандитских группировок, контролирующих контрабанду и другой криминальный бизнес в провинции Алеппо [12], а также проасадовские отряды местной самообороны. Численность этого ополчения оценивается от 60 до 100 тыс. человек [13]. Наконец, на стороне Б. Асада воюют члены проиранских шиитских формирований из Ливана, палестинских и некоторых других террористических группировок, общей численностью около восьми тысяч человек, из которых примерно половину составляют члены *Хезболлы*. Военнослужащие иранского *Корпуса стражей иранской революции* в основном выполняют обязанности советников в вооруженных силах режима, участвуют в разведывательных

операциях, подготовке и обучении личного состава, в первую очередь элитных частей и соединений.

Общая численность оппозиционных режиму Б. Асада группировок оценивается приблизительно в 100–120 тыс. человек, точных цифр никто не знает. Их обычно объединяют в четыре основные категории. Первая — *Свободная сирийская армия* (ССА), сформированная, главным образом, из бывших солдат и офицеров армии Б. Асада. Она и примыкающие к ней группировки выступают в большинстве своем за светский характер будущего сирийского государства. Эта часть сирийской оппозиции пользуется политической поддержкой западных государств, получает от них, хотя и в небольших количествах, некоторые виды оружия.

Вторая состоит из двух экстремистских террористических исламистских организаций: *Джабхат ан-Нусра* (*Фронт помощи*), являющейся одним из самых яростных противников Б. Асада, и *Исламского государства* (ИГ). Первая возникла в 2012 г. как отделение *Аль-Каиды* в Сирии и привлекла к себе наиболее радикальные исламистские элементы в стране и из-за рубежа. Вторая изначально появилась в Ираке в 2006 г., в середине 2013 г. проникла в Сирию и приобрела широкую известность летом 2014 г., после того как объявила о создании своего государства. ИГ вступило в вооруженное противоборство со всеми оппозиционными Б. Асаду группами, в том числе со своим идеологическим близнецом *Джабхат ан-Нусрой*, но, по мнению многих специалистов, заключило с Дамаском молчаливую договоренность: по возможности минимизировать столкновения друг с другом.

Третья категория состоит из формирований, выступающих за построение будущего сирийского государства на основах шариата. Эти группировки пользуются поддержкой Саудовской Аравии, Катара, других государств Персидского залива и Турции. Одни из них занимают относительно умеренные позиции, сходные с установками *Братьев-мусульман*, например признают необходимость проведения демократических выборов, в результате которых рассчитывают прийти к власти. Другие, прежде всего объединенные в так называемый *Джабхат аль-Исламийя* (*Исламский фронт*), занимают намного более одиозные позиции, требуя, в частности, создания в будущем государстве неких совещательных органов, сформированных из авторитетных людей (*маджлис аш-шура*), которые, в свою очередь, выбирают лидера или, точнее, халифа.

Наконец, населенные курдами северные районы страны вдоль границы с Турцией фактически обрели независимость. Курдские вооруженные формирования действуют, главным образом, против *Исламского государства*, которое контролирует большую часть соседних с курдскими районами территорий.

ВОЙНА БЕЗ ПОБЕДЫ

Хотя вооруженные силы режима Б. Асада в 2–2,5 раза превосходят оппозиционные формирования по численности личного состава, имеют полное господство в воздухе и оснащены тяжелым вооружением, которого у противника почти нет, одержать военную победу они не могут. По некоторым подсчетам, для победы в антипартизанской войне, предполагающей установление эффективного контроля над территорией, где действуют партизанские группировки, регулярные войска должны превосходить их в соотношении примерно 10 к 1. Следовательно, даже

в том случае, если благодаря успешным политическим мероприятиям удастся вывести из активного противоборства, скажем, половину антиасадовских сил, для подавления сопротивления оставшихся потребуется полумиллионная армия, что заведомо превышает возможности режима и его союзников.

При этом вооруженные силы режима Б. Асада решают не только несколько стратегических задач, таких как оборона Дамаска, бои за вторую столицу страны Алеппо и ключевые города Хаму и Хомс, контроль над магистральным шоссе, связывающим Дамаск с Алеппо, оборона подступов к районам, населенным алавитами в провинции Латакия. Помимо этого они контролируют или пытаются контролировать множество небольших городов и населенных пунктов. В результате они распылены как в географическом, так и в тактическом отношениях и не способны к крупным наступательным операциям.

Далее, армия Б. Асада испытывает все более острую нехватку личного состава. Мобилизационный потенциал алавитского религиозного меньшинства, составляющего 10–12% населения страны, практически исчерпан, а призванные в вооруженные силы сунниты в большинстве своем недостаточно лояльны (или вообще нелояльны) алавитской верхушке режима[14]. Нарастает недоверие и противостояние между офицерским корпусом, во многом состоящем из алавитов, и рядовым составом: сирийские сунниты отнюдь не стремятся воевать и умирать за сохранение чуждого и надоевшего им режима. В итоге боевой дух армии в массе своей низок, что еще более снижает ее боеспособность.

Сокращается поддержка режима со стороны алавитского населения, которое обычно считается главной опорой правящего клана. Алавиты оказались в исключительно сложной и опасной ситуации. С одной стороны, они опасаются, что поражение Б. Асада приведет к массовому вторжению исламских радикалов суннитского толка в населенные ими территории. С другой, — в их среде нарастает недовольство кланом Б. Асада, втянувшим алавитов в противоборство с суннитами, грозящее им тяжелыми последствиями. Этому способствуют также крупные потери среди алавитов, служащих в асадовских вооруженных силах. Идеальным выходом из складывающейся ситуации для них был бы уход Б. Асада и его клана. Это снизило бы давление на них со стороны суннитских группировок и облегчило бы договоренность об автономии их районов в будущем государстве.

Важным элементом военной стратегии режима Б. Асада являются авиа- и артиллерийские удары по гражданскому населению районов, контролируемых оппозицией, с тем чтобы сократить мобилизационный потенциал противостоящих группировок, запугав их или вынудив мигрировать из страны. С одной стороны, это действительно приводит к массовому бегству за рубеж или перемещению населения в районы, контролируемые правительством Б. Асада, но с другой, — резко увеличивает число противников режима.

Снижение боеспособности вооруженных сил режима Б. Асада привело весной-летом 2015 г. к ряду его серьезных поражений. В частности, в марте 2015 г. оппозиционные группировки, принадлежащие к *Армии завоевания* (*Army of conquest*), заняли столицу провинции Идлиб, а два с половиной месяца спустя вытеснили верные Б. Асаду войска из всей этой провинции[15]. Возникла прямая угроза для населенных алавитами районов в провинции Латакия.

Российская воздушная операция в Сирии помогла режиму Б. Асада избежать если не катастрофы, то, по крайней мере, тяжелого поражения. Однако переломить военно-политическую ситуацию в Сирии не удалось. По сообщению начальника российского Генерального штаба генерала В. Герасимова, к 17 ноября 2015 г., то есть через 48 дней после начала интенсивных российских бомбардировок, армия режима Б. Асада «освободила 80 населенных пунктов, обеспечив установление контроля над территорией более 500 квадратных километров»[16]. Столь незначительные результаты воздушных ударов — *освобождена* территория размером 25х20 километров — подтверждают выводы, многократно сделанные военными экспертами: массированные авиационные бомбардировки не могут обеспечить победу в контрпартизанской войне, а вооруженные силы Б. Асада и его режима не в состоянии провести крупные наземные операции. Но и оппозиция, в свою очередь, не имея тяжелых вооружений, не в состоянии взять Дамаск, Алеппо и другие крупные города, а также начать активные действия в районах, населенных алавитами. Иными словами, ни одна из сторон в сирийской гражданской войне одержать военную победу не может.

ПОЛИТИЧЕСКОЕ УРЕГУЛИРОВАНИЕ В СИРИИ: БЕЗ ПЕРСПЕКТИВ

Военный тупик в Сирии в сочетании с российской военной операцией и террористической атакой в Париже стимулировал осенью 2015 г. международные усилия по политическому урегулированию сирийского конфликта. 14 ноября 2015 г. Международная группа поддержки Сирии (МГПС) согласовала некоторые принципы такого урегулирования[17]. Конкретно, члены Группы договорились:

- предпринять все возможные шаги по обеспечению соблюдения режима прекращения огня теми группами или лицами, сторонниками которых они являются, которым они предоставляют материальную поддержку или на которых они оказывают влияние;
- немедленно предпринять шаги по поощрению мер укрепления доверия, которые будут способствовать жизнеспособности политического процесса, а также создадут условия для общенационального прекращения огня;
- оказывать давление на стороны в целях обеспечения немедленного прекращения любого применения подобного оружия неизбирательного действия;
- поддержать процесс, осуществляемый под руководством самих сирийцев, целью которого является создание в течение шести месяцев надежной, инклюзивной и неконфессиональной системы управления, а также определение сроков и процедуры разработки новой конституции;
- что в течение 18 месяцев должны быть проведены свободные и справедливые выборы в соответствии с положениями новой конституции;
- что прекращение огня не распространяется на *Исламское государство*, *Джабхат аш-Нусру* и другие организации, которые МГПС сочтет террористическими[18].

Само по себе согласие важнейших внешних *игроков* в сирийском конфликте по этим моментам, бесспорно, важно. И тем не менее, трудно отделаться от впечатления, что это не более чем дипломатическая имитация политического процесса урегулирования сирийского кризиса, но отнюдь не само урегулирование.

Об этом предельно ясно писал ведущий российский специалист-ближневосточник Г. Мирский:

«Ничего не получится, пока у власти Б. Асад. Ни один оппозиционер, повстанец, а тем более тот, кто четыре года воюет, ни за что не согласится жить под властью этого человека. И ведь все это понимают, но с непостижимым упорством продолжают твердить о том, что мы, дескать, не за Б. Асада персонально, а за право народа решать свою судьбу на выборах. Опомнитесь, какие выборы в залитой кровью стране, где разрушена половина жилого фонда и предприятий, где насчитывается, по оценкам Центра Картера, 7 тыс. различных группировок? В стране, из которой бежали миллионы граждан (тоже ведь избиратели)?»[19]

Это важная, но далеко не единственная причина тщетности всех нынешних усилий по политическому урегулированию сирийского кризиса. Помимо всего прочего, в МГПС не участвуют те, от кого на практике зависит прекращение огня, — командиры вооруженных групп и отрядов, сражающихся с режимом Б. Асада и подчас друг с другом. Они далеко не всегда и не во всем склонны подчинятся органам, претендующим на политическое руководство, а также своим иностранным союзникам. И самое главное — не решен ключевой вопрос о судьбе Б. Асада и его режима. Речь при этом идет не только и не столько о будущем самого сирийского президента, сколько о будущем семейного клана Асадов/Махлуфов и тесно связанных с ними персонажей и группировок, контролирующих армию, органы госбезопасности и ключевые сегменты экономики[20].

НОВАЯ ЯЛТА?

После терактов в Париже и саммита G20 в Анталье политики и эксперты стали всерьез обсуждать перспективы сотрудничества России с Западом, переходящего в своего рода *новую Ялту*. Предполагается, что *Исламское государство* и международный терроризм — глобальная опасность, сопоставимая с нацистской Германией. Для борьбы с этим злом Запад должен объединиться с Россией, отказаться от ее сдерживания, отменить санкции и забыть о конфликте с Украиной. Россия должна на равных с США решать судьбы мира, а Запад должен признать ее интересы в бывшем СССР и Центрально-Восточной Европе.

Логика российского руководства понятна. Массированное военное вторжение в Украину чревато слишком большими издержками, привести к власти в Киеве пророссийские силы не удалось, а вместо Новороссии России приходится иметь дело с пресловутыми Л/ДНР, которых часто и со всем на то основанием называют в России *чемоданом без ручки*. *Поворот на Восток* не состоялся: Китаю и другим восточноазиатским странам не нужны российские углеводороды в тех объемах, которые пытается им продать Москва. Ситуация на мировых рынках нефти и газа никакого оптимизма в России не вызывает. В результате холодной войны с Западом Кремль получил экономические санкции, консолидировал НАТО и столкнулся с перспективой гонки вооружений. С тем, чтобы прервать эту цепь неприятностей, была предпринята интервенция в Сирии. В случае ее успеха в России надеются выйти из изоляции, спасти своего незадачливого союзника, Б. Асада и утвердиться на Ближнем Востоке как влиятельная военно-политическая сила. И тогда перспектива стратегических договоренностей с Западом могла бы, как считают многие российские и некоторые западные эксперты, обрести практические

очертания, если, разумеется, инцидент с уничтоженным российским самолетом в Сирии не перерастет в полномасштабный военно-политический кризис между Россией и НАТО.

Впрочем, пока это — только перспектива, реализация которой весьма сомнительна. Несмотря на террористические акты в Париже, лидеры ведущих западных стран договорились продлить санкции против России еще на полгода. Они также согласились, что «все элементы Минских соглашений должны быть выполнены, прежде чем можно будет рассмотреть облегчение санкций» [21]. Иными словами, было сказано *нет* российским попыткам добиться отмены санкций или, по крайней мере, их смягчения в обмен на частичное выполнение Минских соглашений без передачи Украине контроля над границей. Продление санкций означает, что о *новой Ялте* речь пока идти не может. Их отмена — ключевой элемент стратегической сделки России и Запада и просто нормализации отношений между ними.

Но одновременно в США и Европе усилились голоса тех, кто поддерживает сотрудничество с Россией в борьбе с терроризмом. Среди них — президент Франции Ф. Олланд. Его понять можно. Он должен изобличить и наказать террористов, устроивших бойню в Париже, и их вдохновителей, а также предотвратить повторение чего-либо подобного в будущем. Для этого необходимо использовать любую возможность, договариваться не только с Кремлем, но и с самим дьяволом. В противном случае его и его партию ожидает политическая катастрофа. Избиратели этого не прощают. Однако от Франции и ее президента мало что зависит во взаимоотношениях России и Запада. Можно, например, вспомнить, что во время первой холодной войны Франция, особенно во времена де Голля, занимала весьма своеобразную позицию в отношении бывшего СССР, что, правда, не слишком сильно сказывалось на тогдашних международных отношениях.

Но события осени 2015 г. ставят и более широкий вопрос: насколько вообще справедливы аналогии между нынешней ситуацией и Второй мировой войной, когда ведущие демократические государства были вынуждены объединиться со сталинским режимом в борьбе против общей угрозы? Может ли сотрудничество России и Запада против международного терроризма, пока скорее потенциальное, чем реальное, привести к *новой Ялте*?

Нацистская Германия представляла для Великобритании смертельную опасность, а для США — большую угрозу, чем СССР, бывший до войны сугубо региональной державой. Союз с СССР для Лондона был необходимостью, а для Вашингтона, вовлеченного в изнурительную войну на Тихом океане, оптимальной стратегией. Но *Исламское государство* и подобные ему террористические группировки при всей своей омерзительности все же уничтожить европейские государства и США не могут. Кроме того, в Ялте и Потсдаме США и Великобритания были вынуждены согласиться с разделом Европы на сферы влияния во многом потому, что многомиллионные сталинские армии расположились в самом сердце этого континента; коммунисты входили в правительства Италии и Франции, были готовы *взять Париж по телефону* и воевали в Греции против близкого США и Великобритании правительства. Иными словами, Сталин в то время действовал с позиции силы.

Возможности России сегодня совершенно иные. Новая холодная война может вылиться в ядерный катаклизм в Европе, но победить НАТО и даже одну только Турцию в неядерном конфликте Россия не способна, как и не в состоянии решающим образом повлиять на исход войны в Сирии. Наконец, российская внешняя политика в последние два года поставила под вопрос международный порядок, основанный на праве, неприменении силы, мирном разрешении споров и нерушимости границ. Пережив две катастрофические мировые войны, европейские государства осознали, что только безусловное соблюдение этих норм может избавить континент от новой войны, последствия которой трудно себе представить. В этих условиях потенциальная *антиигиловская* коалиция в Сирии, включающая в себя Россию, если она состоится, вряд ли приведет к радикальному пересмотру сложившихся отношений Москвы с ведущими западными странами. По сути дела, в обмен на удовлетворение своих геополитических амбиций российское руководство может предложить только обещание не угрожать применением ядерного оружия. Но для того, чтобы такое обещание оказалось убедительным, требуется восстановить доверие между Россией и Западом, подорванное в результате украинского кризиса.

МИГРАЦИОННЫЙ КРИЗИС

Миграционный кризис 2015 г. в Европейском союзе вызвал бурную, во многом эмоциональную реакцию в средствах массовой информации, аналитическом и политическом сообществах в Европе и в России. Четко проявились две полярные точки зрения. Первая — европейцы обязаны сделать все возможное, чтобы помочь беженцам, покинувшим свои страны из-за войн, репрессий, экономических и природных бедствий, обеспечить им защиту и более или менее сносные условия существования. Этого, утверждают сторонники данной точки зрения, требует принцип солидарности, одна из основных ценностей современной европейской цивилизации. Вторая — не отрицая необходимости принимать в странах Европы людей, спасающихся от войн или подвергающихся репрессиям в силу своих политических взглядов или религиозных убеждений, требует ограничить беженцам материальные пособия и сократить до минимума приток в Европу инокультурных экономических мигрантов, прежде всего из Африки и мусульманского мира. В России же широкое распространение получила поддерживаемая официальной пропагандой мысль о том, что нынешний *кризис беженцев* и вообще миграционная политика Европейского союза — один из ключевых признаков *заката Европы*, ее глубокой цивилизационной слабости и неспособности справится с вызовами современного мира.

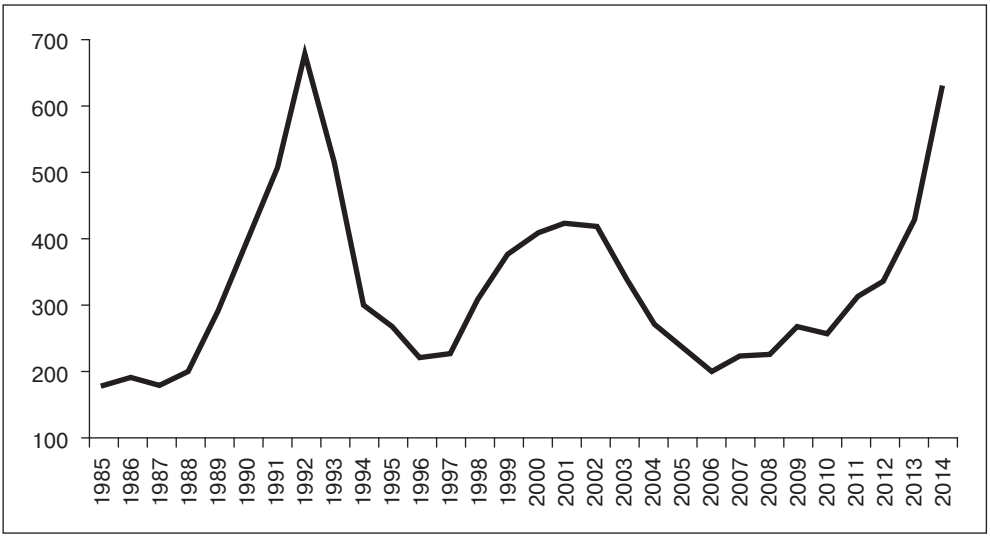
Фраза «Европу накрыла невиданная ранее, подрывающая ее единство волна беженцев» с унылым постоянством повторяется в СМИ и многих аналитических материалах. Это, мягко говоря, свидетельство плохой успеваемости по истории, в том числе новейшей. Не затрагивая здесь великие переселения народов, крестовые походы, войны древности и Средневековья, вспомним, например, что после Второй мировой войны из Восточной Европы в течение нескольких месяцев были изгнаны 14 млн этнических немцев, из которых около двух миллионов погибли по дороге[22]. Это не первый и, увы, не последний случай, когда за преступления правящей клики расплачиваются миллионы рядовых граждан. Но так или иначе, в конце 1940-х гг. немцы получили первый тяжелый опыт приема многих миллионов

беженцев и на практике осознали, что требования солидарности, тогда по отношению к соотечественникам, — отнюдь не пустая риторика. В весьма сложной ситуации оказался Израиль в 1990–92 гг., когда туда переселилось около одного миллиона выходцев из бывшего СССР. Тем не менее, и Германия после Второй мировой войны, и Израиль смогли решить крайне сложные проблемы, возникшие в результате переселения на их территории крупных масс нового населения.

Далее, если исходить не из фантазий журналистов и людей, называющих себя экспертами, а из сравнительно объективных данных европейской статистики, то можно увидеть, что за последние 30 лет Европа пережила, по крайней мере, две крупных волны беженцев. Первая — в конце 1980-х — начале 90-х годов, порожденная всплеском локальных конфликтов в зоне *третьего мира*, а также прогрессирующим распадом так называемой социалистической системы. В частности, по мере ослабления репрессивной политики в странах-сателлитах СССР в Восточной Европе, оттуда нарастал поток беженцев на Запад. Свой вклад вносили массы беженцев из бывшей Югославии в результате начавшихся там войн. Вторая волна в конце 1990-х годов, уступавшая первой, была, как и та, вызвана во многом войнами в бывшей Югославии. Не углубляясь более в историю, стоит лишь подчеркнуть, что утверждения о *невиданной ранее* волне беженцев никак не согласуются с реальностью.

Статистика не подтверждает также широко распространенное мнение о том, что взрывной рост беженцев в страны ЕС в 2012–2015 гг. вызван главным образом гражданской войной в Сирии и конфликтами в ряде других стран *третьего мира*. Большинство заявлений о предоставлении убежища в странах ЕС — 60–65 процентов — было в эти годы подано выходцами из стран со стабильной или относительно стабильной политической обстановкой, в которых нет или почти нет значимых вооруженных конфликтов, ставящих под угрозу жизнь основных групп населения.

Количество обращений о предоставлении убежища в ЕС в 1985–2014 гг. (тыс. чел)[23]



Количество заявлений о предоставлении убежища в странах ЕС, 2012–2015 (тысяч заявлений по крупнейшим странам и регионам исхода) [24]

		2012	2013	2014	2015			Σ
					1st Q	2nd Q	Σ	
	Всего в ЕС	336	432	627	185	213,2	398,3	1793,3
В том числе из	**Западные Балканы**	51,6	71,8	106,5	67,0	36,9	103,9	333,8
	Сирия	23,5	50,8	122,1	29,3	43,9	73,2	269,6
	Афганистан	26,2	26,3	41,3	12,2	27	39,2	133,0
	Россия	23,4	41,3	19,6	3,1	3,6	6,7	91,0
	Пакистан	19,3	20,9	22,1	5,3	8,8	14,1	76,4
	Сомали	12,8	18,7	16,9	3,4	5,3	8,7	57,1
	Иран	12,4	12,8	10,8	2,3	3,1	5,4	41,4
	Ирак	11,3	11,2	21,3	7,3	13,9	21,2	65,0
	Эритрея	5,9	14,7	36,9	3,2	9,7	12,9	70,4
	Σ	180,7	261,4	386,8	131,6	150,6	285,3	1137,7
	Доля в потоке	54%	60%	62%	71%	70%	71%	63,4%

В частности, в последние три с половиной года гражданами государств Западных Балкан (Албания, Босния и Герцеговина, Косово, Македония и Сербия), было подано около 334 тыс. таких заявлений, что составило почти 19% от их общего количества. Среди них лидирует по этому показателю Косово. Нельзя не заметить, что на третьем месте среди государств, граждане которых запросили убежища в ЕС, находится Россия. Другое дело, что возрастает доля лиц, подавших заявление о предоставлении убежища в странах ЕС, из государств, пораженных внутренними конфликтами (Сирия, Афганистан, Ирак) или управляемых террористическими режимами (Эритрея). В 2012 — первой половине 2015 г. 538 тыс. граждан этих четырех государств обратились с такой просьбой к правительствам стран ЕС, что составило 30% от общего числа попросивших убежища. Из них примерно половину составили граждане Сирии. Их доля в общем потоке беженцев, ищущих убежища, возросла с 7% в 2012 г. до почти 20% в 2014 г.

Уже упоминавшийся исторический опыт показывает, что появление одного-двух миллионов беженцев в Европейском Союзе, население которого составляет примерно 500 млн человек, само по себе серьезной, тем более цивилизационной угрозы для Европы не представляет. Нынешний миграционный кризис обусловлен в основе своей техническими причинами. В частности, так называемый регламент *Дублин II*, заменивший в 2003 г. Дублинскую конвенцию, возлагает ответственность за рассмотрение ходатайства лица, ищущего убежища, на одно и только одно государство — член ЕС, а именно то, в которое после первого пересечения внешней границы ЕС прибыл потенциальный беженец. Иными словами, основное бремя по содержанию сотен тысяч новых беженцев и рассмотрению их ходатайств должно было лечь на несколько государств, в первую очередь Италию и Грецию, которые явно не были к этому готовы. Это положение вошло также в противоречие с требованиями основной массы беженцев, которые стремятся в Германию

и Швецию. Далее, пограничные службы стран ЕС и особенно государств, входящих в Шенгенскую зону, оказались совершенно неготовы к сдерживанию десятков и сотен тысяч чеовек, по сути дела, нелегально пересекающих границу. И, наконец, в ЕС удовлетворяется от 40 до 45% прошений о предоставлении убежища, но при этом возможности входящих в него государств по депортации тех, кому в этом статусе было отказано, несопоставимы с количеством лиц, подлежащих депортации. При всей серьезности этих проблем их решение требует пересмотра некоторых юридических процедур и дополнительных расходов, но не смены установившихся в Европе базовых ценностей и принципов.

РЕГИОНАЛЬНЫЕ И МЕСТНЫЕ ВЫБОРЫ В УКРАИНЕ

25 октября 2015 г. в Украине состоялись региональные и местные выборы, политическое значение которых заведомо серьезнее, чем вопрос о составе областных и городских выборных органов власти. Медленное продвижение реформ, прежде всего, в сфере борьбы с коррупцией, исключительно сложное экономическое положение, продолжающийся конфликт на востоке и непреодоленный шок от потери Крыма вызвали в украинском обществе усиливающееся недовольство как исполнительной, так и законодательной властями, сформированными после крушения режима Януковича. В этих условиях многие эксперты, особенно в России, ожидали нарастания реставрационных настроений, создающих условия для возвращения к власти сил, потерпевших поражение в начале 2014 г. Эти ожидания не оправдались. Итоги выборов свидетельствуют, что *Оппозиционному блоку*, возникшему на развалинах *Партии регионов*, не удалось взять реванш.

Итоги региональных и местных выборов в Украине 25 октября 2015 г. [25]

Партия/блок	% голосов	Примечания
Блок Порошенко	19,5	
Батькивщина	12,2	Лидер — Ю. Тимошенко
Оппозиционный блок	10,5	
УКРОП	7,4	Партия, близкая к И. Коломойскому
Самопомощь	6,4	
Возрождение	5,5	Партия, близкая к И. Коломойскому
Свобода	6,9	
Радикальная партия	6,8	Лидер — О. Ляшко
Наш край	44,4	Партия, близкая к П. Порошенко
Аграрная партия	3,2	Партия, близкая к П. Порошенко

Вместе с тем, итоги этих выборов показывают, что политический пейзаж в Украине претерпевает заметные изменения. Так, потерпел крушение *Народный фронт* во главе с А. Яценюком и А. Турчиновым, одержавший весомую победу на парламентских выборах 2014 г. Его избиратели в большей своей части перешли к *Батькивщине* и двум новым партиям — *УКРОПу* и *Самопомощи*. Появились новые

лидеры общенационального масштаба, прежде всего мэр Львова А. Садовый. Важную роль на политической арене принадлежит одному из крупнейших украинских олигархов И. Коломойскому, сумевшему в 2014 г. самыми решительными мерами остановить пророссийские силы в ключевой Днепропетровской области. И, пожалуй, самое главное — нарастающее недовольство нынешней властью приводит к постепенному укреплению реформистских сил, выступающих за радикальное обновление украинских политической и экономической систем и сближение с Европой.

***

Противоречивые, динамичные, в чем-то хаотичные процессы, происходящие в последние год-два на мировой арене, показывают, что евроатлантическая цивилизация не нашла адекватный ответ на усиливающееся влияние сил и кругов, пытающихся остановить и повернуть вспять социально-политическую и экономическую модернизацию. Это, естественно, приводит к нарастанию конфликтности в международной политике, преодоление которой требует обновления концептуальных подходов и моделей, определяющих внешнюю и военную политику США и Европейского союза. Что же касается российской внешней политики, то, пожалуй, наиболее точный вывод был сделан В. Фроловым в короткой, но очень важной статье *Внешняя политика. Дипломатия освобождения* (имеется в виду освобождение от необходимости соблюдать международные правила, якобы сформированные без участия России после проигрыша в холодной войне, — что, мягко говоря, не совсем так — и направленные на сдерживание претензий РФ на ведущую роль в мире). Он пишет:

«Впервые в постсоветской истории внешняя политика России оторвана от экономических интересов и возможностей страны. Они оттеснены на задний план, а некоторые внешнеполитические успехи наносят ущерб экономике. Понятно, что бесконечно так продолжаться не может и будет произведена перекалибровка в пользу экономических интересов. Тогда станет понятна реальная цена *дипломатии освобождения*» [26]

Юрий Федоров

ГЛАЗАМИ КОНСЕРВАТОРА: СИРИЙСКИЙ ПРОЦЕСС КАК ЗЕРКАЛО БУДУЩЕГО

ВМЕСТО ВВЕДЕНИЯ: ЕЩЕ РАЗ К ВОПРОСУ О *ТОЧКЕ БИФУРКАЦИИ*

Хаос... Это слово повторяют теперь все политики и аналитики применительно практически к любой значимой точке земного шара. И к Ближнему Востоку, и к Северо-Восточной Азии, и к Юго-Восточной Азии, и к Европе, на наших глазах захлестнутой волнами беженцев с понятными последствиями, в том числе в сфере безопасности. Дымок от назревающего хаоса в Центральной Азии уже стал ощущаться всеми. И даже — не поверите — местными *великими сердарами*. Островками стабильности в этом мире хаоса пока возвышаются водимая железной рукой Ким Чен Ына Северная Корея и США, которых многие *злые языки* упрекают в том,

лидеры общенационального масштаба, прежде всего мэр Львова А. Садовый. Важную роль на политической арене принадлежит одному из крупнейших украинских олигархов И. Коломойскому, сумевшему в 2014 г. самыми решительными мерами остановить пророссийские силы в ключевой Днепропетровской области. И, пожалуй, самое главное — нарастающее недовольство нынешней властью приводит к постепенному укреплению реформистских сил, выступающих за радикальное обновление украинских политической и экономической систем и сближение с Европой.

***

Противоречивые, динамичные, в чем-то хаотичные процессы, происходящие в последние год-два на мировой арене, показывают, что евроатлантическая цивилизация не нашла адекватный ответ на усиливающееся влияние сил и кругов, пытающихся остановить и повернуть вспять социально-политическую и экономическую модернизацию. Это, естественно, приводит к нарастанию конфликтности в международной политике, преодоление которой требует обновления концептуальных подходов и моделей, определяющих внешнюю и военную политику США и Европейского союза. Что же касается российской внешней политики, то, пожалуй, наиболее точный вывод был сделан В. Фроловым в короткой, но очень важной статье *Внешняя политика. Дипломатия освобождения* (имеется в виду освобождение от необходимости соблюдать международные правила, якобы сформированные без участия России после проигрыша в холодной войне, — что, мягко говоря, не совсем так — и направленные на сдерживание претензий РФ на ведущую роль в мире). Он пишет:

«Впервые в постсоветской истории внешняя политика России оторвана от экономических интересов и возможностей страны. Они оттеснены на задний план, а некоторые внешнеполитические успехи наносят ущерб экономике. Понятно, что бесконечно так продолжаться не может и будет произведена перекалибровка в пользу экономических интересов. Тогда станет понятна реальная цена *дипломатии освобождения*» [26]

Юрий Федоров

ГЛАЗАМИ КОНСЕРВАТОРА: СИРИЙСКИЙ ПРОЦЕСС КАК ЗЕРКАЛО БУДУЩЕГО

ВМЕСТО ВВЕДЕНИЯ: ЕЩЕ РАЗ К ВОПРОСУ О *ТОЧКЕ БИФУРКАЦИИ*

Хаос... Это слово повторяют теперь все политики и аналитики применительно практически к любой значимой точке земного шара. И к Ближнему Востоку, и к Северо-Восточной Азии, и к Юго-Восточной Азии, и к Европе, на наших глазах захлестнутой волнами беженцев с понятными последствиями, в том числе в сфере безопасности. Дымок от назревающего хаоса в Центральной Азии уже стал ощущаться всеми. И даже — не поверите — местными *великими сердарами*. Островками стабильности в этом мире хаоса пока возвышаются водимая железной рукой Ким Чен Ына Северная Корея и США, которых многие *злые языки* упрекают в том,

что США, мол, этот хаос и создали. Но давайте отмотаем на некоторое время назад и посмотрим, КАК это все могло бы быть. Ведь все же могло быть иначе.

В мае 2014 г. ЕС и США могли принять решение о признании итогов референдума в Крыму. Могли. Нужна была лишь политическая воля и понимание неизбежности партнерства с Россией. Россию бы *обременили* долгосрочной — лет на 10–15 — скидкой на газ для Украины и единовременной выплатой некоторого вспоможения Киеву (миллиардов 30–35 долларов), а также потребовали бы торжественных обещаний полной неприкосновенности оставшейся территории. И не было бы бойни на Донбассе. И пассажиры злополучного малазийского Боинга остались бы живы. И россияне по-прежнему пребывали бы в убеждении о том, что они с украинцами — братский народ.

Весной и летом 2014 г. Б. Обама не стал бы убеждать саудовских принцев максимально провалить цену на нефть, а озаботился бы рентабельностью собственной нефтяной промышленности. Нефть осталась бы в комфортном коридоре 65–74 долл. США за баррель, а российские нефтедоллары исправно подпитывали бы американские и британские банки. Не было бы тревожного ожидания *домино* банкротств среди сланцевых инвесторов, которое толкает США к различным нефтяным авантюрам, в том числе с нефтью, прямо скажем, сомнительного происхождения, да и к становящимся уже откровенными махинациям со статистикой.

С Москвой можно было бы как минимум говорить о плавном переезде Б. Асада на одну из рублевских дач и поддержке плавного перехода власти к *оппозиции с человеческим лицом*, которую являл т. н. *Южный фронт*, нашпигованный американскими и израильскими инструкторами и оружием. Нет, конечно, резня христиан и шиитов все равно бы произошла, но о ней, вероятно, мало кто смог бы узнать. Ведь европейскому и американскому обывателю — разумеется, в рамках *свободы слова* — нельзя показывать то, что может ранить его толерантное сердце. Вряд ли бы в Европу потек такой поток беженцев. Он был бы существенно меньше, да и проходил бы, вероятно, без той драмы, которую мы регулярно наблюдаем по телевизору. Да и ИГ не стали бы раскручивать и накачивать вооружением до такой степени, как это было в 2014–2015 гг. Россияне, погибшие при подрыве аэробуса над Синаем, тоже остались бы живы. Думаю, террористических актов в Париже вряд ли удалось бы избежать, но, возможно, их масштаб был бы меньше.

Москва продолжала бы бесконечный торг с Анкарой об условиях экономического сотрудничества, упорно делая вид, что не замечает ускоряющейся исламизации Турции и сращивания турецких правящих кругов с исламистским криминалом. А также активизации пантюркистских кругов в Поволжье и на Северном Кавказе.

Россия бы сохранила — при всех публичных декларациях — дистанцированность от КНР в военно-стратегических вопросах. И вряд ли бы после этого Пекин был столь активен, если не сказать агрессивен, в территориальных коллизиях со своими соседями. Ведь только появление полноценного российского стратегического ядерного зонтика на фоне юбилейного парада в Пекине позволяет Поднебесной изображать из себя фигуру, равную США: с точки зрения военно-стратегических возможностей США и КНР находятся, мягко говоря, на разных стадиях развития.

В России бы всерьез обсуждали инновации и возвращение к власти коалиции либералов в различных конфигурациях, приводя в пример соседнюю Украину, которая бы еще оставалась *стратегическим партнером*. И, вероятно, живой Б. Немцов собирал бы каждый месяц какое-то количество протестующих на радость московским корреспондентам западных агентств.

Это и многое другое вполне могло бы быть. Только надо было сказать два слова: **«Крым — ваш».**

Но не случилось. Увы. Побрезговали наши западные партнеры, понадеялись на то, что Россия быстро сломается. В действительности эти надежды свидетельствовали о том, что они совершенно не представляли себе страну, которую собрались политически побеждать.

А дальше началось то, что называется в социальной философии *сила вещей*, из чего, собственно и вырос нынешний хаос. Как говорится, не захотели *по-хорошему*, будет, как будет. Причем только наивный может считать, что этот хаос носит чисто политический или военный характер. Нынешний *хаос*, который и не хаос вовсе, а кризис с неопределившимся пока вектором развития, — это комплексное явление, которое повлечет за собой передел всего или почти всего операционного пространства мировой политики и экономики.

Мораль: момент истины для любого политика — его способность увидеть ту самую *точку истинной бифуркации*, которая, возможно, случается лишь раз в жизни. А, бывает, и не случается. Точку, когда политический выбор будет иметь скорые, но долгосрочные последствия. Увы, ни один из современных действующих западных политиков этим умением не обладает. И это надо иметь в виду всем. И нам, и политикам по обе стороны Атлантики.

ГЛОБАЛЬНЫЙ ТЕРРОРИЗМ КАК ПОБОЧНОЕ СЛЕДСТВИЕ ГЛОБАЛИЗАЦИИ И СЕТЕВИЗАЦИИ

Безусловно, крупнейшим событием последних месяцев стала цепь террористических актов, которая прокатилась от Парижа до Африки, в которой наиболее крупными были подрыв российского самолета над Синаем и бойня — по-другому не скажешь — в Париже. То, что мы увидели, это не привычный нам терроризм. Он не то чтобы совсем новый, но сильно отличающийся от основной массы террористических действий последнего десятилетия. Причем не столько своей жестокостью и масштабностью (в конечном счете, теракты 11 сентября 2001 г. в данном случае задали определенную планку, которую непросто будет преодолеть даже ИГ). Новелла последних террористических актов — это некая *новая системность*, новый организационный уровень. Его же следует считать наиболее значимой террористической угрозой.

Нацеленность террористических действий на создание, в первую очередь, паники в обществе. Не на достижение неких политических или экономических целей, не на оказание давления на политическую элиту, а именно на создание паники с нанесением максимального ущерба, прежде всего психологического. Хотел бы ошибиться, но, кажется, исламские террористы нащупали в европейских обществах ту идеологическую и психологическую трещину, расширяя которую, можно усугублять и без того заметное безволие европейских властей. Поэтому заявле-

ния о бессмысленности террористических актов в Париже совершенно не верны. В них как раз есть большой, можно сказать, стратегический смысл.

Активное взаимодействие и даже сращивание с криминалом. След от террористических актов во Франции привел в абсолютно криминализированные кварталы Парижа и Брюсселя, что очень о многом говорит. Европейский исламский терроризм естественным образом встроен в экономическую систему современного Евросоюза, который годами смотрел сквозь пальцы на интеграцию мигрантов в общество именно через криминальные каналы. В расчете, видимо, на *боснийский* опыт, когда бывших боевиков, в частности радикальных исламистов, отваживали от террористической деятельности путем вовлечения в разного рода криминальные бизнесы. Например, контрабанду сигарет и тому подобные шалости. Ну, то есть, пытались заменить *тяжелые* наркотики на *легкие*. Такая замена — вообще известный европейский стиль. И, поверьте, наши европейские партнеры будут пожинать последствия этой близорукости еще долгие годы.

Стал полноценной и апробированной операционной реальностью *распределенный, сетевой* терроризм. Этот принцип неоднократно описывался в профессиональной литературе, но на практике встречался сравнительно редко. Та же *Аль-Каида* даже по официальной версии представляла собой вполне структурированную и организационно консолидированную организацию. В данном же случае вообще сомнительно, что присутствовало какое-то централизованное управление, во всяком случае, на операционном уровне. Можно даже допустить, что не было полноценного сигнала к действию, а решение принималось инициативно или по команде относительно случайного человека.

Мы столкнулись с явлением, которое можно определить как *спящий терроризм*. То есть на постоянной основе могут существовать организованные ячейки, которые в обычной жизни никак не проявляются. Триггером становится сигнал от 1–2 человек. Здесь главная угроза даже не в том, что предельно сокращается время на подготовку террористического акта, а в том, что, с учетом масштабов и слабой контролируемости миграционных потоков в Европу в последние годы таких ячеек может быть бесконечное множество. И обычные, проверенные методики борьбы с терроризмом тут вряд ли помогут. Помните, что рефреном говорили про парижских террористов? *Они были обычными людьми*. И, вероятно, это совершенная правда. Для сегодняшней Европы они и правда были *обычными* людьми.

Мы столкнулись с явлением, которое можно назвать *контр-технологический терроризм*. В последние годы многие страны и на Западе, и на Востоке вкладывали колоссальные средства в создание разного рода технологических средств для превентивного выявления террористов и предотвращения террористических актов. Крупные европейские города буквально нашпигованы средствами видеофиксации, детекторами. Прослушивание телефонных разговоров и контроль электронной почты приобрели фантасмагорические масштабы, позволяющие говорить практически об отсутствии полноценной частной жизни. И все это оказалось бесполезным против кустарных бомб из селитры и старых АК, купленных у брюссельских бандитов. Объем инвестиций в технологизацию борьбы с терроризмом, похоже, оказался совершенно непропорционален полученному результату. И тут закрадывается другое смутное подозрение. А что, если не только инвестиции в борьбу с терроризмом, но и вся технологизация военной сферы,

которая происходила последние 25 лет, была тупиковым направлением развития военной мысли? И как тут не вспомнить формулу полузабытого военного теоретика *из отмороженных белогвардейцев* Е. Месснера о *мятежвойне* как о полноценной глобальной силовой парадигме[27]. Правда, он связывал это с деятельностью Коминтерна. А Коминтерн отличался от новых мятежников, прежде всего, претензией на централизацию и смертностью от руки И. Сталина. У новых террористов этих уязвимостей нет.

Иными словами, хотя с тактической точки зрения последние террористические акты не несут в себе чего-то принципиально нового, в стратегической перспективе в них очень много очень нового. Нового и очень опасного. Более того, создается впечатление, что в стремлении *вбомбить ИГ в каменный век* мы начинаем упускать именно этот, наиболее опасный стратегический момент. Проблема заключается в том, что *новый* терроризм совершенно необязательно будет и дальше проявляться в связи с Ближним Востоком. Есть куда более экономически привлекательные регионы, которые также стоят на пороге начала силовой реструктуризации. Например, Азиатско-Тихоокеанский регион.

УМЕНИЕ *ДЕРГАТЬ ЗА УСЫ.* НОВАЯ ПАРАДИГМА ГЛОБАЛЬНЫХ ВОЕННО-ПОЛИТИЧЕСКИХ ОТНОШЕНИЙ

Если последовательно читать новости, касающиеся развития военно-политической ситуации в мире, создается впечатление, что крупнейшие геополитические силы современности целенаправленно ведут дело к военному столкновению. Патрулирование вблизи границ, военные учения со стрельбой в направлении границы, взаимные перехваты самолетов и кораблей, облеты спорных территорий, порой резкие, *на грани фола* заявления политических лидеров. С точки зрения формальной логики международных отношений, такие действия каждодневно подтачивают международную стабильность, что привело бы в ужас любого политика времен *холодной войны*, не исключая и Н. Хрущева. И все это происходит на фоне кардинально сократившейся военно-силовой прозрачности в мире, а также институциональной недостаточности в сфере военно-политических отношений.

На этом фоне важным, причем не в тактическом, а уже в стратегическом плане моментом являются российско-американские договоренности об избегании военных столкновений авиации в небе над Сирией. Казалось бы, мелочь, но она не просто крайне важна, но и откровенно индикативна с точки зрения сегодняшнего уровня отношений между Россией и США. А уровень этот характеризуется углубляющимся стратегическим недоверием. И в таких условиях даже тактическое взаимодействие на формализованной базе способно многое изменить. Хотя, конечно, надо изначально признать, что выстраивание новых отношений в военно-политической сфере между Россией и США придется начинать с очень низкой точки, вероятно, с отрицательных значений.

Но ведь дело тут не только в России и США. Ровно то же самое можно сказать о бесчисленных взаимных жестких заявлениях по ситуации в Южно-Китайском море, а главное, действиях, которые также балансируют на тонкой грани между *военными демонстрациями* и *военными провокациями*.

То есть все, подчеркнем, все крупные военные (правильнее говорить, вероятно, военно-силовые) державы мира сознательно — маловероятно, что в руководстве сразу всех ключевых стран мира сидят откровенные безумцы, — снижают уровень международной стабильности, подводя ситуацию к той опасной границе, когда одна ошибка может привести к совершенно неконтролируемым последствиям. Но что это, если не безумие?

Вероятно, мы имеем дело с некоей самозащитной реакцией политических и военных лидеров современного мира, которые, утратив институциональные ориентиры в области безопасности — согласимся, что работающих институтов в этой сфере человеческой деятельности больше нет, — пытаются такого рода действиями *пометить* границы своей операционной территории. Причем, повинуясь естественному для политиков инстинкту, они стремятся хотя бы слегка *залезть* на территорию партнера и тем более оппонента. Просто обратите внимание на географию силовых демонстраций.

Конечно, есть существенная разница между поведением России, которая открыто демонстрирует свою способность к эскалации (примером чему является применение в локальном конфликте стратегических сил) и ее контролю, и усилением *предупредительной* риторики со стороны Китая, попытками Израиля расширить границы своего воздушного контроля в восточном Средиземноморье и стыдливыми демонстрациями силы (силы ли?) со стороны США в Южно-Китайском море, которые тут же сопровождаются заходом в какой-то китайский порт, чтобы Поднебесная не сильно обиделась. Да, все это — существенно отличающиеся примеры, но цель их примерно одна и та же: понять, *как еще* можно использовать военную силу в современном мире. Вероятно, старые модели применения военной силы, характерные для периода *постбиполярности,* уже утратили актуальность.

В целом, необходимо констатировать, что степень управляемости военно-политических процессов в современном мире существенно сократилась, что естественно в условиях если не распада, то существенного ослабления основных институтов, которые в той или иной степени регулировали глобальную и региональную военную деятельность. В конечном счете, трагический и крайне тревожный эпизод с уничтожением турецким истребителем российского самолета Су-24 М в небе над Сирией свидетельствует о тех крайне опасных последствиях, с которыми могут столкнуться государства в новом мире, когда один политик — в данном случае Т. Р. Эрдоган — утрачивает ощущение границ допустимого в демонстрации силы. Этот эпизод, в действительности, крайне важен. Он может послужить либо к возникновению новых *институтов,* которые будут предотвращать подобные события, либо спровоцировать исключительно опасную дестабилизацию международной обстановки сперва на *ближневосточном театре*, а затем и в более широком контексте. Главное, что стало очевидно: в современной системе силовых взаимоотношений *защиты от дурака* более не существует.

Но это понимание еще больше обостряется растущим ощущением не то чтобы политической безответственности, но явной глобальной политической несдержанности, характерной для все большего числа политиков. Политическая диффамация становится одним из легитимных инструментов внешней политики.

Правда, иногда случаются постыдные моменты, как, например, с Б. Обамой, которому пришлось конструктивно разговаривать с В. Путиным — лидером страны,

только недавно объявленной наряду с ИГ одной из главных угроз миру, экономику которой Б. Обама так героически *порвал*. Но и это тоже свидетельство кризиса глобальной политической институциональности, прежде всего, в той части, которая определяет пределы дозволенного в поведении сторон.

Значимость договоренностей, достигнутых по координации действий в Сирии, состоит прежде всего в том, что они становятся первыми ростками еще не доверия, но хотя бы понимания между странами, которые оказались вовлечены одновременно сразу в несколько локальных военно-политических ситуаций на фоне ухудшающихся двухсторонних отношений. Хотя надеяться на то, что из этих тактических договоренностей вырастет что-то действительно стратегическое, конечно, не приходится. Но хоть что-то.

В конечном счете, именно способность управлять эскалацией и не смешивать военные демонстрации с решением частных политических проблем и отделяет серьезного участника системы международных отношений от несерьезного, неспособного вести предметный разговор с партнерами и соблюдать обязательства.

СИРИЯ В ГЛОБАЛЬНОМ КОНТЕКСТЕ

Ситуация вокруг Сирии развивалась политически стремительно, а военно-политически — по-восточному неспешно. Увлекшись вопросами стратегии и тактики, мы, кажется, упускаем из вида, что этот кризис имеет и ярко выраженный стратегический фон, и эффект.

Ключевой момент во всей ситуации вокруг Сирии представляет собой некую концептуальную петлю. Эта петля началась в тот момент, когда прозападный, в сущности, режим решили свергнуть без какой-либо жгучей необходимости, просто в рамках переформатирования пространства, которое перестало отвечать текущим геополитическим задачам. Эта петля еще больше закрутилась в тот момент, когда режим вопреки давлению не сломался, а стал активно защищаться. Петля затянулась еще туже, когда созданную первоначально для пропагандистских целей *зонтичную* структуру пришлось превращать в политический фактор, а затем в основу переформатирования региона. Эта петля превратилась в узел, когда *виртуальная реальность*, имитация *борьбы с ИГ* стала определять реальную политику ключевых государств мира, совершенно не стыкуясь с тем, что начало происходить *на земле*. Узел этот пришлось разрубать силой российской авиации, дабы вновь совместить политику, ставшую уж слишком виртуальной, с объективной реальностью.

Но, кажется, имеет смысл остановиться на тех *прото-уроках* — извлечение полноценных уроков потребует более серьезного осмысления — которые дала нам история *сирийского* конфликта.

Первое. Главная проблема, которая и порождает нестабильность в современных международных отношениях, — это отсутствие политической воли. А заменой политической воли выступает риторика. Думаю, много кто отметил, что чем больше от политика исходит риторики, тем меньше у него на деле политической воли. Но попытка заменить агрессивной риторикой и информационными технологиями политическую волю уже породила немало *серых зон* в мировой политике и продолжит порождать их и впредь. Одной из таких *серых зон* стала пресловутая

территория ИГ. Рискну предположить, что второй станет ситуация вокруг *сладкой парочки* мировой политики — Саудовской Аравии и Катара. Ибо у Запада не хватает политической воли для того, чтобы приструнить эти зарвавшиеся *не по чину* государства. Это грозит большими и неприятными глобальными осложнениями. Есть в этой ситуации и оборотная сторона: современная мировая политика построена по принципу *кто первый встал, того и тапки*. То есть тот, кто первый проявляет политическую волю, получает неоспоримые политические дивиденды. Как Россия, которая первой стала по-настоящему бороться с ИГ.

Второе. Так называемый *сирийский конфликт* был и продолжает оставаться территорией виртуальной реальности, которая наполнена бесчисленным количеством *фейков*, причем как информационных, так и операционных. Начнем с того, что само название не отражает реальности. Конфликт уже давно перестал быть *сирийским*, а захватывает как минимум несколько других государств, являясь уже не локальным, а классическим региональным конфликтом с элементами внешнего вмешательства. *Сирийский конфликт* показал и колоссальные возможности социального и политического конструирования, и пределы возможностей такого конструирования. Которые — пределы — оказались очень просты и банальны: созданная или финансируемая кем-то сущность всегда обладает значительной автономностью от создателя и реализует свои и только свои интересы. Но главное даже не это. Главное, что процесс социального проектирования можно запустить, но очень сложно остановить.

Третье. *Сирийский конфликт* выявил масштабы *теневых* экономических интересов в глобальной экономике. *Прото-государственность* ИГ, а такая, безусловно, сформировалась на наших глазах, имела весьма солидную экономическую базу, которая в мире была широко востребована. Причем в том числе и в странах, которые считают себя частью глобальной экономики. Например, в Турции. И это неслучайно. Если хотите, *сирийский кризис* показал неизбежность кризиса современной мировой экономики, которая не может одновременно наполняться все более изощренными и мощными регулятивными инструментами и одновременно расширять *теневой* сектор в значимом и полностью глобализированном сегменте мировой экономики. Тут надо отметить, что экономическая база ИГ состояла не только из нелегально добываемой нефти, о чем многократно писалось[28], или предметов античности, любезно поставляемых боевиками в частные коллекции, но и, например, фосфатов. А это существенно более сложный для продвижения на рынке продукт. Однако же, у ИГ получалось. Ну и, конечно, нельзя не отметить, что приговор современной экономической системе вынесло именно ИГ (запрещенная в России террористическая организация), когда начало выпускать собственные деньги и когда их стали принимать не только на территории, которую ИГ захватило.

Четвертое. *Сирийский конфликт* был фактически первым конфликтом современной эпохи, в котором идеология, а не иные факторы (этничность, экономика, политические противоречия) сыграла роль драйвера. Конечно, идеологические факторы были заметны и в вооруженных конфликтах раньше, но они никогда не были решающими. И в *сирийском* конфликте тоже есть и экономика, и политика (хотя в гомеопатических дозах), и этнический фактор. Но главным был все же фактор идеологический. То есть система глобализации, которая не предусматривает никакого идеологического наполнения, треснула настолько, что появилось значимое место для идеологических конструктов весьма сложносочиненного типа (сно-

ска на идеологию ИГ), которые, несмотря на свою ярко выраженную антисистемность, становятся привлекательными.

Пятое. *Сирийский конфликт* стал первым конфликтом, в котором явственно прослеживается фактор цивилизационного разлома. Впервые возникла реальная сила, которая, по крайней мере на политическом уровне (экономические связи и скрытые отношения оставим чуть в стороне, в данном случае это не столь важно), организованно и небезуспешно боролась за то, чтобы перестать быть тем, что именуется *цивилизованный мир*, то есть Запад и его сателлиты. Самое важное в том, что эта парадигма оказалась очень привлекательной. При всем этом *структура* сирийского конфликта существенно отличается от предсказаний С. Хантингтона, поскольку не является в чистом виде этно-религиозной. Раскол по признаку *цивилизационности* оказался гораздо грубее, но одновременно глубже и комплекснее. Мы, вероятно, имеем дело с новым геополитическим феноменом, который еще только предстоит осмыслить в полной мере, но который уже становится фактором глобальной дестабилизации военно-политической обстановки.

Шестое. Прецедент огосударствления *сетевой* организации на базе антисистемной идеологии. Самое опасное в прецеденте ИГ — это не то, что эта организация смогла захватить значимые, в том числе с точки зрения ресурсов, территории. И даже не в том, что она смогла встроиться в экономические потоки. Сомалийские *пираты* тоже вполне успешно глобализировались, а затем монетизировались. Проблема в том, что изначально *сетевая* организация ИГ смогла как минимум выработать в себе зародыш иерархической организационной структуры с вектором развития в сторону государства. Нет, конечно, никаким *прото-государством ИГ* на момент начала российской операции не было, до этого статуса было очень далеко. Почти недостижимо. Но вектор, в том числе и идеологический, на создание именно иерархической структуры был совершенно очевиден.

Наконец, **седьмое.** *Сирийский конфликт* в том виде, как мы его наблюдали последние два года, стал, как это ни странно прозвучит, продуктом отсутствия российско-американского партнерства. Не просто разлад, но отсутствие стратегического взаимопонимания между Россией и США, потеря ощущения *пределов риторики*, а также — в не меньшей степени — игнорирование друг друга, неготовность американской элиты не то чтобы признать, но даже обсуждать новый статус России в мире при неготовности российской элиты системно доказать свой новый статус и демонстрировать возможности и привели к тому, что в трещины российско-американского взаимодействия стали заползать *иные* силы. *Профит* которых заключался именно в эксплуатации напряженности между двумя странами. И, надо сказать, у них это неплохо получилось. Т. Р. Эрдоган под шумок российско-американских разборок сумел построить практически тоталитарную исламистскую империю, вскормленную на нефти ИГ. Что-то подобное уже было в 1980-е, когда *на дрожжах американских денег* для борьбы с советским присутствием зарождалась идея *большого Пакистана*, превратившаяся в движение *Талибан*.

Вопрос, что из этих проявлений особого, если хотите, *пионерного* характера *сирийского конфликта* станет стратегической тенденцией, впрочем, следует оставить открытым. Но то, что конфликт в Сирии и Ираке создал целую *россыпь* весьма опасных прецедентов и обстоятельств, — бесспорно.

НАТО ВО МГЛЕ

Одной из наиболее очевидных коллизий современной глобальной военной политики является практически полное исчезновение НАТО с информационной и операционной арены. В ситуации вокруг Украины НАТО еще проявляло признаки жизни, пусть и в качестве младшего пропагандистского партнера США. Достаточно вспомнить скалькированные с американских заявлений доведенные до пропагандистского предела по форме высказывания Ф. Расмуссена и Й. Столтенберга — они хотели быть *святее* американского президента, но сказать им было особо нечего. Конфликт в Сирии и Ираке для НАТО в принципе не существовал, причем ни с политической, ни с военной точек зрения. Не считать же участием НАТО в конфликте разовые комментарии его Генерального секретаря, да еще, как правило, *не по делу.* Тут даже участием в пропагандистском обеспечении не пахнет.

И это несмотря на декларирование глобального характера интересов Альянса и то, что конфликт развивался в одном из наиболее чувствительных для НАТО регионов мира, в Восточном Средиземноморье, да еще был отягощен *кризисом беженцев, заполонивших* страны НАТО. Так что говорить, что конфликт в Сирии не затрагивал интересы НАТО, могут только очень наивные люди. Затрагивал, в том числе и с формальной точки зрения.

В этом, вероятно, есть очень большой политический смысл: кризис НАТО длится уже довольно долго. Можно, вероятно, говорить, что он был инициирован неудачным опытом прямого управления операцией по стабилизации в Афганистане. Однако в тех случаях, когда НАТО и, прежде всего, США *играли первым номером,* кризис был контролируемым и не выходил за рамки обычных разговоров, что, мол, *НАТО уже не то,* которые ведутся *с* 1970-х годов. Когда же НАТО столкнулся с активным и агрессивным противником, который стремился навязать свои *правила игры,* — отложим пока в сторону конспирологические версии произошедшего в Сирии и Египте, — этот кризис стал до неприличия явным. НАТО просто исчез с операционной арены как интегрирующая и управленческая структура, хотя, объективно говоря, более удобной структуры, чем НАТО, для координации усилий западной антитеррористической коалиции трудно себе представить. Тем более что все *детские* ошибки уже были и сделаны, и исправлены в ходе операции в Афганистане. И можно было показать *класс* военной координации и оперативного реагирования. Показательно, что в мерзкой и трагичной истории с уничтожением российского самолета Су-24 М НАТО практически самоустранился от участия в судьбе одного из своих членов, который еще некоторое время назад считался ключевым.

Помимо того приятного для российских специалистов обстоятельства, что скрытый кризис НАТО, о котором иные говорили еще с 1970-х годов в связи с политикой *разрядки,* наконец-то стал явным, нельзя не обратить внимания еще на несколько важных обстоятельств.

Прежде всего, на то, что вопрос о *европейской оборонной идентичности* через некоторое время, хотя бы и в рамках усиления антитеррористической риторики, может стать вновь актуальным. Особенно учитывая тот шок, который произвели на *вовлеченных обывателей* террористические акты в Париже. При этом молчание Германии и ее отказ участвовать в антитеррористической коалиции против ИГ не только говорят о глубине кризиса европейских оборонных институтов, но и под-

черкивают то неожиданное, прямо скажем, обстоятельство, что место лидера *европейской оборонной идентичности* вдруг оказалось вакантным. Понятно, что на это место не так много претендентов (по сути, если *откинуть* Германию, то это Франция и Польша), но сама по себе ситуация весьма интересна.

Не исключу в связи с этим, что некоторые политические силы могут поставить вопрос о пересмотре характера и глубины военно-политических обязательств США перед Европой. В конечном счете, НАТО как таковой был частью общей системы атлантических взаимоотношений, которая интенсивно надстраивалась в последние годы политическими (санкции против России и политическое участие в украинской гражданской войне) и экономическими (Трансатлантическая зона свободной торговли) компонентами. Вопрос в том, что обязательства США перед Европой в последние два года стали неадекватны тем рискам, которые США стали создавать для европейских стран. Причем риски эти стали понятны не только *яйцеголовым* из университетов, но и весьма широкой массе европейцев. Кто и почему ответственен за *кризис беженцев* в Европе, в действительности хорошо поняли, и именно с этим связан рост пророссийских настроений в рядах общественности при сохранении подчеркнуто негативного отношения к России со стороны элит.

Не надо забывать, что от разговоров о *европейской оборонной идентичности* полшага до постановки вопроса о европейской политической идентичности, которая и так сильно пострадала из-за ренационализации политики безопасности (хотя бы в форме контроля границ) в ходе *кризиса беженцев*. А это такой *ящик Пандоры*, который европейцам стоит открывать только в самом крайнем случае.

Причем все это происходит на фоне относительного падения авторитета США и втянутости американцев в слишком большое количество военно-силовых и военно-политических ситуаций, для участия в которых ресурсов стало не хватать. То есть вопрос о *европейской оборонной идентичности* начинает приобретать вполне очевидный *прикладной* характер.

Итак, основания для пересмотра характера отношений имеются, вопрос в том, насколько европейские политики обладают волей для того, чтобы поставить вопрос о *перераспределении бремени* и указать Вашингтону, что свои завтраки американцы должны оплачивать сами.

ВМЕСТО ЗАКЛЮЧЕНИЯ: РОССИЙСКИЙ БРОСОК ЧЕРЕЗ *БИТОЕ ПОЛЕ*

Конечно, в завершение этого материала можно пуститься в пространные рассуждения о том, что Россия с возвращением Крыма и операцией в Сирии вернулась в число *великих держав.* Благо США и ЕС своим безволием и любовью к разного рода сомнительным комбинациям с сомнительными контрагентами сами создали тот вакуум, в который и вошла Россия со своими нехитрыми и, если допустим этот термин, *искренними* политическими подходами. А также с зубодробительными военными инструментами. С другой стороны, можно порассуждать о развитии международной ситуации в терминах *прорыва Россией дипломатической блокады*, которую Запад милостиво позволил прорвать[29], чтобы не усугублять и без того неблестящую международную ситуацию.

Однако более продуктивным было бы посмотреть на наблюдаемые нами в последние полгода процессы с более долгосрочной точки зрения. В конечном счете, мы

все, вероятно, согласны с тем, что прежний комфортный потребительский мир уходит в геополитическое и геоэкономическое небытие, и ему на смену приходит нечто новое и существенно менее комфортное. Значит, и действия крупнейших держав мира сейчас — и именно сейчас — нацелены на то, чтобы сделать рождение этого нового мира, вернее, *прорастание* нового мира через мир старый чуть более комфортным. А то, что действия ключевых стран мира (США, Китая, Индии, России, в какой-то степени Германии) были продиктованы именно неким видением будущего стратегического контекста (возможно, ошибочным и точно сильно разнящимся — это к вопросу о *конце истории*), сомневаться не приходится.

Итак, в конечном счете в основе всех основных процессов современного мира лежит борьба за контроль над логистикой будущей системы международных отношений. Для каждой страны логистика бывает внешняя и внутренняя. Внутренняя логистика — это *связность* территории, обеспечивающая эффективность системы политического и экономического управления. Внешняя логистика — это наличие контролируемого доступа к внешним рынкам и ключевым в глобальном смысле транспортным коммуникациям.

С этой точки зрения внешняя логистика постсоветской России находилась в чудовищном состоянии. Неконтролируемый доступ Россия имела к тем направлениям, где нас *не ждали,* как, например, к Дальнему Востоку: согласимся, наши *замечательные китайские партнеры* далеко не в восторге от перспективы получить Россию в качестве самостоятельного геоэкономического игрока. Либо к тем направлениям, где почти не было инфраструктуры (Север, Арктика) и создавать ее было крайне сложно и затратно. Остальные же транспортные коридоры контролировались *нашими замечательными партнерами* по СНГ, которые, надо сказать, с Россией не очень церемонились. И тут показательны даже не чудовищные, доходящие порой до хамства поступки со стороны постсоветских государств, относящиеся к середине 1990-х, а наша недавняя действительность. То, с каким *пониманием* наши партнеры по ЕАЭС восприняли решение России об экономических санкциях в отношении Запада.

В этом смысле, когда разные американские политики говорили о России, как о региональной державе, они, в сущности, были правы. С той внешней (да и внутренней) логистикой, которая была у нашей страны после 1991 г., претендовать на глобальный статус было бы опрометчиво, если не бессмысленно. Даже с Европой Россия была вынуждена говорить через посредников.

То, что происходит сейчас, — активизация России на *внешнем контуре* своего геоэкономического пространства, в Сирии, в Иране, во Вьетнаме, в Египте, даже в забытой одно время Никарагуа — это попытка выйти из тупика *ближней логистики*. То есть до известной степени снять риски, связанные с попытками наших соседей по постсоветскому пространству взымать с России дополнительную *логистическую ренту*, регулируя доступ страны на внешние рынки.

Действительно, в последние годы обозначились новые направления глобальной логистики, участие в которых в той или иной степени является исключительно важным для России уже в среднесрочной перспективе. США могут хотя бы надеяться обеспечить себе лидирующие позиции за счет продавливания соглашений о свободной торговле. Классическим примером чего стало почти тайное подписание соглашения о Транстихоокеанском партнерстве, которое уже откровенно являет-

ся замкнутым торговым блоком с неявно выраженной пока военно-политической составляющей. А вот для России принципиальной задачей является снятие *барьеров для доступа* к рынкам. Задача, мало сказать, нетривиальная. Если мыслить пределами постсоветского пространства — в принципе нерешаемая.

Да, конечно, в такого рода действиях важно соблюдать баланс между военными и невоенными инструментами. Однако совершенно необязательно, что в новом мире будет сохранять правоту традиционная идея о том, что главными должны быть инструменты экономические. Тем более что в том регионе, через который Россия пробивает себе коридор к новым рынкам, военная сила может оказаться более эффективной, нежели экономические договоренности, ей не подкрепленные.

Маленький пример: наличие стратегических договоренностей с Ираном и контролируемого коридора на Сирию даст возможность осуществлять реализацию проекта стратегического коридора *Север-Юг* с меньшей зависимостью от наших партнеров по постсоветскому пространству. А если посчитать косвенные расходы, то и много дешевле. В конечном счете, в условиях острого противостояния с США лояльность постсоветских стран России приходилось покупать втридорога. И в этом смысле соглашения с Ираном о развитии экономического сотрудничества с акцентом именно на транспортную отрасль можно и нужно считать действительно *прорывными.*

Насколько этот маневр окажется стратегически успешным, пока сказать очень трудно. Но то, что он совершается и будет иметь существенные политические и экономические последствия, в том числе и внутри России, — бесспорно. Прежде всего, для тех постсоветских государств, которые исходили из незыблемости своего статуса регуляторов доступа российского экспорта на мировую арену. И, к слову, это говорит о глубоком скепсисе российского руководства относительно перспектив постсоветского пространства, особенно с точки зрения экономических перспектив.

Собственно, трансформация нового военно-политического статуса России в некие геоэкономические дивиденды и будет, вероятно, составлять главную задачу российской политики на наступающий 2016 г. Это, нравится нам или нет, безальтернативная реальность, данная нам в политических ощущениях.

А уж как эта задача будет выполнена, то нам пока неведомо. Но если эта трансформация случится, то следует признать все издержки, связанные с действиями России в последние годы, включая санкции, вполне оправданными.

Дмитрий Евстафьев

Примечания

1 Хоть это и безумие, но в нем есть логика. William Shakespeare. Hamlet. Act 2, scene 2

2 Транстихоокеанское партнерство (ТТП) включает в себя создание зоны свободной торговли, а также меры по улучшению инвестиционного и делового климата, соблюдению трудовых и экологических стандартов, прав на интеллектуальную собственность и либерализации инвестиционного режима и так далее. В ТТП входят США, Канада, Мексика, Перу, Чили, Австралия, Новая Зеландия, Сингапур, Бруней, Вьетнам, Малайзия и Япония. Большие выгоды от создания ТТП получат США, экспорт которых вырастет к 2025 г. на 124 млрд долл.; Япония, ее экспорт может вырасти на 14%, а ВВП — более чем на 2% ежегодно, Вьетнам и Малайзия, чей ВВП вырастет в 2012 г. на 6 и 13%

соответственно. Наибольшие потери понесет Китай — примерно на 0,3 процентных пункта ВВП в год и 1,2 процентных пункта экспорта в год, а также Европа, Индия и Россия. Подробно см.: Ярослав Лисоволик. Мегаломания мегаблоков. Транстихоокеанское партнерство как высшая стадия регионализма. *Россия в глобальной политике*. № 6, ноябрь/декабрь 2015 г.

3 Владимир Путин. *О наших экономических задачах*. Ведомости. № 3029. 31 января 2012 г.

4 *Table S3: R&D expenditure as a share of GDP and in purchasing power parity (PPP) dollars, 2009–2013.* Statistical annex. UNESCO Science Report. Towards 2030. Paris. 2015. Pp. 756–758

5 Leonid Gokhberg and Tatiana Kuznetsova. *Russian Federation.* UNESCO Science Report. Towards 2030. Paris. 2015. P. 357

6 Технология плазменного импульса себестоимостью в настоящее время чуть выше 20 долларов за баррель, вытесняющая гидроразрыв пластов, не требует больших объемов воды, экологически более безопасна и существенно повышает отдачу месторождений.

7 Владимир Фролов. *Внешняя политика: Дипломатия освобождения.* Ведомости. № 3969 от 27 ноября 2015 года. http://www.vedomosti.ru/opinion/articles/2015/11/27/618588-diplomatiya-osvobozhdeniya#/.

8 Václav Havel "A Conscience Slumbers in Us All: Commencement Speech at Harvard University". June 1995. Цит. по: Сейла Бенхабиб. «Притязания культуры». Москва. Логос. 2003 г. Стр. XLIX

9 Игорь Яковенко. *Терроризм*. Нева. 2005 г. № 12. http://magazines.russ.ru/neva/2005/12/ia11.html

10 Вооруженные сила режима Асада состоят из сухопутные войск — Сирийской арабской армии (Syrian Arab Army), ВВС и ВМФ. Сирийская арабская армия (САА) включает в себя, помимо восьми *обычных* (conventional) дивизий, также *специализированные*, а точнее, элитные соединения: Республиканскую гвардию (мотострелковая дивизия численностью около 25 тыс. человек), предназначенную для обороны Дамаска, — единственное войсковое соединение, которому разрешен вход в центр столицы; Силы специального назначения (14-я и 15-я дивизии и четыре полка специального назначения), представляющие собой мобильные соединения легкой пехоты, части которых перебрасываются на наиболее опасные участки фронта, а также 4-ю бронетанковую дивизию, командиром которой является младший брат Б. Асада и фактически второй человек в иерархии режима М. Асад.

11 Joseph Holliday. *The Assad Regime: From Counterinsurgency to Civil War*. Institute for the Study of War. March 2013, P. 33; Christopher Kozak. *An Army in all corners. Assad's campaign strategy in Syria*. Middle East *Security* Report 26. The Institute for the Study of War. April 2015. P. 13.

12 «*Призраки на стероидах»: СМИ рассказали о тайных убийцах Асада.* NEWSru.co.il. 11 июня 2012 г. — http://newsru.co.il/mideast/11jun2012/shabiha_a205.html

13 Christopher Kozak. *An Army in all corners. Assad's campaign strategy in Syria*. Middle East Security Report 26. The Institute for the Study of War. April 2015. P. 15.

14 Алавитов обычно называют разновидностью шиизма или шиитской сектой, но, строго говоря, их даже нельзя назвать мусульманами. Одни ученые считают их религию своеобразной смесью раннего христианства и дохристианских верований, распространенных в древности на Ближнем Востоке. Другие добавляют к этой смеси элементы, заимствованные из ислама. Сами алавиты называют себя шиитами. Но они отвергают шариат, соблюдают христианские праздники, во время которых читается Евангелие, причащаются вином и в то же время практикуют поклонение солнцу, луне, вечерней и утренней заре. Их священные книги не опубликованы и доступны только членам общины. Алавиты провозгласили себя шиитами по вполне очевидной причине: сирийская конституция предполагала, что президентом страны может быть только мусульманин. Поэтому в 1973 г., вскоре после захвата власти Х. Асадом, Совет алавитских шейхов заявил, что они почитают 12 имамов и, следовательно, такие же шииты, как и в Иране и Ираке. По похожим политическим причинам в том же 1973 г. лидер иракских шиитов Великий аятолла Хакими подтвердил это, издав специальную фетву, а после победы исламской революции аналогичную фетву издали в Иране.

15 *Армия завоевания (Джейш аль-Фатх)* — возникшая в марте 2015 г. зонтичная коалиция оппозиционных группировок, главную роль среди которых играет *Харакят Ахрар аш-Шам аль-Ислами (Исламское движение свободных людей Шама)*, являющаяся, в свою очередь, союзом салафитских группировок. Помимо *Ахраар аш-Шам* в *Армию завоевания* входят *Джабхат ан-Нусра*, а также ряд относительно умеренных исламистских формирований.

16 *Совещание о действиях Вооруженных Сил России в Сирии*. 17 ноября 2015 г. — http://kremlin.ru/events/president/news/50714

17 В МГПС входят Германия, Европейский союз, Египет, Иордания, Ирак, Иран, Италия, Катар, Китай, Ливан, Лига Арабских Государств, Объединенные Арабские Эмираты, Оман, Организация Объединенных Наций, Россия, Саудовская Аравия, Соединенное Королевство, США, Турция и Франция.

18 *Заявление Международной группы поддержки Сирии*, Вена, 14 ноября 2015 г. — http://www.mid.ru/web/guest/foreign_policy/international_safety/conflicts/-/asset_publisher/xIEMTQ3OvzcA/content/id/1941109

19 Георгий Мирский. *Сирия: коалиция или показуха?* Эхо Москвы. Блог. 19 ноября 2015 г. — http://echo.msk.ru/blog/georgy_mirsky/1661394-echo/

20 Махлуфы — семейный клан А. Махлуф, жены Х. Асада

21 Western leaders agreed to extend Russia sanctions by six months: diplomat. Reuters. Nov 21, 2015 http://www.reuters.com/article/2015/11/21/us-eu-russia-sanctions-idUSKCN0TA0XH20151121#SJL1JveVPkJwv25j.99

22 Сергей Сумленный. *Изгнаны и убиты*. Эксперт online. 28 июля 2008 г. — http://expert.ru/expert/2008/30/izgnany_i_ubity/

23 Составлено по данным: Asylum-seekers and refugees. A Statistical report. Volume1. EC Member States. Statistical Office if the European Communities. Luxemburg. 1993; Focus Migration. Country profile European Union. N 17. March 2009. Hamburg Institute of International Economics. Hamburg; Migrants in Europe. A statistical portrait of the first and second generation. Eurostat Statistical book. Luxemburg. 2011; Asylum applicants and first instance decisions on asylum applications. Eurostat. Доклады за 2011–2015 годы.

24 Составлено по данным Eurostat: Asylum applicants and first instance decisions on asylum applications за соответствующие годы.

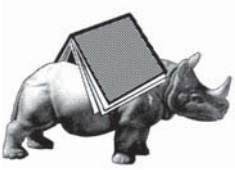
25 Украина после выборов: обострение в Донбассе. 2 декабря 2015 г. www.svoboda.org/content/transcript/27370541

26 Владимир Фролов. Внешняя политика: Дипломатия освобождения. Ведомости. № 3969 от 27 ноября 2015 г. — http://www.vedomosti.ru/opinion/articles/2015/11/27/618588-diplomatiya-osvobozhdeniya#/.

27 См. Месснер Е. Э. Всемирная мятежвойна. — Москва: Издательство «Кучково поле», 2004

28 Tracking Crude's Journey — From Islamic State To Western Markets. http://oilpro.com/post/20211/tracking-crude-journey-islamic-state-to-western-markets

29 Классический пример подобного подхода: развернутая статья А. Баунова «Венский концерт. Почему России простили Сирию». http://carnegie.ru/commentary/2015/11/02/ru-61836/iksf?mkt_tok=3RkMMJWWfF9wsRouu6zIZKXonjHpfsX56OgpUKa3IMI%2F0ER3fOvrPUfGjI4GS8VIl%2BSLDwEYGJlv6SgFSrnAMbBwzLgFWhI%3D



Павел Палажченко

ДИПЛОМАТИЯ САММИТОВ: ЖЕНЕВА И РЕЙКЬЯВИК ГЛАЗАМИ ПЕРЕВОДЧИКА

Время движется только в одном направлении, и через тридцать лет после женевской встречи руководителей СССР и США, годовщина которой прошла почти незамеченной у нас в стране, осталось не так много людей, которые в той или иной роли принимали в ней участие.

Моя роль тогда была скромной — я был одним из переводчиков советской делегации. Участие в этом историческом событии было для меня до некоторой степени случайным, но моя предшествующая карьера — работа в ООН в 1974–1979 гг. и на переговорах по сокращению и ограничению вооружений в первой половине 80-х гг. — дала мне довольно полное представление о проблемах, которые завели в тупик наши отношения с Западом, прежде всего проблемах безопасности.

Я бы сказал, что эти переговоры лишь по инерции называли *переговорами по разоружению*. Работа на них была интересной и в профессиональном отношении очень полезной для меня. Там я по-настоящему сформировался как профессионал. Но как человек и гражданин своей страны я не мог не испытывать чувство тревоги. Переговоры годами находились в глухом тупике, никакого сокращения вооружений и вооруженных сил не происходило, отношения с Западом, особенно с США, обострялись, а жизнь подавляющего большинства людей в СССР становилась все более трудной.

Тяжелое впечатление оставляли и сами переговоры. Главами делегаций на переговорах по ракетам средней дальности были выдающиеся профессионалы — Юлий Александрович Квицинский и Поль Нитце, понимавшие, что лучше договоренность, чем конфронтация. Но позиции сторон не оставляли им пространства для маневра. Приходится признать, что отправным пунктом движения в тупик стало развертывание наших твердотопливных ракет средней дальности *Пионер* (SS-20). Они действительно резко меняли баланс сил в этой категории вооружений и по-настоящему беспокоили европейцев. В интервью Брежнева, данном незадолго до начала переговоров, была сделана попытка доказать, что равновесие сохраняется. Но подготовленный в генштабе *баланс*, куда включались вооружения Англии и Франции, старые самолеты и тому подобные *средства* средней дальности даже наши переговорщики характеризовали как надуманный. Однажды об этом в моем присутствии откровенно высказался Л. Мастерков, который в делегации выполнял роль хранителя *институциональной памяти* — историю переговоров по ядерному оружию, количественные параметры договоренностей и многочисленные детали он знал буквально наизусть. Конечно, это понимал и Квицинский. Когда однажды Нитце

сказал ему «вы хотите иметь столько же оружия, сколько все ваши потенциальные противники вместе взятые», он — при всем его остроумии и дипломатической хватке — не нашелся, что ответить.

На первом заседании делегаций Квицинский хлестко и эффектно охарактеризовал предложенный Рейганом *нулевой вариант* решения проблемы — ликвидацию советских ракет в обмен на отказ от развертывания американских баллистических и крылатых ракет в Европе — как «дырку от бублика». К счастью, это фразеологизм не поставил меня в тупик и в переводе вызвал ожидаемый автором смех. Переговорный расчет советской стороны был на антивоенное движение в европейских странах и на противоречия в самой американской позиции.

Действительно, многотысячные антивоенные демонстрации беспокоили США, а стремление развернуть хотя бы крылатые ракеты у американских военных и политиков иногда, казалось, перевешивало их приверженность позиции собственного президента, т. е. *нулевому варианту*. Именно это было в *подтексте* предложений, неофициально изложенных Нитце Квицинскому во время так называемой *прогулки в лесу* в Сен-Серге летом 1982 г. Надо сказать, что договоренность на основе этих предложений была бы для СССР, наверное, еще более *неприятной*, чем *нулевой вариант*. Трудно представить себе, как наша пропаганда могла бы объяснить соглашение, согласно которому США развертывали бы крылатые ракеты в Европе, а СССР значительную часть своих ракет ликвидировал, причем под американским контролем. В Москве *прогулочный вариант* отвергли, хотя год спустя давали понять, что готовы рассмотреть нечто подобное. Но было уже поздно.

В итоге в декабре 1983 г., несмотря на протесты демонстрантов, началось развертывание американских ракет. Делегация предложила руководству прервать переговоры *для оценки сложившейся ситуации*, но это не касалось других переговоров — по стратегическим наступательным вооружениям, которые параллельно шли в Женеве. В Москве решили иначе. В заявлении, подписанном тяжело больным Андроповым, было сказано, что в этих условиях мы прерываем и те, и другие переговоры. Я видел, что члены делегации были несколько шокированы таким решением. Тупик выглядел не только полным, но и всеобъемлющим. 1984 г. не принес ничего нового, ничего обнадеживающего.

В общем, к моменту смены поколений в советском руководстве в 1985 г. ситуация в мире и в отношениях двух тогдашних сверхдержав была крайне тревожной. Руководители СССР и США не встречались уже шесть лет. Р. Рейган не очень дипломатично объяснял это тем, что его потенциальные собеседники *по очереди умирали*. Но отношения были практически заморожены и на других уровнях. А тем временем гонка вооружений продолжалась и ускорялась, в Европе развертывались новые ракеты, продолжалась конфронтация и в других регионах.

Начало моей работы на высшем уровне совпало с приходом нового советского руководства. В МИДе в общем понимали, что изменения должны затронуть и внешнюю политику, но назначение на пост министра Э. Шеварднадзе стало для всех большой неожиданностью. Понимая необходимость появления нового человека, в подавляющем большинстве мидовцы ожидали назначения из своих рядов, *министра-эксперта*, а не *политического министра*. Лично я думаю, что министром иностранных дел должен быть крупный политик, иначе невозможно обеспечить реальный вес министерства в принятии решений. Опыт многих стран показывает, что

именно это важнее всего, а *экспертизу* вполне могут обеспечить дипломаты, роль которых при таком подходе даже возрастает.

Новый министр начал со встреч с руководителями отделов и других подразделений министерства, побуждая их к откровенным оценкам и предложениям. Как мне потом рассказывали, они высказывали самые разные идеи и предложения, в том числе в духе *зажать и не пущать*, *усилить и дать отпор*. Но большинство понимало, что ни сил, ни желания вести такую политику у руководства нет. Нужно было избавлять страну от гонки вооружений и все более дорогостоящих *обязательств* чуть ли не на всех континентах. Как конкретно это делать — большой вопрос. Многие в МИДе традиционно считали ключом ко всему отношения с США. Ждали первой встречи с госсекретарем Дж. Шульцем, которая должна была состояться в Хельсинки на конференции, посвященной 10-летию подписания Заключительного акта Совещания по безопасности и сотрудничеству в Европе.

С этой встречей связано важное событие в истории переводческой профессии: впервые на двусторонних советско-американских переговорах на этом уровне был применен синхронный перевод. Предложили это американцы, МИД согласился не сразу (рассказывали, что против был Г. Корниенко, который в течение еще почти года оставался на посту первого заместителя министра), но Шеварднадзе решил, что надо попробовать. С тех пор синхрон закрепился как вполне *законный* вид перевода на переговорах не только министров, но и глав государств. Разумеется, не всегда для этого есть подходящие условия и технические возможности. Поэтому по-прежнему используется и традиционный последовательный перевод, особенно в беседах один на один. Зато переговоры в составе делегаций действительно удобно проводить с синхронным переводом.

Вот так я попал в Хельсинки. Накануне встречи мы посмотрели и протестировали предоставленное американцами оборудование, оно оказалось не очень *высокотехнологичным*, но вполне подходящим.

Внимание дипломатов было, конечно, приковано к Шеварднадзе, для которого Хельсинки стал первым выходом на международную арену. Было видно, что он волнуется. Когда я смотрел из зала, как он идет к трибуне, я даже удивился: он шел медленно и очень скованно. Свою речь он начал не очень уверенно, иногда запинаясь и делая паузы. *Разогрелся* только к середине выступления.

Зато на встрече с Шульцем он уже выглядел иначе. Видимо, преодолев напряжение, почувствовал, что готов к разговору, который был вполне конструктивным по тональности. Министры сопоставили позиции по всей повестке дня, и хотя особенно нового в этих позициях я тогда не заметил, главное было в другом. В отдельной беседе они договорились сделать все от них зависящее, чтобы вывести отношения из тупика, преодолеть рутину, способствовать созданию благоприятной атмосферы. Надо сказать, это обещание они выполнили, многое сделав для того, чтобы движение в правильном направлении не было сорвано из-за неизбежных *ухабов* внешне- и внутриполитического характера.

Важным этапом в подготовке женевского саммита была встреча Шеварднадзе с Р. Рейганом в Белом доме в сентябре 1985 г. К этому времени министр уже вполне освоился с *материалом* и не так волновался, как в самом начале. Выступая на Генеральной Ассамблее ООН, он держался очень уверенно, и в тексте выступления содержались некоторые новые нюансы. К встрече с президентом США Шеварднад-

зе готовился очень тщательно, делая выписки из подготовленных для него *разговорников*, иногда просиживая за полночь в поисках собственных формулировок. И в самолете по пути в Нью-Йорк продолжал в своем салоне обсуждение предстоящей встречи с ближайшим кругом советников.

Перед посадкой стало ясно, что погода в Вашингтоне ужасная. За пару дней до нашего приезда бушевал ураган *Глория*, *хвост* которого мы застали. Шульц даже предлагал не лететь в Вашингтон самолетом, а поехать специальным поездом. Мы вспомнили об этом предложении, когда сильный порыв бокового ветра накренил самолет влево буквально над посадочной полосой. Проливной дождь и сильный ветер продолжались почти всю ночь, но наутро, как в каком-нибудь романе, небо прояснилось, и когда мы ехали на встречу в Белый дом, солнце сияло вовсю. Думаю, многие увидели в этом хорошее предзнаменование.

Рейган тогда еще был для нас загадкой. Все помнили его высказывания об *империи зла*, и хотя Шульц, Миттеран и другие собеседники говорили о его способности к компромиссам, верилось в это с трудом. Поэтому так важно было посмотреть, какую атмосферу на встрече создаст хозяин Белого дома. Не знаю, что сказал Шеварднадзе в узком кругу после встречи (тогда еще он не приглашал меня на эти обсуждения), но мне показалось, что Рейган стремился расположить к себе собеседника, послать Горбачеву позитивный сигнал.

Встречи на высшем уровне всегда требуют тщательной подготовки. Недавно бывший посол США в СССР Дж. Мэтлок, который координировал подготовку к саммиту президента США и *настраивал* его на встречу с Горбачевым, дал интересное интервью, где довольно подробно рассказал о том, как шла к саммиту американская сторона. Из этого интервью ясно, что не всем в Администрации США нравилась сама идея саммита и главное — любые шаги, способные изменить отношения к лучшему. И у нас были противники конструктивного диалога с США, равно как и те, кто, понимая его необходимость, считали, что *с этой Администрацией ничего не получится*. Такая позиция — рецепт инерции и рутины, что очень опасно в любых переговорах и вообще в межгосударственных отношениях. Поэтому так важно было не просто встретиться, но и обозначить новый этап в отношениях. Лучше всего — закрепить в политическом документе. И здесь начались трудности.

С обеих сторон были желающие устроить *перетягивание каната* по поводу сроков и места проведения встречи. По-разному понимали стороны и ее возможные результаты. Американцы долго — фактически вплоть до самой встречи — противились принятию какого-либо совместного документа, считая работу над ним потерей времени: дескать, главное — встретиться, познакомиться и дать импульс переговорам. Приходилось по ходу подготовки решать и множество организационных и протокольных вопросов, которые иногда приобретали самодовлеющее значение. Во всем виделось соперничество. Дж. Мэтлок вспоминает, как уже во время саммита американская *пиар-команда* позаботилась о том, чтобы Рейган (в холодный и ветреный день) вышел в костюме и без головного убора встречать Горбачева, вышедшего из автомобиля в пальто и шляпе. Пресса писала по этому поводу, что Рейган выглядел динамичнее. И у нас некоторые обратили на это внимание.

Мне кажется, что акцентирование подобных вещей в СМИ и в разговорах *пикейных жилетов* идет от непонимания сути саммитов. Их задача — определить направление *большой политики*, а не соревноваться в том, какое впечатление произведет тот или

иной руководитель. И надо сказать, что на каждом следующем саммите можно было констатировать, что на первый план все больше выходит содержание, а не форма.

Думаю, в ноябре 1985 г. в Женеве произошли две вещи. Во-первых, несмотря на огромные идеологические и политические различия двух стран, да и личностные различия их лидеров, изменилась атмосфера отношений. Немалую роль в этом сыграло неформальное общение Рейгана и Горбачева, в котором участвовали также их супруги.

Мне довелось в качестве переводчика участвовать в обеде в советском представительстве при ООН, который состоялся в первый день саммита. Тогда мне показалось, что стороны приятно удивили друг друга — настроение и разговор были дружелюбными и неформальными. А когда Горбачев в своем тосте процитировал Библию — «Всему свое время... время рождаться, и время умирать... время разбрасывать камни, и время собирать камни» — это произвело на гостей ожидаемое впечатление. Так что первый контакт состоялся, и это в конце концов оказалось важнее, чем возникшие в последующие годы *шероховатости*, в частности в отношениях *первых леди*, о которых любила порассуждать пресса.

И второе: все-таки удалось принять совместное заявление, причем содержательное. Думаю, Дж. Мэтлок совершенно прав, выделяя в нем тезис о том, что «ядерная война никогда не должна быть развязана, в ней не может быть победителя». И далее в заявлении говорилось, что стороны не будут стремиться к достижению военного превосходства друг над другом. Кстати, далеко не все в СССР и США были согласны с этими тезисами. Идеи достижения *решающего военно-технического превосходства над потенциальным противником* витали не только в военных кругах. Но последнее слово всегда остается за политическим руководством.

Тезис о недопустимости ядерной войны стал основой не только для активной работы на переговорах по сокращению ядерных вооружений, но и одной из основ личных отношений Рейгана и Горбачева. Неприятие ядерного оружия сближало их. И если сегодня мы можем говорить о том, что в арсеналах двух держав на порядок меньше ядерных носителей и боезарядов, чем на пике холодной войны, то именно благодаря тому, что произошло тогда в Женеве и через год в Рейкьявике.

Делегации работали над текстом совместного заявления буквально круглосуточно, и в конце концов его удалось согласовать к утру последнего дня встречи. По некоторым вопросам Горбачеву приходилось советоваться с Москвой, что, кстати, происходило и на последующих саммитах, на которых я переводил. Это важно вспомнить потому, что сегодня его обвиняют в принятии *волевых*, волюнтаристских решений вопреки мнению других членов руководства. Эти обвинения совершенно голословны, не подкреплены какими-либо документальными доказательствами.

Вообще у меня всегда было впечатление, что и Горбачев, и американские президенты полностью осознавали, что они работают в определенных политических рамках и должны взвешивать различные позиции внутри своих стран. Отчасти поэтому полностью реализовать *дух Женевы* в период президентства Рональда Рейгана все-таки не удалось. В частности, договор о 50-процентном сокращении стратегических наступательных вооружений был подписан лишь в 1991 г. с Дж. Бушем, хотя основные его параметры были согласованы в октябре 1986 г. в Рейкьявике. В своих мемуарах Дж. Шульц возлагает главную ответственность за это на *ястребов* внутри администрации США.

Препятствия на пути строительства новых отношений между СССР и США стали возникать почти сразу же после саммита. Были серьезные разногласия, были недоразумения и *недопонимания*, были и очевидные провокации. Напомню хотя бы о заходе двух кораблей американских ВМФ в территориальные воды СССР в феврале 1986 г. (как потом писал заместитель министра обороны США Р. Армитедж, в этой акции «не было никакой оперативной необходимости»). Но главное — несмотря на *дух Женевы* и серьезные сдвиги в советской позиции, содержавшиеся в известном заявлении М. С. Горбачева от 15 января 1986 г. (помнится, перевод этого заявления на английский язык мы закончили в 4 часа утра), переговоры в Женеве застопорились и буксовали на протяжении нескольких месяцев. Надо было как-то выбираться из этой раскисшей колеи. Такая возможность открылась в конце лета.

Я был в отпуске и большую часть времени проводил за городом, в Монино. Дозвониться туда в те годы было непросто (коммутатор, добавочный…), но мне все-таки дозвонились из секретариата заместителя министра А. Бессмертных. Александр Александрович, извинившись, что прерывает мой отпуск, попросил срочно приехать в Москву. За мной прислали машину, и через час я уже переводил письмо Горбачева Рейгану. Как вспоминал потом Михаил Сергеевич, причиной письма было его недовольство положением дел на переговорах по ядерному оружию и желание вырваться из рутины, которой было пронизано полученное им письмо Рейгана и подготовленный в МИДе проект ответа. Сам он был в отпуске и вместе с А. Черняевым, который незадолго до этого стал его помощником по международным делам, написал ответ, главной мыслью которого было предложение встретиться как можно скорее где-нибудь *на полпути* (упоминался Рейкьявик), чтобы преодолеть инерцию и договориться по главным нерешенным вопросам. О деталях должны были договориться Шульц и Шеварднадзе на встрече в Нью-Йорке во время очередной сессии Генеральной Ассамблеи ООН.

Однако буквально накануне отъезда министра в Нью-Йорк произошли события, которые произвели эффект разорвавшейся бомбы и вполне могли сорвать предложенную Горбачевым встречу. В Нью-Йорке был арестован по подозрению в шпионаже советский сотрудник Секретариата ООН Захаров, причем сделано это было с большой оглаской и с перспективой громкого суда (если бы Захаров был просто выдворен из страны, многих проблем можно было избежать). Сразу же после этого был арестован московский корреспондент журнала *U. S. News and World Report* Николас Данилофф, давно работавший в Москве и имевший репутацию *чистого* журналиста.

В аэропорт я ехал вместе с помощником Шеварднадзе Теймуразом Степановым (Мамаладзе) — единственным человеком, которого год назад новоназначенный министр *привез* с собой из Грузии. Теймураз был его главным речеписцем и очень эмоциональным человеком. Своего подавленного настроения и пессимизма он не скрывал. Я попытался кое-как успокоить его, дескать, такие дела обычно рано или поздно решаются. Но Теймураз, я думаю, опасался, что если миссия Шеварднадзе окончится неудачей, позиции министра будут сильно подорваны. И сам Шеварднадзе начинал свою вторую поездку в Нью-Йорк в плохом настроении.

Шпионский скандал (к сожалению, не последний в отношениях между СССР и США — как правило, они возникали, когда в отношениях появлялось что-то обнадеживающее) был первым, о чем журналисты спросили Шеварднадзе у трапа самолета. На карту было поставлено очень много, и решение просматривалось с тру-

дом — слишком много было в этом деле, если воспользоваться известной фразой, *гордости и предубеждения*.

Шульц в первой же беседе дал понять, что предложение о встрече на высшем уровне имеет шансы только в том случае, если будет освобожден Данилофф, арест которого он назвал совершенно необоснованным. Стало ясно, что надо найти вариант решения, который хотя бы внешне не уравнивал двух арестованных. Ни одна из сторон не хотела *терять лицо*. Выход из положения пришлось искать дипломатам. Но сначала важно было оценить настроение Рейгана, встреча с которым в Белом доме состоялась несколько дней спустя.

Это была действительно встреча один на один. Кроме Рейгана и министра были только два переводчика — я и мой американский коллега Д. Заречняк. По пути на встречу и на обратном пути в посольство Шеварднадзе молчал. В посольстве он предложил мне пройти вместе с ним в *защищенное помещение*, где его ждали посол Ю. Дубинин, Бессмертных и помощники — Степанов и С. Тарасенко.

Несколько минут все молчали, ожидая, чтобы кто-то сказал первое слово. Наконец, посол спросил:

— Эдуард Амвросиевич, какое впечатление?

— Впечатление не очень хорошее, — после небольшой паузы ответил Шеварднадзе и неожиданно посмотрел на меня. — А вам как кажется?

Я был удивлен. Казалось бы, никакого веса мое мнение иметь не должно. Но если спрашивают, надо отвечать. Поднявшись с места, я сказал:

— По-моему, беседа прошла не так плохо. Рейган, конечно, повторил официальную позицию по шпионскому делу, но выражался не очень резко, а по другим вопросам — конструктивнее, чем можно было ожидать. И не отверг идею встречи с Горбачевым.

Возможно, моя оценка показалась министру несколько приукрашенной, но он не возражал. Полный текст записи беседы был отправлен в Москву. Теперь надо было выстроить стратегию выхода из этой ситуации. И в обеих столицах — по разным, разумеется, причинам — Шеварднадзе надо было демонстрировать твердость.

Вернувшись в Нью-Йорк, министр продолжал встречи со своими коллегами из разных стран, но — не преувеличиваю — десятки часов ушли на беседы с Шульцем по урегулированию *шпионского кризиса*. На этих беседах присутствовали Бессмертных и заместитель Шульца Розан Риджуэй. Одновременно шли двусторонние обсуждения по вопросам разоружения, региональным проблемам, двусторонним отношениям. Контактов такой интенсивности я не помню. Было ясно, что либо разругаемся всерьез и надолго, либо найдем выход из положения.

В какой-то момент в ходе казавшихся бесконечными обсуждений был упомянут Ю. Орлов, осужденный по политическому обвинению еще в брежневские времена. В то время он находился в административной ссылке (как, кстати, и академик Сахаров). Тогда еще не было известно, что политзаключенные и высланные вскоре будут освобождаться в массовом порядке, и возвращение Орлова из ссылки и его выезд за границу были включены в *пакет*, благодаря которому удалось преодолеть очень серьезный кризис в советско-американских отношениях. Обставлено это было так, что и та, и другая сторона сумели *спасти лицо*, но вплоть до момента освобожде-

ния Захарова в зале суда, после очень резкого заявления судьи, всё, как казалось, висело на волоске. Бессмертных ждал у телефона звонка нашего дипломата, находившегося в здании суда, и я видел, что он волнуется (происходило это задолго до появления мобильных телефонов). Данилофф был выпущен в тот же день, а через несколько дней (как бы отдельно от *обмена*) — Орлов, сразу же выехавший за рубеж.

В те дни мне редко удавалось выспаться. Полная запись каждой беседы должна была как можно скорее уйти в Москву, а сделать такую запись после двух-трехчасовой беседы — это как минимум *столько и еще полстолько*. Но все, кто участвовал в этом марафоне, были в итоге довольны: дорога в Рейкьявик была открыта.

О встрече в Рейкьявике написано много, но мне кажется, что *сюжет* встречи часто теряется в многочисленных деталях, не говоря уже о том, что он искажается домыслами, не имеющими ничего общего с тем, что там произошло. Записи бесед опубликованы как американцами, так и нами (кстати, хотя правила ведения записи у нас и у них разные — от первого лица у нас и *в изложении*, т. е. от третьего лица, у американцев — никаких разночтений в них не обнаружено). Не раз высказывались и участники встречи, и хотя они дают разные интерпретации того, что там произошло (так, в книге бывшего директора Агентства по контролю за вооружениями США К. Адельмана главным героем выступает Рейган, *спасший программу СОИ*), но фактическая сторона дела выглядит у всех одинаково.

После короткой беседы один на один, в ходе которой Горбачев изложил Рейгану основные пункты наших предложений, главы делегаций пригласили в комнату, где шла их беседа, Шульца и Шеварднадзе, которые разговаривали отдельно. Попутно скажу, что, поскольку первоначальная идея Горбачева предполагала неформальную встречу с минимальным количеством советников и экспертов, для встречи выделили небольшой дом у берега моря — Хёфди-хаус — очень симпатичный, но, мягко говоря, тесноватый для всех собравшихся. Разговаривали и в узких коридорах, и на лестницах. Рейгану нужна была помощь Шульца, чтобы выяснить, что нового привез с собой Горбачев. А новое в предложениях, безусловно, было. Горбачев предложил резко упростить схему будущего договора о стратегических вооружениях — всё сократить наполовину, в том числе советские тяжелые МБР (СС-18). Это был серьезный шаг, в ответ на который американцам предлагалось ограничить программу СОИ *лабораторными исследованиями*. РСД предлагалось сократить до 100 боеголовок. Эти позиции были утверждены в Политбюро. В директивах к встрече было два варианта оформления возможной договоренности — либо как взаимоувязанного пакета, либо отдельно по РСД и СНВ/ПРО.

Самым трудным вопросом была, конечно, проблема ПРО. Прежде всего потому, что программа СОИ была для Рейгана *любимым ребенком*. Он был, как мне кажется, вполне искренен, когда говорил, что ее цель — *сделать ядерное оружие бессильным и устаревшим*. Искренен в том смысле, что он действительно считал ядерное оружие аморальным, оружием геноцида, и хотел его уничтожения. У нас его программу воспринимали совершенно иначе. В ней видели попытку получить после существенного сокращения ядерного оружия новую стратегическую конфигурацию, позволяющую нанести первый удар и парировать ответный. Как минимум, это дестабилизировало бы ядерный баланс. Конечно, при тех уровнях СНВ, которые были тогда (да и в два раза меньших), развертывание системы ПРО вряд ли могло сломать баланс, но наши военные говорили, что надо видеть перспективу, потенциальные возможности, и настаивали на жесткой позиции.

У Рейгана были готовые тезисы, которые он отрабатывал на сто процентов. Большинство его аргументов носили нетехнический характер. Когда Горбачев спрашивал его, зачем нужна ПРО, если ядерное оружие будет, как хочет того сам президент, полностью уничтожено, Рейган отвечал, что это будет своего рода окончательная гарантия против какого-нибудь безумца, своего рода *противогаз* (gas mask) *на всякий пожарный случай*. Более того, говорил Рейган, мы будем готовы поделиться с вами технологиями ПРО. Горбачев, естественно, реагировал на эту идею очень скептически (даже многие американцы удивлялись, что президент США всерьез предлагает нечто подобное). Разговор все время упирался в проблему ПРО, но, хотя разногласия были глубокими, тон беседы был совершенно неконфронтационным.

После окончания первого дня переговоров советская делегация вернулась на теплоход *Георг Отс*, где во время саммита жили Горбачев и его советники. Горбачев пригласил всех в кают-компанию и попросил меня прочитать по моей записи основные моменты беседы. Время от времени он вставлял свои комментарии. Поскольку в конце беседы лидеры договорились о том, что вечером (фактически ночью) поработают эксперты, он поручил С. Ахромееву возглавить группу с нашей стороны. С американской стороны группу возглавлял П. Нитце.

Экспертам удалось согласовать основные параметры будущего договора по стратегическим наступательным вооружениям. Схема оказалась несколько сложнее, чем то, что предлагал Горбачев, но в целом понятной и не перегруженной техническими деталями. Горбачев предложил договориться о нулевом уровне РСД в Европе. Прогресс был налицо, но снова возникла проблема ПРО. Рейган заявил, что не может согласиться на ограничение программы лабораторными испытаниями даже на срок в 10 лет. Горбачев еще раз спросил, зачем понадобится ПРО, если мы договоримся о полном уничтожении ядерного оружия в течение того же десятилетнего срока.

И тут разговор пошел в направлении, которое удивило многих в американской делегации, а также союзников США, особенно англичан, когда они узнали о содержании этого разговора. Рейган сказал, что он хочет мира без ядерного оружия и готов обсудить ликвидацию «не только стратегических ракет, но и тактических». В доктринах США и НАТО ликвидация ядерного оружия обставлялась многочисленными условиями, о которых Рейган не упоминал. Интересно, что Шульц даже не пытался его остановить или *подкорректировать*. У меня это вызвало удивление. Было ли это связано с его собственными соображениями или с сомнениями относительно СОИ, или же он хотел посмотреть, насколько далеко его президент готов зайти в этом обсуждении? Трудно сказать. Но я помню, что в конце 80-х гг., когда Шульц уже не занимал своего поста, он встречался с Шеварднадзе в Нью-Йорке и сказал ему следующее: «Когда наши лидеры, каждый по-своему, заговорили о мире без ядерного оружия, эксперты считали, что они неправы, что это недостижимая цель. Но эксперты не поняли, что Рейган и Горбачев почувствовали одну важную вещь: этого хотят люди, это отвечает их чаяниям».

Общеизвестно, что *рейкьявикская лодка* разбилась о СОИ. Но трактовка этого факта — разная. В США распространено мнение, что Горбачев заманил Рейгана в Рейкьявик, чтобы уговорить его отказаться от программы ПРО или выхолостить ее, но Рейган стоял твердо и не поддался. Это очень примитивная интерпретация. Предложение ограничить программу исследованиями и лабораторными испытаниями не могло привести к ее прекращению, тем более что (особенно после саммита) мы давали понять, что готовы трактовать понятие *лаборатория* довольно широко.

Как показывают последующие события, программа СОИ — как проект глобальной противоракетной обороны — замедлилась сама по себе, хотя бы потому что бросать деньги на ветер ни конгресс, ни администрация Дж. Буша не хотели. Но Рейган фактически хотел, чтобы Горбачев дал *зеленый свет* ничем не ограниченным испытаниям и развертыванию ПРО, обещая поделиться технологиями, рисуя перспективы сотрудничества и партнерских отношений во всех областях. Пойти на это Горбачев не мог. Так он и сказал президенту. Тот был очень огорчен, и когда я вышел вместе с двумя лидерами к американскому кортежу, это было заметно по поведению Рейгана и его последним словам.

Американская делегация сразу после этого покинула Рейкьявик. Шульц перед отлетом успел сделать короткое заявление, охарактеризовав встречу как неудачную. А Горбачеву предстояла пресс-конференция. До места ее проведения было пять-десять минут ходьбы, и я шел рядом с Е. Примаковым, который расспрашивал о подробностях завершившихся переговоров. Конечно, всех интересовал один вопрос: что скажет Горбачев? В зале было больше ста журналистов, настроение среди них было подавленное — они уже знали о заявлении Шульца. Видимо, знал о нем и Горбачев.

Как потом вспоминали он и Черняев, директивы Политбюро предусматривали в случае отклонения советских предложений использовать пресс-конференцию для осуждения позиции США как не соответствующей интересам международной безопасности и разоружения. Это было бы проще всего: сказать, что, цепляясь за программу СОИ, президент США отверг возможность масштабного сокращения вооружений. Но Горбачев неожиданно для многих сказал, что то, что произошло на встрече, «не провал, а прорыв». Должен сказать, что, переводя его выступление, я внутренне соглашался с ним. «Мы заглянули за горизонт, — продолжал он, — мы говорили о мире без ядерного оружия. И я, и президент — за то, чтобы избавить мир от этого оружия. Мы по-разному видим путь к этой цели, но оба согласны, что надо начать с сокращения наполовину стратегических наступательных вооружений и ликвидации РСД в Европе. Теперь надо всем обдумать ситуацию. Мы подумаем, как быть дальше. Пусть подумает президент, конгресс. Я уверен, что мы продолжим диалог».

Это не стенографическая запись, но суть сказанного в тот вечер Горбачевым была именно такой. И я уверен, что время подтвердило, что его реакция на произошедшее была оптимальной. Основные параметры договоренностей, достигнутых в Рейкьявике, стали сигналом к прекращению наращивания ядерных вооружений, изменению планов военного строительства. В 1987 и 1991 гг. на основе этих договоренностей были подписаны Договоры по РСМД и СНВ, в соответствии с которыми были ликвидированы сотни носителей ядерного оружия и тысячи боезарядов. Ничего подобного в истории человечества не было.

Сегодня уроки тех лет вновь актуальны. Отношения между Россией и США переживают трудные времена. Можно до бесконечности спорить о том, кто виноват (или кто больше виноват) в нынешнем обострении напряженности. Но лучше этого не делать. Внимание и усилия надо сосредоточить на диалоге, который в течение почти целого года был по существу заморожен. Нельзя позволять, чтобы конфликты, кризисы, личное недопонимание между лидерами задавали тон в отношениях. Тем более нельзя допускать, чтобы в них доминировала пропаганда. Надо восстанавливать взаимное доверие и уважение, как бы трудно это ни было.

Арно Леклерк. Русское влияние в Евразии. Геополитическая история от становления государства до времен Путина. Альпина Паблишер, 2014 г. 368 стр.

В наш век, когда большинство уже не пишет больших книг, а еще меньшее количество людей берутся их читать, А. Леклерк решился на крайне отважный шаг. *Русское влияние в Евразии* — это фундаментальный труд, своего рода энциклопедия российской истории и внешней политики. Конечно, с учетом безумной динамики современного мира актуальность некоторых умозаключений автора слегка померкла, но в большинстве своем выводы вполне применимы к реальности.

В стилистическом плане работа Леклерка ближе всего к путевым заметкам и докладам западных исследователей России образца XVIII–XIX веков, поражающим всеохватностью и остротой наблюдений. Тут и краткое изложение истории православия, и описание транспортной системы, и анализ экономической географии, и препарирование политики российских императоров и президентов, и обзор отношений России с ее соседями и ключевыми контрагентами на международной арене. И пусть автор иногда не грешит глубокими выводами, а отделывается техникой описания и просто выкладывает факты — каждый из этих элементов так или иначе укладывается в общую концептуальную мозаику.

Прочтение книги напоминает движение по спирали: проходя через череду повторяющихся фактов, читатель попадает в сужающуюся аналитическую воронку, где каждое событие играет разными гранями и подводит к ключевым выводам по поводу неизбежной роли России в мире и почти кармическому предназначению ее отношений с другими странами. Произведение Леклерка — крайне ценный взгляд со стороны, возможность приподняться над текучкой и оценить внешнюю политику с точки зрения укорененных в столетиях глубинных процессов. Забавно, что внешняя политика России, зачастую представляющаяся российским исследователям хаотичной, лишенной внятной стратегии, в изложении Леклерка обретает логику. Более того, возникает ощущение следования четким национальным интересам.

Русское влияние в Евразии, на самом деле, не о влиянии и не о Евразии. Это произведение о статусе России в мире, ее глобальных амбициях и связи с Европой. В целом, история страны представляется как череда нелепостей, каждый раз отодвигающих вполне естественное сближение Московии и ее европейских соседей. Любопытно выглядит в этом смысле перекличка между реакцией *просвещенного монарха* Екатерины Великой на события во Франции и ответом современной рос-

сийской власти на череду *цветных революций* — и в том, и в другом случае произошел откат от сотрудничества с Западом в резкую *самодостаточность*. Пророчески звучат слова Петра I: «Европа необходима нам на несколько десятилетий, однако затем нам должно отдалиться от нее».

При этом автор отмечает, что несмотря на подобное нормальное *потребительское* отношение к западным ценностям и достижениям и несмотря на возрождение русской самобытности — возвращение к корням, укрепление православия, рост национального самосознания — более натуральным для элиты является проевропейский вектор. Движение по нему сдерживается историческими опасениями Москвы в отношении Европы и неспособностью Запада адекватно воспринять Россию. Поэтому для того, чтобы состояться, стране просто необходимо стать евразийской державой (на крайний случай, просто *евросибирским государством*), а не чисто европейским актором.

На этом пути неизбежны противоречия с другим крупным игроком — США. Примечательно, что, по мнению Леклерка, у России почти никогда не было именно глобальных амбиций. Даже постоянное расширение территории шло не ради мирового господства, а для того, чтобы обеспечить естественную безопасность в условиях крайне непростого окружения. И именно поэтому в XIX веке империя добровольно остановилась в своей экспансии, продав Аляску и отказавшись от претензий на тихоокеанское побережье США — именно это предопределило геополитические расклады века двадцатого. Сверхдержавные претензии, как отмечает автор, стали результатом большевистской революции и попыток создать всеобъемлющий проект-конструкт, который до 1980-х гг. был довольно конкурентоспособен и радикально отличался от идеологических *предложений* современного капитализма. Реформы 1990-х были направлены на то, чтобы окончательно выжечь элементы *советского*, однако в 2000-х восстановление российского могущества произошло именно на сплаве исторически обусловленной национальной самобытности и ментального наследия СССР.

Будучи профессиональным финансистом, Леклерк, почти как врач, диагностирует проблемы в российской экономике и системе управления. Однако его не перестает восхищать колоссальный потенциал страны, который еще более заметен при взгляде через призму великой истории. И в этом лейтмотив книги — вера в будущее России, которое неразрывно связано с ее способностью поддерживать свое влияние на евразийском континенте.

Дмитрий Поликанов

Andrew Korybko. Hybrid Wars: The Indirect Adaptive Approach To Regime Change. Global Research, Moscow, 2015. 159 pp.

В свой книге 2015 г. *Гибридные войны: непрямой адаптивный подход к смене режимов* Э. Корыбко внимательно изучает и описывает возникший более десяти лет назад феномен *цветных революций*. В основу книги легло солидное исследование, которое автор проводил в течение нескольких лет. Он провел анализ того, каким образом Соединенные Штаты ведут гибридные и неконвенциональные войны с целью смещения правящих режимов в странах, окружающих ядро евразийского материка, и используют их результаты для дестабилизации периферии сво-

их стратегических противников — России, Китая и Ирана. Область исследования весьма нова и открывает серьезные перспективы для будущих исследователей. В этом смысле работу по праву можно назвать пионерской. В книге приводятся описание и анализ конкретных случаев, что дает читателю довольно полное представление о методах, которые используют США, пытаясь сохранить глобальное лидерство в мире, который на глазах становится многополярным. Процессы хаотизации Сирии и Украины, сходства и различия двух случаев также подробно разбираются в книге.

В названии книги зафиксированы два подхода: смена режима и ведение гибридной войны, которые ясно описаны и подробно расшифровываются. При попытке смены режима организация *цветной революции* — очень удачный и целесообразный первый шаг, поскольку занимает мало времени, требует меньших затрат и позволяет достичь неплохих результатов. Автор перечисляет случаи, имевшие место на периферии Евразии, и подробно разбирает некоторые из них. Кроме того, в книге анализируется ситуация вокруг Украины. Особое внимание уделяется методам и каналам, используемым для ведения *непрямой войны*, в частности социальным сетям и средствам массовой информации. По мере путешествия по страницам книги читатель знакомится с методами организации и провокации огромной толпы, отбора руководителей.

Второй вид смены режима, намного более затратный, применяется в случае провала *цветной революции.* Его можно описать термином *нетрадиционная война*. Речь идет о разжигании вооруженного конфликта между правительством и гражданами либо о полноценной гражданской войне, которая развязывается для достижения политических целей. В качестве примера приводится продолжающаяся война в Сирии. Второй тип смены режима является менее востребованным, потому что сопряжен с большими издержками, как в политическом, так и в экономическом плане, и не позволяет надеяться на быстрое достижение цели. Таким образом, результат становится менее определенным. В книге подчеркивается тот факт, что смена режима будет вестись независимо от социальных, экономических и физических последствий для населения страны.

Исследование настоятельно рекомендуется для всех интересующихся международной политикой для лучшего понимания широко распространенной трактовки причин современных конфликтов в Евразии и на Ближнем Востоке. Книга Корыбко безусловно откроет читателю глаза на новую реальность.

Умат Аслан

Confidential

RUSSIA

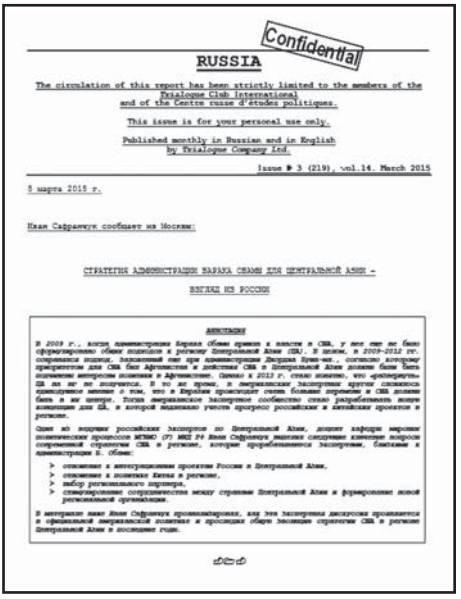
The circulation of this report has been strictly limited to the members of the *Trialogue* Club International. This issue is for the personal use only.

ИСТОЧНИК В МОСКВЕ СООБЩАЕТ:

ПИР-Центр и Международный клуб Триалог информируют о развитии аналитического проекта RUSSIA CONFIDENTIAL.

ЦЕЛИ ПРОЕКТА:

- аналитическое сопровождение новостей мировой политики;
- информирование читателей об особенностях и нюансах внешней политики России.


Confidential

RUSSIA

The circulation of this report has been strictly limited to the members of the Trialogue Club International and of the Centre russe d'études politiques.

This issue is for your personal use only.

Published monthly in Russian and in English by Trialogue Company Ltd.

Issue ▶ 3 (219), vol.14. March 2015

5 марта 2015 г.

Иван Сафранчук сообщает из Москвы:

СТРАТЕГИЯ АДМИНИСТРАЦИИ БАРАКА ОБАМЫ ДЛЯ ЦЕНТРАЛЬНОЙ АЗИИ – ВЗГЛЯД ИЗ РОССИИ

АННОТАЦИЯ

В 2009 г., когда администрация Барака Обамы пришла к власти в США, у них еще не было сформулировано обзора подходов к региону Центральной Азии (ЦА). В целом, в 2009-2012 гг. сохранялся подход, заложенный еще при администрации Джорджа Буша-мл., согласно которому приоритетом для США был Афганистан и действия США в Центральной Азии должны были быть подчинены интересам политики в Афганистане. Однако к 2013 г. стало понятно, что «достигнуть ЦА не мог не получится. В то же время, в американских экспертных кругах сложилось единодушное мнение о том, что в Вашингтоне происходит очень большое переоценка в США должно быть в их центре. Тогда американское экспертное сообщество стало разрабатывать новую концепцию для ЦА, в которой надлежало учесть прогресс российских и китайских проектов в регионе.

Одно из ведущих российских экспертов по Центральной Азии, доцент кафедры мировых политических процессов МГИМО (У) МИД РФ Иван Сафранчук выделил следующие ключевые вопросы современной стратегии США в регионе, которые прорабатываются экспертами, близкими к администрации В. Обамы:

- отношение к интеграционным проектам России в Центральной Азии,
- отношение к политике Китая в регионе,
- набор региональных партнеров,
- стимулирование сотрудничества между странами Центральной Азии и формирование новой региональной организации.

В материале Ивана Сафранчука проанализированы, как эти экспертные дискуссии применяются в официальной американской политике и происходит сборе эволюция стратегии США в регионе Центральной Азии в последние годы.

- аналитическое сопровождение новостей мировой политики;
- информирование читателей об особенностях и нюансах внешней политики России.

В ПРОШЛЫХ НОМЕРАХ:

- В шаге от сделки: российско-американские рекомендации для всеобъемлющего соглашения по иранской ядерной программе
- Есть ли будущее у договора о ликвидации ракет средней и меньшей дальности
- Военно-техническое сотрудничество в новых реалиях: кризис вокруг Украины, западные санкции и российский ОПК
- Поворот России на Восток: проблемы и перспективы
- Стратегия администрации Барака Обамы для Центральной Азии - взгляд из России
- БРИКС в глобальном управлении интернетом: время для шага вперед?

В основе каждого номера RUSSIA CONFIDENTIAL — эксклюзивные материалы, переданные в редакцию аналитиками из разных точек мира.

Бюллетень RUSSIA CONFIDENTIAL выходит ежемесячно; рассылка осуществляется по электронной почте членам Международного клуба *Триалог* на русском или английском языках — по выбору получателя.

Международный клуб Триалог: **secretary@trialogue-club.ru**
Russia Confidential: **rc.pircenter.org**

Confidential

ИСЛАМСКОЕ ГОСУДАРСТВО И ЯДЕРНОЕ ОРУЖИЕ

С интересом прочитал опубликованную в прошлом номере *Индекса Безопасности* статью Антона Уткина *Исламское государство — новый участник химической войны?* Хотел бы попытаться ответить на вопрос, который, безусловно, заслуживает пристального внимания и анализа, — о возможностях запрещенной террористической организации *Исламское государство* (ИГ) в каком-то виде использовать ядерный компонент в военных действиях на территории Сирии или Ирака или в террористических целях на территории других государств.

Рассматривая возможности ИГ по созданию и применению ядерных или радиоактивных материалов, необходимо оценить следующие составляющие:

1. Наличие информации о свойствах и возможных последствиях применения ядерного материала или радиоактивного вещества;
2. Интеллектуальный потенциал участников ИГ;
3. Наличие исходных материалов;
4. Наличие производственных мощностей;
5. Способность обеспечить доставку и привести заряд в действие.

Рассмотрим каждую из них.

1. Информация о свойствах и возможных последствиях применения ядерного материала или радиоактивного вещества широко представлена в интернете, поэтому сложностей с ее получением не возникнет. Это вопрос только времени и квалификации людей, которым это будет поручено.
2. Вопрос интеллектуального потенциала людей, примкнувших к ИГ, требует прояснения на уровне национальных служб безопасности тех государств, из которых уехали участники ИГ. Вполне вероятно, что под знамена террористов встали люди с высшим или средним образование в технической области, т. е. имеющие знания по основам физики и химии. Собрать и обобщить основную информацию по тем материалам, которые могут попасть им в руки, или заказать поиск нужных материалов на территории, захваченной ИГ или за рубежом, по-видимому, не представит большой сложности для таких специалистов.

3. По состоянию на март 2003 г. (после выведения групп инспекторов ЮНМОВИК из Ирака) ядерный компонент программы ОМУ Ирака выглядел следующим образом:

- Все ядерные материалы оставались на складе в ядерном центре Тувайта под печатями МАГАТЭ. Ядерные материалы в основном содержали уран естественного обогащения. Обогащенное топливо исследовательского реактора было вывезено еще в 1992 г. (свежее в Россию, а облученное — в Великобританию);
- Различные радиоактивные источники, разбросанные по территории Ирака, были учтены и оставлены в местах их использования;
- Хранилище высокоэффективной взрывчатки типа RDX/HVX на заводе Аль Ка Ка находилось под печатями МАГАТЭ. Эта взрывчатка была закуплена Ираком для проведения взрывных экспериментов в секретной ядерной программе.

Инвентарные списки ядерных материалов и радиоактивных источников находились в офисе ядерной группы инспекторов МАГАТЭ (Action Team 687) в Вене, а их копии — в иракском офисе комиссии по мониторингу (контактная организация с иракской стороны).

Ядерные материалы, находившиеся на территории Ирака в 1993 г., напрямую использовать для создания примитивного взрывного устройства не представляется возможным. Доработать эти материалы до нужного состояния (через обогащение, например) также невозможно. Получить необходимое количество ядерного материала нужного качества для создания примитивного ядерного взрывного устройства с помощью контрабанды из-за рубежа представляется чрезвычайно маловероятным. Даже разработать проект такого устройства и приобрести все необходимые компоненты (помимо ядерного материала) — задача, которая потребует слишком много времени и усилий, тем более в условиях постоянных военных действий. Вариант приобрести готовое ядерное взрывное устройство или выкрасть его (например, с американской базы на территории ЕС или Турции) скорее напоминает сюжет для фильма о Джеймсе Бонде, чем реальность. По моему личному мнению, создать и применить ядерное оружие ИГ не сможет.

Другой вопрос — *грязная бомба*. Собрать какое-то количество радиоактивного материала, например извлечь его из гражданских источников (ядерных установок, используемых в госпиталях, на промышленных предприятиях и др.), находящихся на подконтрольной ИГ территории, наверное, возможно. Потребуется группа специалистов и специальное оборудование для сбора, транспортировки, обработки и хранения радиоактивных источников и извлеченного радиоактивного материала. Упаковать радиоактивный материал в простейший контейнер с взрывчаткой с соответствующим оформлением — технически несложная задача. Обеспечить хранение этого устройства и его дальнейшую транспортировку — задача сложная, но решаемая. Вопрос о наличии взрывчатки обсуждать не приходится.

4. Оценивая производственную базу для изготовления *грязной бомбы*, можно учесть информацию командования российских ВКС, которая связана с ударами, наносимыми по *производственным зданиям по изготовлению примитивных взрывных устройств*. Очевидно, что на территории, занятой ИГ, таких зданий (мастерских) имеется много. Безусловно, не все эти мастерские пригодны для таких работ, поэтому потребовалось бы приобрести специальное оборудо-

вание и установить его. На территории, подконтрольной ИГ, может находиться несколько установок, которые были задействованы в секретной ядерной программе Ирака. Однако наиболее важные компоненты большинства этих установок либо приведены в непригодное для использования состояние, либо собраны в центральное хранилище в районе ядерного центра Тувайта южнее Багдада, т. е. находятся на территории, подконтрольной правительству.

5. Наконец, необходимо попытаться оценить цель, которую могут выбрать террористы для использования *грязной бомбы*. Взрывные устройства (машины, начиненные взрывчаткой, смертники с поясами шахидов и др. акции с применением взрывчатки) использовались террористами неоднократно. Как правило, взрывы устраиваются в местах скопления людей — на рынках, стадионах, в торговых центрах и других общественных местах.

Основной эффект от применения *грязной бомбы* кроме обычных разрушений и прямых жертв — это загрязнение места проведения акции и дальнейшее отчуждение загрязненной территории (кратковременное или долговременное) до ее дезактивации, заниматься которой до окончания военных действий никто, скорее всего, не будет. Это само по себе служит серьезным сдерживающим фактором.

Если же предположить, что несмотря на все сложности террористы решились бы на создание *грязной бомбы*, местом ее применения они скорее всего выбрали бы крупный город на территории, подконтрольной правительству Сирии или Ирака, либо за пределами подконтрольной ИГ территории, но в непосредственной от нее близости — в любом месте, куда сможет доехать транспорт (автомашина, фура, морское судно небольшого размера и др.). Поскольку исполнителями террористических актов, как правило, становятся смертники, высока вероятность доведения акции до максимально запланированного финала, если только подготовка акции со всеми деталями (место изготовления заряда, организаторы и исполнители, предполагаемое место акции, пути доставки и другие детали) не будет своевременно раскрыта.

Резюмируя: вероятность создания ИГ ядерного оружия пренебрежимо мала. Теракт с использованием радиоактивных и ядерных материалов в теории возможен, но на практике также маловероятен, особенно с учетом того, что у данной террористической организации в избытке имеются обычные вооружения, использование которых не связано с серьезными сложностями и, как показали недавние события в Париже, дает желаемый результат

Геннадий Пшакин,
бывший инспектор UNSCOM/UNMOVIC в Ираке

Членство в Клубе включает в себя: **ПРИГЛАШЕНИЯ** на заседания Клуба и мероприятия ПИР-Центра; **ПОДПИСКУ** на электронную версию журнала *Индекс Безопасности*, на ежемесячный бюллетень эксклюзивной аналитики *Russia Confidential* и другие публикации; **ДОСТУП** к монографиям и докладам Клуба и его партнеров.

Международный клуб *Триалог*, отметивший свое двадцатилетие в 2013 г., является местом встреч дипломатов, экспертов и представителей бизнеса.

Триалог — международный экспертный клуб, предлагающий своим членам профессиональный взгляд на внешнюю политику России и эксклюзивный анализ подходов страны к ключевым вопросам международной повестки дня.

В состав клуба *Триалог* входят более 40 индивидуальных и корпоративных членов, включая дипломатов, экспертов и бизнесменов.

На заседаниях Клуба выступали заместитель министра обороны РФ Анатолий **Антонов**, Постоянный представитель России при ОДКБ Виктор **Васильев**, президент Группы разработки финансовых мер борьбы с отмыванием денег Владимир **Нечаев**, председатель комитета Государственной Думы РФ по образованию Вячеслав **Никонов**, заместитель министра иностранных дел РФ Сергей **Рябков**.

Заседания Клуба проводятся четыре раза в год в Москве и один раз в год за рубежом в формате делового завтрака. Общение носит неформальный характер, основной доклад сопровождается серией вопросов и ответов.

secretary@trialogue-club.ru — телефон: +7 (985) 764-98-96

FROM THE EDITOR

INTERVIEW

ANALYSIS

COMMENTARY

INTERNATIONAL REVIEW

ОБ АВТОРАХ

Баклицкий Андрей Александрович — директор программы ПИР-Центра «Россия и Ядерное нераспространение». Научный сотрудник Центра глобальных проблем и международных организаций Дипломатической академии МИД России. Редактор бюллетеня *Ядерный Контроль.* Выпускник факультета международных отношений Уральского федерального университета. Специалист в области регионоведения. В 2008–2009 гг. проходил обучение в Университете Севильи (Испания). Выпускник Международной Летней школы по проблемам безопасности 2011. В 2011–2013 гг. — Руководитель Интернет-проекта ПИР-Центра, с 2013 — Директор информационных проектов ПИР-Центра. Участник сессий подготовительного комитета к Обзорной конференции ДНЯО 2013–2014 гг. и Обзорной конференции ДНЯО 2015 г. Редактор Белой Книги ПИР-Центра «Десять шагов к зоне, свободной от оружия массового уничтожения, на Ближнем Востоке», редактор доклада «Иран в региональном и глобальном контексте». Сфера научных интересов: международная безопасность, большой Ближний Восток, ядерная энергетика и ядерное нераспространение.

Ван Гоюй — заместитель директора Института космического права Пекинского Технологического Института. Доктор юрид. и эконом. наук. Доцент. Выпускник Цзилиньского университета (2005), получил степень магистра международного права. Защитил докторскую диссертацию в 2008 г. С 2014 г. является старшим научным сотрудником Королевского института международных отношений (Великобритания). Консультант по вопросам космической безопасности Института ООН по исследованию проблем разоружения (ЮНИДИР, 2015). Входил в состав делегаций Китая в Комитете ООН по использованию космического пространства в мирных целях (КОПУОС) и Межучрежденческого координационного комитета по космическому мусору (МККМ). Участвовал в заседаниях Рабочей группы КОПУОС по долгосрочной устойчивости космической деятельности в качестве эксперта с китайской стороны. Опыт работы включает анализ юридических и политических аспектов проблем в сфере космической безопасности, таких как контроль над вооружениями в космическом пространстве, предупреждение образования и ликвидация космического мусора, кибербезопасность в космическом пространстве, использование космических ресурсов и урегулирование кризисных ситуаций

в космосе, управление космическим движением и глобальное управление в космической области.

Гаврилова Мария Станиславовна — старший юридический советник Региональной делегации Международного Комитета Красного Креста в Российской Федерации, Беларуси и Молдове. В 2011 г. окончила Московский государственный юридический университет им. О. Е. Кутафина по направлению «международное право». В 2013 г. получила степень магистра в области изучения проблем мира в Университете Нотр Дам (Индиана, США), специализировалась на политическом анализе и политических преобразованиях. В 2012 г. была юридическим стажером некоммерческой организации «Раввины за права человека» (Израиль). С 2013 г. участвовала в различных программах Международного Комитета Красного Креста. В 2014 г. работала юристом совместной программы Правозащитного центра «Мемориал» и Европейского центра по защите прав человека «Защита прав человека с использованием международным механизмов». Научные интересы: защита прав человека в условиях вооруженного конфликта, право оккупации, *jus post bellum*. Владеет английским языком.

Демидов Олег Викторович — консультант ПИР-Центра. Аспирант Факультета политологии МГИМО (У) МИД России (с 2010 г.). Закончил факультет государственного управления МГУ имени Ломоносова. В 2011–2012 гг. занимал позицию координатора проектов Центра политических и международных исследований (ЦПМИ) при Международной Федерации мира и согласия (ФМС). С 2012 г. — эксперт Комиссии по информационной безопасности и киберпреступности Российской ассоциации электронных коммуникаций (РАЭК). Выпускник Зимней школы-2011 Центра международной и региональной политики (CIRP), выпускник Международной Летней Школы ПИР-Центра по проблемам глобальной безопасности. Участник Рабочей группы по кибербезопасности АТССБ в 2011 г., участник международного проекта «*Новый Концерт держав в XXI веке*» Франкфуртского института по изучению проблем мира и конфликтов (PRIF) (2011–2014 гг.). Автор ряда статей и исследований по вопросам информационной безопасности, глобального управлению интернетом, развития БРИКС в журнале *Индекс Безопасности* и ряде других изданий. Является Секретарем Рабочей группы ПИР-Центра при Экспертно-Консультативном Совете по международной информационной безопасности и глобальному управлению интернетом с 2012 года. В 2012–2014 гг. — координатор, директор программы «Международная информационная безопасность и глобальное управление интернетом».

Евстафьев Дмитрий Геннадиевич — Профессор Кафедры интегрированных коммуникаций Высшей школы экономики. Канд. полит. наук. Эксперт-политолог. Профессор Национального исследовательского университета — Высшей школы экономики. Ранее — заместитель генерального директора Национальной лаборатории внешней политики, вице-президент ЗАО «Компания развития общественных связей» (КРОС). Также работал в качестве директора Департамента по информационной политике ОАО «Техснабэкспорт». В 1995–2003 гг. — старший научный сотрудник ПИР-Центра. Ранее — ведущий и старший научный сотрудник Российского института стратегических исследований (РИСИ) и Института США и Канады РАН (ИСКРАН). Сфера научных интересов — военно-политические аспекты национальной безопасности России, проблемы внешней и военной политики США, региональные аспекты нераспространения ядерного оружия. Член Редакционной

коллегии журнала *Индекс Безопасности*. Является членом Совета ПИР-Центра с 2014 года.

Козик Андрей Леонидович — генеральный секретарь Ассоциации международного права. Канд. юрид. наук (международное право), доцент. Окончил Академию управления при Президенте Республики Беларусь (2000). Получил образование в области экономики и финансов в Международном университете «МИТСО» (2011), прошел аттестацию ICFM. Работал в министерстве иностранных дел Белоруссии. Стаж преподавательской деятельности более 15 лет. В качестве приглашенного профессора работал в Белоруссии, России, Азербайджане, Армении, Бельгии. В 2001–2005 гг. работал в издательском доме *JW*, возглавлял юридический отдел, был вице-президентом. Был одним из основателей юридической фирмы *АргументЪ* (ныне *Алейников и Партнеры*). В 2005–2014 гг. занимал административные должности в Международном университете «МИТСО», последняя из которых — первый заместитель ректора университета. В качестве эксперта сотрудничал с правительством Республики Беларусь, Всемирным банком, Международной организацией труда, Управлением Верховного комиссара по правам человека, Международным Комитетом Красного Креста. Является арбитром двух международных арбитражей. В качестве члена экспертной группы работал в Группе правительственных экспертов ООН по информационной безопасности. Член совета директоров Международного общества права войны и международного права (Брюссель). Член комиссии по имплементации Международного гуманитарного права при Совете Министров Республики Беларусь (Минск). Член редакционных советов журналов и ежегодников по международному праву в России, Украине, Армении, Белоруссии. Член рабочей группы *Таллинского руководства v. 2.0*. Автор более 40 научных публикаций, включая 5 книг.

Колесников Андрей Вячеславович — директор Координационного центра национального домена сети Интернет (2009–2015 гг.). Начал свою работу в области телекоммуникаций в 1988 г., занимаясь общественными инициативами по установлению телекоммуникационных мостов между СССР и США. В 1993 г. был одним из восьми представителей интернет-провайдеров, которые подписали соглашение, на основе которого был делегирован национальный домен .RU. В 1994 г. Андрей Колесников принимал участие в разработке первой лицензии на телематические услуги, а в 1995 — руководил запуском первой в России массовой интернет-услуги «Россия-Он-Лайн». В 2000 г. в рамках ECOSOC в ООН представлял Россию в части разработки первой международной концепции по информационным и коммуникационным технологиям, впоследствии принятой лидерами стран G8 в Окинаве как документ «Окинавская Хартия Глобального Информационного Общества». С 2005 по 2009 гг. являлся членом Совета КЦ НДСИ, а также занимал должность заместителя медиа директора Вымпелкома, телекоммуникационного гиганта России. Награждён почётной грамотой Министра связи и массовых коммуникаций РФ, входит в состав программных, экспертных комитетов крупнейших российских интернет-форумов и конференций. В 2010 г. стал одним из инициаторов создания Евроазиатской группы сетевых операторов (ENOG). На международном уровне Андрей Колесников выступает за более активное включение России в процессы управления и развития интернета, представляет интересы российского интернет-сообщества, регулярно участвует в интернациональных конференциях и глобальных форумах, таких как IGF, конференции ICANN, RIPE,

CENTR, APTLD, заседаниях МСЭ и других. В 2009 г. был избран в члены Правления gNSO и стал первым российским экспертом, вошедшим в состав управляющих органов корпорации ICANN.

Лукацкий Алексей Викторович — бизнес-консультант по информационной безопасности Cisco Systems. В 1996 году окончил Московский институт радиотехники, электроники и автоматики (МИРЭА) по специальности «Прикладная математика» (специализация — «Защита информации»). Входит в рабочую группу ЦБ по разработке требований по безопасности Национальной платежной системы (382-П). Участвует в экспертизе нормативно-правовых актов, в области информационной безопасности и персональных данных. Является участником Подкомитета № 1 «Защита информации в кредитно-финансовой сфере» Технического Комитета № 122 «Стандартизация финансовых услуг» Федерального агентства по техническому регулированию и метрологии. Является участником Подкомитета № 127 «Методы и средства обеспечения безопасности ИТ» Технического комитета № 22 «Информационные технологии» Федерального агентства по техническому регулированию и метрологии. Является участником Технического комитета № 362 «Защита информации» Федерального агентства по техническому регулированию и метрологии и ФСТЭК. Член Консультативного совета при Роскомнадзоре по защите прав субъектов персональных данных. Член Рабочей группы при ЭКС Пир-Центра по международной информационной безопасности и глобальному управлению Интернетом с 2012 года. С 2014 года — член Экспертного совета ПИР-Центра.

Макарова Ольга Вячеславовна — директор Департамента Интернет и канальных ресурсов ПАО МТС. Закончила МГТУ им. Баумана по специальности инженер-системотехник. Работает в телеком-сфере с 1998 г. Была начальником коммерческого отдела в Центре информационных технологий в должности начальника коммерческого отдела. В 2001 г. перешла на работу в *ЗАОМТУ-Интел* (торговая марка *Точка RU*) на должность начальника отдела взаимодействия с операторами связи. Принимала участие в формировании пиринговой политики и создании региональных Tier 1 в России. Работала в качестве руководителя Департамента разработки и управления продуктами ЗАО *Телеком — Центр* (впоследствии присоединен к ЗАО *Синтерра*). Занималась разработкой продуктов и услуг, реализуемых с использованием технологии *WiMax*, а также продуктового ряда контентных услуг Компании, включая услуги IP-TV. С 2011 г. работает в ПАО МТС в должности директора Департамента Интернет и канальных ресурсов Блока по развитию операторского бизнеса Корпоративного Центра. В 1999–2006 гг. участвовала в рабочих группах АДЭ по вопросам, связанным с разработкой положений ФЗ-127 «О связи». В 2007–2008 гг. участвовала в рабочих группах Мининформсвязи РФ по вопросам развития интернета в России и построения сетей передачи данных. Неоднократно участвовала в качестве докладчика на выставках и конференциях, включая ИнфоКом, CSTB, Transnet, Broadband Russia и др. В настоящий момент участвует в различных рабочих группах по обсуждению и формированию предложений в части сетевого нейтралитета, взаимодействия с контент-сервис провайдерами, антипиратского законодательства, блокировок в сети Интернет и др. Является членом Совета Координационного центра национального домена сети Интернет.

Малов Андрей Юрьевич — старший советник Постоянного представительства Российской Федерации при Отделении ООН и других международных организа-

циях в Женеве. Канд. истор. наук. Окончил переводческий факультет Московский государственный педагогический институт иностранных языков им. М. Тореза. Работал в Комитете молодежных организаций СССР. С 1991–1994 гг. занимался исследовательской и преподавательской деятельностью в Институте экономических стратегий РАН (Москва). В 1992 г. работал приглашенным преподавателем в Западном Международном Университете США (Финикс, Аризона). С 1994 г. — сотрудник МИД РФ. Работал в «горячих точках» по линии ОБСЕ: в Нагорном Карабахе (1994–1996 гг.), а также в Боснии и Герцеговине (1996–1998 гг.). С 1998 г. занимается в МИД РФ вопросами контроля над вооружениями, нераспространения и разоружения. Участник переговоров в области многостороннего разоружения.

Мостинская Ольга Сергеевна — главный редактор *Индекса Безопасности*. 2003 г. окончила Московский государственный лингвистический университет, изучала лингвистику и межкультурную коммуникацию. В 1999–2000 гг. была вольным слушателем факультета социологии и антропологии Universite Libre de Bruxelles (Бельгия). В 2005–2015 гг. работала в Министерстве иностранных дел России, завершила службу в должности советника Департамента лингвистического обеспечения.

Мостовюк Михаил Анатольевич — Государственный советник Российской Федерации 2 класса. Канд. юрид. наук. С 2001 г. проходил службу в центральном аппарате МВД России. В 2009–2013 гг. работал в посольстве России во Франции. Основные научные интересы связаны с вопросами противодействия новым вызовам и угрозам. Автор ряда публикаций.

Стрельцов Анатолий Александрович — заместитель директора Института проблем информационной безопасности МГУ имени М. В. Ломоносова. Доктор техн. наук, доктор юрид. наук, профессор. Заслуженный деятель науки Российской Федерации. Действительный государственный советник Российской Федерации 3 класса. Полковник в отставке. Окончил Военную артиллерийскую академию имени М. И. Калинина (1969). До 1994 г. проходил службу на различных должностях в организациях Министерства обороны России, занимался, в частности, созданием автоматизированных систем управления. В 1994–2011 гг. работал в аппарате Совета Безопасности РФ на должностях от консультанта до начальника департамента проблем информационной безопасности. Член российской делегации на консультациях по проблематике информационной безопасности в США, Бразилии, Китае и других странах. Автор более 160 научных работ, ряда монографий по теме обеспечения информационной безопасности России и международной информационной безопасности.

Палажченко Павел Русланович — руководитель Службы международных связей и контактов с прессой «Горбачев — Фонда». Окончил Московский государственный педагогический институт иностранных языков им. М. Тореза в 1972 году. После окончания курсов переводчиков ООН работал в Секретариате ООН в Нью-Йорке (1974–1979). С 1980 работал в МИД СССР, с 1991 — в аппарате Президента СССР. Принимал участие в переговорах между СССР и США по вопросам безопасности и разоружения, а с 1985 года был переводчиком на советско-американских встречах министров и на высшем уровне. Участник саммитов лидеров СССР и США в Женеве, Рейкьявике, Вашингтоне, Москве, на Мальте, в Хельсинки и вновь в Москве в 1991. С 1992 г. работает в Горбачев-Фонде, с 1996 года — руководитель Службы международных связей и контактов. Автор книг My Years with Gorbachev

and Shevardnadze (1997) («Мои годы с Горбачевым и Шеварднадзе»), «Мой несистематический словарь» (2006), а также многочисленных статей в российской и зарубежной прессе по истории перестройки и проблемам современной российской и международной политики.

Пшакин Геннадий Максимович — ведущий научный сотрудник Лаборатории ФЭИ по анализу стратегии развития ядерной энергетики в части нераспространения и применения гарантий. Канд. техн. наук (1980). Окончил Московский технический университет им. Баумана (1965). В 1965–1985 гг. работал в Физико-энергетическом институте в области физических вопросов ядерной безопасности быстрых реакторов. Участвовал в пусках советских быстрых реакторов БОР-60, БН-350, БН-600 в качестве физика. В 1985–1993 гг. был командирован в МАГАТЭ и работал в качестве инспектора отдела операций «А» по гарантиям странах дальнего востока: Индии, Вьетнаме, Австралии, Индонезии, Южной Корее, Филиппинах, Китае — а также в Канаде. В 1993–2012 гг. — начальник бюро по нераспространению международного отдела Физико-энергетического института им. А. И. Лейпунского (ФЭИ, Обнинск), координатор программы сотрудничества *ФЭИ — национальные лаборатории США* по учету, контролю и физической защите ядерных материалов. Участвовал в работах по трехсторонней инициативе, в организации учебных курсов МАГАТЭ, в разработке концепции второй линии защиты, в разработке лекционных материалов и представлении лекций по проблеме нераспространения на курсах УМЦУК и других курсах, проводимых ЦИПК. В 1995, 1996, 1997 и 2002–2003 гг. участвовал в качестве инспектора в мониторинге и уничтожении ядерной программы Ирака в составе группы инспекторов МАГАТЭ (Action Team 687). В 1996–2003 гг. принимал участие в технических проработках по подготовке режима международных проверок избыточных оружейных материалов в рамках трехсторонней инициативы. С 2002 г. по настоящее время участник рабочих групп по проекту ИНПРО в части защищенности инновационных ядерных энергетических систем от распространения. Участник подготовки документов МАГАТЭ по учету мер гарантий на ранней стадии проектирования ядерных установок. Является руководителем Аналитического центра по нераспространению в рамках проекта *РАНСАК*. Является членом INMM с 1997 г. и президентом Обнинского отделения Института по обращению с ядерными материалами (INMM). Соавтор ряда публикаций по проблемам сохранности ядерных материалов на конференциях INMM в 1996–2015 гг., соавтор учебников по проблемам ядерного нераспространения и других публикаций по данной теме.

Роскошная Мария Станиславовна — консультант отдела ядерной техники Управления экспортного контроля Федеральной службы по техническому и экспортному контролю России (ФСТЭК). Советник государственной гражданской службы 3 класса. Выпускница Московского государственного университета экономики, статистики и информатики (МЭСИ), институт менеджмента (2012). В 2014 г. окончила магистратуру Финансового Университета при Правительстве Российской Федерации по совместной программе с Внешэкономбанком «Управление проектами государственно-частного партнерства». Проходила профессиональную переподготовку в Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, стажировку в Женевском институте международных отношений и развития. Участвовала в образовательной программе Университета Джорджии «Стратегический трейд менеджмент» (2011).

Участница Международной Летней Школы ПИР-Центра 2013. В настоящее время обучается в аспирантуре Института мировой экономики и международных отношений Российской академии наук (ИМЭМО РАН) по специальности «Мировая экономика». Проходила практику в ГК *Внешэкономбанк* (2014). В составе делегации Российской Федерации участвовала в заседаниях по программе Госдепартамента США «Экспортный контроль и безопасность границ» и в мероприятиях по формированию Российско-Китайской рабочей группы по экспортному контролю и торговле продукцией двойного назначения в рамках Российско-Китайской комиссии по подготовке регулярных встреч глав правительств. Награждена медалью ФСТЭК России «За укрепление государственной системы защиты информации» II степени.

Сентюрин Юрий Петрович — заместитель министра энергетики Российской Федерации. Канд. полит. наук (2007). Окончил Военный Краснознаменный институт по специальности «референт-переводчик» (1982), Военно-дипломатическую академию Советской Армии (1991). В 1997 г. прошел обучение в ФГБОУ ВПО «Всероссийская академия внешней торговли Министерства экономического развития РФ» по специальности «мировая экономика». В 2002 г. — Российскую академию государственной службы при Президенте РФ по специальности «юриспруденция». В 1977–1995 гг. служил в Вооружённых силах СССР и России. В 1982–1986 гг. служил военным переводчиком в Афганистане. В 1991–1995 гг. служил в Генштабе ГРУ. В 1995–1998 гг. работал в транспортной компании «Русский мир», последняя должность — директор департамента. В 1998–1999 гг. занимал должность директора департамента транспорта Фонда развития России. В 1999–2001 гг. руководил Департаментом регулирования естественных монополий на транспорте Министерства Российской Федерации по антимонопольной политике и поддержке предпринимательства. В 2001–2003 гг. работал в правительстве Нижегородской области, последний пост — первый заместитель губернатора — член правительства Нижегородской области. Был депутатом Госдумы ФС РФ четвертого созыва («Единая Россия»), заместителем председателя Комитета Государственной Думы по энергетике, транспорту и связи. В 2007–2010 гг. — статс-секретарь — заместитель министра образования и науки Российской Федерации, затем заместитель министра образования и науки Российской Федерации. 12 ноября 2010 года назначен на должность статс-секретаря — заместителя министра энергетики Российской Федерации. Награжден орденом «За службу Родине» в Вооруженных Силах СССР III степени, медалью «За трудовую доблесть», «За безупречную службу», восемью ведомственными медалями, орденом Славы Демократической Республики Афганистан и медалью «Воину-интернационалисту».

Федоров Юрий Евгеньевич — член Совета ПИР-Центра, член Редакционной коллегии журнала *Индекс Безопасности*. Канд. ист. наук, профессор, член Чешской ассоциации международных исследований, профессор Пражского муниципального университета, ранее — научный сотрудник Королевского института международных отношений (Великобритания). Крупный специалист в области проблем международной безопасности, в том числе энергетической безопасности, контроля над ядерными вооружениями. Его многочисленные научные труды по вопросам стратегических наступательных вооружений, тактического ядерного оружия, противоракетной обороны (ПРО), систем предупреждения о ракетном нападении (СПРН) хорошо известны в России и за рубежом. Возглавлял авторский коллек-

тив и является автором ряда глав в ежегодных Докладах о развитии человеческого потенциала в Российской Федерации, публикуемых Программой развития ООН.

Харьковский Евгений Константинович — советник отдела ядерной техники Управления экспортного контроля ФСТЭК России. Выпускник Национального исследовательского ядерного университета МИФИ (НИЯУ МИФИ). В период с 2006 по 2013 г. обучался на специалитете и в магистратуре Факультета управления и экономики высоких технологий НИЯУ МИФИ по направлению: Международное научно-технологическое сотрудничество. В 2010 г. проходил обучение в Школе кадрового резерва по управлению научно-техническим развитием Государственной корпорации по атомной энергии Росатом. В 2012–2013 годах проходил обучение на Факультете государственного управления МГУ им. М. В. Ломоносова в рамках Федеральной программы подготовки и переподготовки резерва управленческих кадров, утвержденной распоряжением Правительства РФ. Выпускник Международной летней школы ПИР-Центра по проблемам глобальной безопасности. Участник международных конференций по экспортному контролю. Работал в управляющей компании Госкорпорации Росатом в сфере обращения с ОЯТ и РАО (Управление международного сотрудничества), а также компании, осуществляющей экспорт обогащенного уранового продукта и услуг по конверсии и/или обогащению урана, производимых предприятиями российской атомной отрасли (Департамент стратегических коммуникаций). В настоящее время работает на государственной службе в сфере контроля за экспортом и импортом продукции ядерного профиля (Управление экспортного контроля).

ПИР-ЦЕНТР

(по состоянию на 20 ноября 2015 г.)

Андрей А. **Баклицкий**, директор программы *Россия и ядерное нераспространение*

Умат **Аслан**, стажер

Евгений П. **Бужинский**, к.в.н., генерал-лейтенант, председатель Совета

Олег В. **Демидов**, консультант

Дмитрий Г. **Евстафьев**, к.п.н., член Совета

Вячеслав А. **Зайцев**, главный бухгалтер

Альберт Ф. **Зульхарнеев**, директор

Галия Р. **Ибрагимова**, к.п.н., консультант

Наталья И. **Калинина**, д.м.н., член Совета

Дмитрий А. **Ковчегин**, консультант

Вадим Б. **Козюлин**, к.п.н., старший научный сотрудник, член Совета

Александра В. **Куликова**, консультант программы *Глобальное управление интернетом и международная информационная безопасность*

Василий Ф. **Лата**, д.в.н., генерал-лейтенант, консультант

Евгений П. **Маслин**, генерал-полковник, член Совета

Владимир А. **Мау**, д.э.н., член Совета

Алена В. **Махукова**, стажер

Владимир А. **Орлов**, к.п.н., советник и член Совета

Дмитрий В. **Поликанов**, к.п.н., член Совета

Галина Д. **Рассказова**, бухгалтер

Максим В. **Старчак**, консультант

Екатерина А. **Степанова**, д.п.н., член Совета

Денис Д. **Токарев**, стажер

Вячеслав И. **Трубников**, генерал армии, Чрезвычайный и Полномочный Посол, член Совета

Юрий Е. **Федоров**, к.и.н., член Совета

Александра В. **Чепелева**, координатор базы данных, секретать международного клуба *Триалог*

Елена В. **Черненко**, к.и.н., член Совета

ЭКСПЕРТНЫЙ СОВЕТ ПИР-ЦЕНТРА

(по состоянию на 20 ноября 2015 г.)

Айнхорн Роберт, старший научный сотрудник, Брукингский институт, Вашингтон, США (с 2007 г.)

Академия ОБСЕ, Бишкек, Киргизия (с 2010 г.)

Антипов Сергей Викторович, д.т.н., заведующий отделом, Институт безопасного развития атомной энергетики РАН, Москва, Россия (с 2004 г.)

Арбатов Алексей Георгиевич, д.и.н., академик РАН, руководитель, Центр международной безопасности, ИМЭМО РАН, Москва, Россия (с 2004 г.)

Ахтамзян Ильдар Абдулханович, к.и.н., доцент, кафедра международных отношений и внешней политики России, МГИМО (У) МИД РФ, Москва, Россия (с 2002 г.)

Баев Павел Кимович, к.и.н., проф., Международный институт исследований проблем мира, Осло, Норвегия (с 2007 г.)

Барановский Владимир Георгиевич, д.и.н., проф., академик РАН, директор, Центр ситуационного анализа РАН, Москва, Россия (с 2002 г.)

Барзегар Кейхан, директор, Институт стратегических исследований Ближнего Востока, Тегеран, Иран (с 2015 г.)

Васильев Виктор Львович, Полномочный представитель Российской Федерации при Организации Договора о коллективной безопасности, Москва, Россия (с 2015 г.)

Всероссийский научно-исследовательский институт технической физики им. акад. Е. И. Забабахина (ВНИИТФ), Российский федеральный ядерный центр, Снежинск, Россия (с 1999 г.)

Всероссийский научно-исследовательский институт экспериментальной физики (ВНИИЭФ), Российский федеральный ядерный центр, Саров, Россия (с 2002 г.)

Волчинская Елена Константиновна, главный специалист по информационному праву, Фонд «Центр инноваций и информационных технологий», Федеральная нотариальная палата, Москва, Россия (с 2015 г.)

Воронков Владимир Иванович, к.и.н., Постоянный представитель, Постоянное представительство Российской Федерации при международных организациях в Вене, Вена, Австрия (с 2009 г.)

Воронцов Александр Валентинович, к.и.н., заведующий отделом Кореи и Монголии, Институт востоковедения РАН, Москва, Россия (с 2013 г.)

Габуев Александр Тамерланович, руководитель программы «Россия в Азиатско-Тихоокеанском регионе», Московский Центр Карнеги, Москва, Россия (с 2015 г.)

Готтемюллер Роуз, заместитель госсекретаря США по вопросам проверки и соблюдения соглашений по контролю над вооружениями, Вашингтон, США (с 1994 г.)

Данилов Дмитрий Александрович, к.э.н., профессор, ведущий научный сотрудник, заведующий отделом европейской безопасности, Институт Европы РАН, Москва, Россия (с 2011 г.)

Дворкин Владимир Зиновьевич, д.т.н., генерал-майор (в отставке), главный научный сотрудник, ИМЭМО РАН, Москва, Россия (с 2003 г.)

Демидов Олег Викторович, консультант, ПИР-Центр, Москва, Россия (с 2015 г.)

Джонсон Ребекка, д-р, директор, Институт *Акроним*, Лондон, Великобритания (с 1994 г.)

Дханапала Джаянта, посол, президент, Пагуошское движение ученых, председатель Совета Университета ООН, Коломбо, Шри-Ланка (с 2004 г.)

Елеукенов Дастан Шериазданович, д. ф.-м. н., Чрезвычайный и Полномочный Посол, посольство Республики Казахстан в Королевстве Швеция, Стокгольм, Швеция (с 1994 г.)

Есин Виктор Иванович, к.в.н., проф., генерал-полковник (в отставке), консультант Командующего ракетными войсками стратегического назначения, Министерство обороны РФ, Москва, Россия (с 2002 г.)

Женевский центр политики безопасности, Женева, Швейцария (с 2005 г.)

Институт стратегической стабильности, Москва, Россия (с 2005 г.)

Загорский Андрей Владимирович, к.и.н., заведующий отделом разоружения и урегулирования конфликтов, Центр международной безопасности, ИМЭМО РАН, Москва, Россия (с 2014 г.)

Кибароглу Мустафа, заведующий кафедрой, кафедра политологии и международных отношений, Университет MEF, Стамбул, Турция (с 2013 г.)

Кириченко Элина Всеволодовна, к.э.н., руководитель, Центр североамериканских исследований, ИМЭМО РАН, Москва, Россия (с 1994 г.)

Ковчегин Дмитрий Алексеевич, независимый эксперт, Москва, Россия (с 2015 г.)

Кожокин Евгений Михайлович, д.и.н., профессор, проректор по научной работе, МГИМО (У) МИД РФ, Москва, Россия (с 2010 г.)

Кортунов Андрей Вадимович, к.и.н., генеральный директор, Российский совет по международным делам, Москва, Россия (с 2003 г.)

Краснов Алексей Борисович, начальник управления, Управление пилотируемых программ, Федеральное космическое агентство, Москва, Россия (с 2003 г.)

Лаверов Николай Павлович, д.г. -м.н., проф., академик РАН, Москва, Россия (с 2002 г.)

Ладыгин Федор Иванович, генерал-полковник (в отставке), советник генерального директора, Авиационная холдинговая компания *Сухой*, Москва, Россия (с 2002 г.)

Лебедев Владимир Владимирович, заместитель руководителя департамента, Департамент внешнеэкономических и международных связей, правительство Москвы, Москва, Россия (с 2000 г.)

Лукацкий Андрей Викторович, консультант по информационной безопасности, компания Cisco, Москва, Россия (с 2014 г.)

Лукьянов Федор Александрович, председатель Президиума, Совет по внешней и оборонной политике (СВОП), Москва, Россия (с 2010 г.)

Лысенко Михаил Николаевич, к.ю.н., заведующий кафедрой «Международные отношения», Национальный исследовательский ядерный университет «МИФИ», Москва, Россия (с 2004 г.)

Льюис Патриция, д-р, директор по исследованиям, *Chatham House*, Лондон, Великобритания (с 1994 г.)

Маргелов Михаил Витальевич, вице-президент, АК «Транснефть», Москва, Россия (с 2002 г.)

Медриш Михаил Абрамович, директор, Фонд содействия развитию интернета «Фонд поддержки интернет» Москва, Россия (с 2015 г.)

Международная жизнь, журнал, Москва, Россия (с 2010 г.)

Московский государственный институт международных отношений (Университет) МИД РФ, Москва, Россия (с 1994 г.)

Мостинский Сергей Борисович, советник президента, ОАО «Группа Е4» (с 2015 г.)

Мурогов Виктор Михайлович, д.т.н., профессор, Государственный технический университет атомной энергетики, Обнинск, Россия (с 2009 г.)

Мурсанков Сергей Геннадьевич, Москва, Россия (с 2010 г.)

Мюллер Харальд, д-р, проф., член совета, Институт проблем мира, Франкфурт, Германия (с 1997 г.)

Мясников Евгений Владимирович, к.ф.-м.н., директор, Центр по изучению проблем контроля над вооружениями, энергетики и экологии, Долгопрудный, Россия (с 2011 г.)

Национальный исследовательский ядерный университет «МИФИ», Москва, Россия (с 1994 г.)

Наумкин Виталий Вячеславович, д.и.н., проф., член-корр. РАН, научный руководитель, Институт востоковедения РАН, Москва, Россия (с 2014 г.)

Никитин Александр Иванович, д.п.н., проф., директор, Центр политических и международных исследований, Москва, Россия (с 1994 г.)

Пархалина Татьяна Глебовна, к.и.н., заместитель директора, ИНИОН РАН, директор, Центр по изучению проблем европейской безопасности ИНИОН РАН, Москва, Россия (с 2002 г.)

Пономарев-Степной Николай Николаевич, д.т.н., проф., академик РАН, Москва, Россия (с 2002 г.)

Поттер Уильям, проф., директор, Центр изучения проблем нераспространения им. Дж. Мартина, Мидлберийский институт международных исследований, Монтерей, США (с 2014 г.)

Радчук Александр Васильевич, к.т.н., советник начальника Генерального штаба Вооруженных сил РФ, Москва, Россия (с 2009 г.)

Рауф Тарик, директор программы по контролю над вооружениями и нераспространению, Стокгольмский институт исследования проблем мира, Стокгольм, Швеция (с 2013 г.)

РНЦ *Курчатовский институт*, Москва, Россия (с 2002 г.)

Рогачев Илья Игоревич, директор, Департамент по вопросам новых вызовов и угроз, Министерство иностранных дел России, Москва, Россия (с 2011 г.)

Рыбаченков Владимир Иванович, к.т.н., ведущий научный сотрудник, Центр по изучению проблем разоружения, энергетики и экологии, Долгопрудный, Россия (с 2000 г.)

Рыжов Юрий Алексеевич, д.т.н., академик РАН, президент, Международный инженерный университет, Москва, Россия (с 2014 г.)

Савельев Александр Георгиевич, д.п.н., заведующий отделом стратегических исследований, Центр международной безопасности, ИМЭМО РАН, Москва, Россия (с 2002 г.)

Сатановский Евгений Янович, к.э.н., проф., президент, Институт Ближнего Востока, Москва, Россия (с 2004 г.)

Сафранчук Иван Алексеевич, доцент, кафедра мировых политических процессов, МГИМО (У) МИД РФ, Москва, Россия (с 2015 г.)

Сачков Илья Константинович, генеральный директор, *Group-IB*, Москва, Россия (с 2014 г.)

Синайский Александр Сергеевич, д.п.н., проф., секретарь Совета министров обороны государств — участников СНГ, Москва, Россия (с 2014 г.)

Сиринционе Джозеф, президент, Фонд Плаушерс, Вашингтон, США (с 2004 г.)

Скуассони Шэрон, директор и старший научный сотрудник программы «Предотвращение распространения ядерного оружия», Центр стратегических и международных исследований, Вашингтон, США (с 2015 г.)

Солтание Али Асгар, советник вице-президента Ирана и главы Организации по атомной энергии Ирана, Тегеран, Иран (с 2015 г.)

Сумский Виктор Владимирович, д.и.н., директор, Центр АСЕАН при МГИМО (У) МИД РФ, Москва, Россия (с 2012 г.)

Тимербаев Роланд Михайлович, Чрезвычайный и Полномочный Посол, д.и.н., профессор, Москва, Россия (с 2010 г.)

Толорая Георгий Давидович, д.э.н., проф., исполнительный директор, Российский национальный исследовательский комитет БРИКС, Москва, Россия (с 2013 г.)

Тренин Дмитрий Витальевич, к.и.н., директор, Московский центр Карнеги, Москва, Россия (с 2002 г.)

Тузмухамедов Бахтияр Раисович, к.ю.н., проф., судья Международного уголовного трибунала по Руанде, советник, Управление международного права, Конституционный Суд РФ, Москва, Россия (с 2001 г.)

Убеев Алексей Вадимович, к.т.н., Москва, Россия (с 2009 г.)

Федоров Александр Валентинович, к. ф.-м. н., эксперт, Москва, Россия (с 2001 г.)

Федоров Валерий Валериевич, к.п.н., генеральный директор, Всероссийский центр изучения общественного мнения, Москва, Россия (с 2011 г.)

Феоктистов Дмитрий Валериевич, заместитель директора, Департамент по вопросам новых вызовов и угроз, Министерство иностранных дел России, Москва, Россия (с 2011 г.)

Фонд нераспространения во имя глобальной безопасности, Буэнос-Айрес, Аргентина (с 2010 г.)

Эггерт Константин фон, журналист, Москва, Россия (с 2002 г.)

Якушев Михаил Владимирович, вице-президент, Корпорация по установлению имен и номеров Интернета *ICANN* по России, Восточной Европе, СНГ, Москва, Россия (с 2014 г.)

Якушкин Дмитрий Дмитриевич, директор по связям с общественностью, Управляющая компания *Русссдрагмет*, Москва, Россия (с 2014 г.)

Ярных Андрей Юрьевич, руководитель стратегических проектов, Лаборатория Касперского, Москва, Россия (с 2015 г.)

РАБОЧАЯ ГРУППА ПО МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ГЛОБАЛЬНОМУ УПРАВЛЕНИЮ ИНТЕРНЕТОМ ПРИ ЭКСПЕРТНОМ СОВЕТЕ ПИР-ЦЕНТРА

(по состоянию на 20 ноября 2015 г.)

Волчинская Елена Константиновна, главный специалист по информационному праву, Фонд «Центр инноваций и информационных технологий», Федеральная нотариальная палата, Москва, Россия (с 2012 г.)

Демидов Олег Викторович, консультант, ПИР-Центр, Москва, Россия (с 2012 г.)

Зинина Ульяна Викторовна, советник по развитию законодательства и регулирования *Microsoft Russia*, Москва, Россия (с 2012 г.)

Зиновьева Елена Сергеевна, старший преподаватель, кафедра мировых политических процессов, МГИМО (У) МИД РФ, Москва, Россия (с 2012 г.)

Каберник Виталий Владимирович, начальник отдела, Управление инновационного развития, МГИМО (У) МИД РФ, Москва, Россия (с 2012 г.)

Касенова Мадина Балташевна, профессор, кафедра международного частного права, Дипломатическая академия МИД России, Москва, Россия (с 2013 г.)

Куликова Александра Владимировна, ответственный секретарь, координатор программы «Глобальное управление интернетом и международная информационная безопасность», ПИР-Центр, Москва, Россия (с 2014 г.)

Левова Ирина Юрьевна, руководитель отдела стратегических разработок, Российская ассоциация электронных коммуникаций (РАЭК), Москва, Россия (с 2012 г.)

Лукацкий Алексей Викторович, консультант по информационной безопасности, компания Cisco, Москва, Россия (с 2012 г.)

Пискунова Наталья Александровна, руководитель проекта, Международный форум по ядерному страхованию, Москва, Россия (с 2013 г.)

Романов Андрей Георгиевич, заместитель директора, Координационный центр национального домена сети Интернет, Москва, Россия (с 2013 г.)

Сачков Илья Константинович, генеральный директор, *Group-IB*, Москва, Россия (с 2012 г.)

Тодоров Леонид Львович, генеральный менеджер, Ассоциация администраторов национальных доменов Азиатско-Тихоокеанского региона, Москва, Россия (с 2012 г.)

Федоров Александр Валентинович, эксперт, Москва, Россия (с 2012 г.)

Черненко Елена Владимировна, заведующая отделом внешней политики, Издательский дом *Коммерсантъ,* Москва, Россия (с 2012 г.)

Якушев Михаил Владимирович, вице-президент, Корпорация по установлению имен и номеров Интернета *ICANN*, Москва, Россия (с 2012 г.)

МЕЖДУНАРОДНАЯ ЭКСПЕРТНАЯ ГРУППА

(по состоянию на 20 ноября 2015 г.)

Абишева Мариан Асафовна, руководитель Службы международных и национальных проектов Библиотеке Первого Президента РК — Лидера Нации, Астана, Республика Казахстан (с 2015 г.)

Аргуэльо Ирма, основатель и руководитель, Фонд нераспространения во имя глобальной безопасности, Буэнос-Айрес, Аргентина (с 2010 г.)

Бужинский Евгений Петрович, к.в.н., генерал-лейтенант, председатель Совета, ПИР-Центр, Москва, Россия (с 2010 г.)

Джаятиллека Дайан, посол, профессор, Университет Коломбо, Коломбо, Шри-Ланка (с 2008 г.)

Дуарте Сержио, посол, высокий представитель Генерального секретаря ООН по вопросам разоружения (2007–2012), Белу-Оризонте, Бразилия (с 2012 г.)

Дунай Пал, директор, Академия ОБСЕ в Бишкеке, Будапешт, Венгрия (с 2010 г.)

Злобин Николай Васильевич, президент, Центр глобальных интересов, Вашингтон, США (с 2014 г.)

Каравели Халил, руководитель проекта по Турции, Институт по изучению Центральной Азии и Кавказа при университете Джона Хопкинса, Анкара, Турция (с 2010 г.)

Кортунов Андрей Вадимович, к.и.н., генеральный директор, Российский совет по международным делам, Москва, Россия (с 2006 г.)

Макгетланенг Сехларе, д-р, директор, Программа государственного управления и демократии, Южноафриканский институт африканских исследований, Претория, ЮАР (с 2012 г.)

Сагер Абдулазиз, основатель и председатель, Исследовательский центр Залива, президент, Sager Group Holding, Джидда, Саудовская Аравия (с 2012 г.)

Санаи Мехди, доктор политологии, Чрезвчайный и Полномочный Посол, посольство Исламской Республики Иран в Российской Федерации (с 2011 г.)

Сатановский Евгений Янович, к.э.н., проф., президент, Институт Ближнего Востока, Москва, Россия (с 2006 г.)

Толипов Фарход Фазилович, к.п.н., директор негосударственного научно-образовательного учреждения *Билим карвони (Караван знаний)*, Ташкент, Узбекистан (с 2010 г.)

Тян Чун-Шэн, профессор, заместитель директора, Китайская ассоциация экономических исследований России и Центральной и Восточной Европы, Пекин, КНР (с 2011 г.)

Унникришнан Нандан, вице-президент, старший научный сотрудник Центра по международным вопросам, Фонд *Observer*, Дели, Индия (с 2010 г.)

Фетоури Мустафа, независимый исследователь, Триполи, Ливия (с 2013 г.)

Эггерт Константин фон, журналист, Москва, Россия (с 2006 г.)