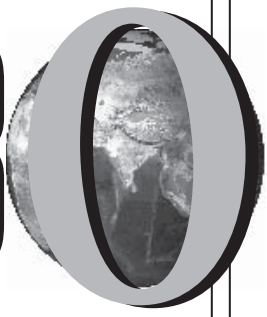
Научно-практический журнал

Non multa, sed multum

Выходит четыре раза в год

ИНДЕКС БЕЗОПАСНОСТИ



№ 3–4 (118–119), Том 22
Осень–зима 2016

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

№ 3–4 (118–119), Том 22

Осень–зима 2016

Дата выхода номера 30.12.2016

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»

Редакция
Зульхарнеев А.Ф.,
и.о. главного редактора
[zulkharneev@pircenter.org]
Сеславинская Ю.С.,
помощник главного редактора
[editor@pircenter.org]
Трухтанова Е.А., технический редактор
Макеева Е.И., корректор

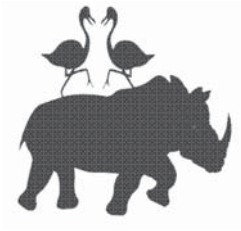
Адрес редакции и издателя
123242, г. Москва, ул. Дружинниковская, д. 30, стр. 1

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

Тираж 500 экз.

Свободная цена

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



ГЛОБАЛЬНАЯ БЕЗОПАСНОСТЬ В *ЭПОХУ СЕРФИНГИСТОВ*

Миру нужна система глобальной безопасности, соответствующая его реалиям. Развитие новых технологий открывает колоссальные возможности для решения мировых проблем, расширяя доступ к энергии, информации, знаниям. В то же время использование новых технологий в деструктивных целях ведет к обострению старых угроз и появлению новых.

Вопрос еще более усложняется особенностью нашего времени — мы пытаемся ответить на вполне конкретные и сугубо практические вопросы безопасности конкретного человека, предприятия, общества или всего мира, а сталкиваемся с фундаментальными вопросами природы человека и его сознания, государства, права, системы международных отношений.

Ныне часто цитируемая исследователь человеческого сознания Татьяна Черниговская отмечает, что с точки зрения способа обретения знания, на смену *поколению аквалангистов* приходит *поколение серфингистов*, то есть с развитием информационных технологий мы входим в эпоху другого знания — быстрого знания, не предполагающего глубокого погружения в тему, в эпоху быстрого восприятия информации, не всегда обстоятельного и системного, и быстрого принятия решений.

В вынесенном Советом Безопасности России в декабре 2016 г. на общественное обсуждение проекте Стратегии развития информационного общества на 2017–2030 гг. в качестве исходного положения заявляется: «Существующие в мире темпы развития технологий, создания, обработки и распространения информации значительно превысили возможности человека по разумному и осознанному освоению и применению знаний. Смещение фокуса восприятия окружающего мира, особенно в сети Интернет, с научной, образовательной и культурной информации на развлекательно-справочную сформировало новую модель восприятия, так называемое *клиповое мышление*, характерной особенностью которого является поверхностное, безоценочное восприятие информации без ее изучения»[1]. Авторы документа обозначают риск навязывания моделей поведения со стороны тех, кто владеет технологиями.

Нас не меньше волнует другой вопрос: можно ли доверить людям с *клиповым мышлением* ядерное оружие? Вместе с трансформацией моделей получения зна-

ния и обработки информации, очевидно, изменятся и системы государственного управления, общественных и международных отношений.

Ядерное оружие, атомная промышленность, а потом и вся система нераспространения возникли в индустриальную эпоху, в сильных централизованных государствах, имевших возможность полностью контролировать эти технологии.

Что будет представлять контроль над ядерными, химическими, биологическими и другими технологиями, например, в сфере робототехники, в эпоху новых коммуникационных возможностей?

Эти вопросы могли бы оставаться вне поля массового интереса, но президентом США, одной из двух крупнейших ядерных держав, стал медиамагнат, никогда ранее не занимавший никакой государственный или военный пост. И не какой-то фрик и радикал, а — да! — горячий сторонник ядерного разоружения, но ответственный и респектабельный эксперт, президент Фонда Плаушерз Джо Сиринционе начинает кампанию *Keep Trump's Finger Off The Button: Take Nuclear Missiles Off Hair-Trigger Alert*[2] — «Уберите палец Трампа с ядерной кнопки. Выведите ядерные ракеты из состояния полной боевой готовности». Приход к власти Трампа для Сиринционе и сотен других ученых и активистов — скорее, не причина, а повод заострить внимание на том, что контроль над оружием, применение которого будет иметь катастрофические последствия, находится в руках буквально нескольких человек. Среди них, кстати, и представитель поколения *миллениалов*, правда, северокорейских *миллениалов*, но предсказуемости от этого не больше.

Страшно. У страха глаза велики, а рекламные, маркетинговые и лоббистские возможности тех, кто этот страх нагнетает и делает на нем деньги, поставлены хорошо, будь то высокотехнологичные компании оборонки, фармацевтики, ИТ-индустрии, сторонники подхода *держать и не пущать* или их оппоненты из числа борцов с Левиафаном и *тотальной слежкой*.

Страх — плохой советчик, особенно в поиске новой модели экономического роста на пути к глобальному технологическому лидерству. Нужно разбираться.

Возникает, как минимум, две группы вопросов при оценке влияния новых технологий на глобальную безопасность:

- Как сделать так, чтобы снизить риски использования новых технологий, не затормозив их развития и не уменьшая степени их полезного использования?
- Надо ли, а если надо, то каким образом, адаптировать существующую систему международной безопасности, нераспространения и контроля над вооружениями к новым технологическим и социальным реалиям?

Поскольку на объективность человека, тем более представляющего интересы той или иной отрасли, полагаться не приходиться, для ответа на эти вопросы необходимо объединить усилия бизнеса, экспертного и политического сообществ. Однако даже если они соберутся вместе, взаимопонимание не гарантировано. Экспертов, одинаково хорошо владеющих знаниями о технологиях, политике, праве и готовых предлагать решения на их пересечении, — единицы. Для начала нужны хотя бы *переводчики* — с технического и экономического языка на политический и правовой. Не забыть при этом про перевод на язык этики.

Экспертов, готовых не только заглянуть в абстрактное будущее, но и предложить решение вполне конкретных задач, с этим будущим связанных, ПИР-Центр и старается собирать на конференциях, Школе или здесь, в новом тематическом номере *Индекса Безопасности*.

О каких технологиях идет речь? Базовые ядерные, ракетные, космические технологии не новые, но они постоянно совершенствуются. Оставаясь технологиями высокими, они перестают быть эксклюзивными, уходят из-под контроля ограниченного круга стран. Создание атомной энергетики в новых регионах позволяет решать энергетические и экологические проблемы. Станислав **Кувалдин** оценивает возможности атомной индустрии в противодействии потеплению климата и заключает, что «мировые сценарии декарбонизации, полностью игнорирующие атомную энергетику, в обозримом будущем представляются маловероятными».

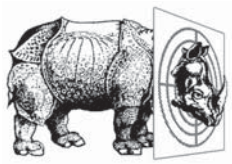
Уже наработанные механизмы регулирования мирного атома и космического пространства находятся под давлением новых технологических и политических реалий. Дискуссии о совершенствовании контроля над ядерными технологиями и материалами — системы гарантий МАГАТЭ — посвящена статья Валерия **Бычкова.**

О том, что можно сделать для снижения риска превращения космоса из пространства предоставления услуг для нашего комфорта в место, где все друг друга боятся, интервью заместителя генерального директора *Роскосмоса* Сергея **Савельева,** комментарии американского ученого и бывшего директора ЮНИДИР Терезы **Хитченс,** крупнейших российских экспертов Владимира **Ермакова** и Василия **Гуднова**.

По-настоящему новые или перспективные технологии *(emerging technologies)* уже появились, но еще не стали повсеместными. Определение этим технологиям и емкую картину их отношений с глобальной безопасностью дает директор *головного мирового think tank* — Института ООН по исследованию проблем разоружения (ЮНИДИР) Ярмо **Сарева.** В список таких технологий Сарева включает автономные оружейные системы, кибер-, био- и космические технологии, трехмерную (3D) печать и оружие направленной энергии. Ключевой вопрос — роль человека в применении этих технологий и определение того, что такое *значимый человеческий контроль*. Неминуемо встает вопрос о том, нужны ли человеку технологии, которые ставят под сомнение его роль хозяина жизни.

Ставки высоки. Природоподобные технологии меняют парадигму развития, выводят из тупика энергетического коллапса, но делают бесполезными все действующие механизмы безопасности, более того, они могут искусственно повлиять на ход эволюции человека как вида. Можно было бы посмотреть на эти рассуждения как на фантастику, если бы об этом не говорили руководители Курчатовского института Михаил **Ковальчук** и Олег **Нарайкин.**

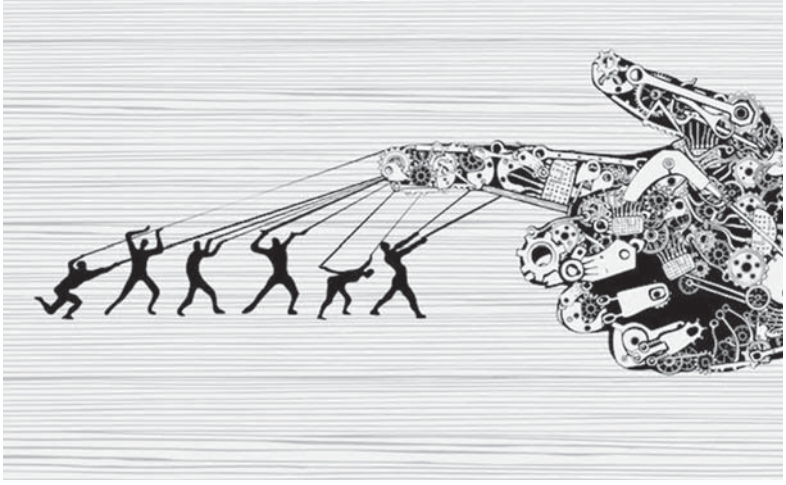
Робот или человек на поле боя. И если робот, распространяются ли на него человеческие законы, в том числе международное гуманитарное право? Впервые на российской площадке состоялось международное обсуждение политических и правовых аспектов развития смертоносных автономных систем. Вадим **Козюлин** собрал дипломатов, юристов, инженеров, правозащитников — читайте в рубрике «Круглый стол».



Три закона роботехники:

1. Робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинен вред.
2. Робот должен повиноваться всем приказам, которые дает человек, кроме тех случаев, когда эти приказы противоречат Первому Закону.
3. Робот должен заботиться о своей безопасности в той мере, в которой это не противоречит Первому или Второму Законам.

Хоровод. **А. Азимов**



...если хорошенько подумать, Три Закона роботехники совпадают с основными принципами большинства этических систем, существующих на Земле... попросту говоря, если Байерли исполняет все Законы роботехники, он — или робот, или очень хороший человек.

Мечты роботов. **А. Азимов**

На пересечении кибер- и ядерной безопасности неминуемо появилась тема кибербезопасности ядерных объектов, и это уже не теоретическая модель, а практическая необходимость. **Доклад ПИР-Центра** предлагает сбалансированную оценку угроз и намечает пути их преодоления.

Кибербезопасность критической инфраструктуры является одной из восьми тем книги-путеводителя «Глобальное управление Интернетом и безопасность в сфере использования ИКТ». Если вы не знаете с чего начать погружение в кибертематику, начните с этой книги, написанной Олегом **Демидовым** и изданной в серии «Библиотека ПИР-Центра». Рецензент Елена **Волчинская** отмечает удачный выбор структуры книги (проблемы–выводы–предложения) и с высоты своего опыта анализирует ее рекомендации. Елена **Черненко** летом 2013 г. немало времени провела в поисках Сноудена в Шереметьево, знает она и других персонажей бестселлера Андрея Солдатова и Ирины Бороган «Битва за Рунет: Как власть манипулирует информацией и следит за каждым из нас». Кому как не Елене было предложить прокомментировать эту книгу?

Глобальная безопасность имеет свою экономику. Создание МАГАТЭ во многом было обусловлено экономическими интересами, связанными с продвижением атомной энергетики на новые рынки. Инициативы, направленные на укрепление стратегической стабильности, глобальной и кибербезопасности, получат поддержку только в том случае, когда за ними будут стоять общественные силы и инициативные люди — именно те, кто заинтересованы в мире, где снижается значение границ, в мире, где меньше политических рисков.

Именно ученые-атомщики — те, кто создавали ядерные технологии, были в первых рядах тех, кто ратовали за их ограничение и прозрачность использования. Уже заявляют о своих позициях те, кто работают в сфере кибертехнологий, космоса, робототехники. Российский высокотехнологичный бизнес имеет свое видение мира.

Мы опасались, что технологии могут вытеснить мораль и право, боялись оказаться во власти тех, кто владеет технологиями. Но практика нашего общения показывает обратное — те, кто занимается высокотехнологичным бизнесом и наукой, могут быть гораздо менее циничными, более настроены на бесконфликтное решение выработку норм и правил поведения, чем политики. Поэтому на страницах этого номера вы найдете комментарии Натальи **Касперской** (Инфовотч), Андрея **Духвалова** (Лаборатория Касперского), Альберта **Ефимова** (Робототехнический центр Фонда Сколково).

А что же политики? Ключевая ось глобальной безопасности — российско-американские отношения. Готовы ли Россия и США вывести отношения из состояния, которое «хуже, чем в худшее время холодной войны»? Исходя из каких принципов Москва будет обсуждать вопросы безопасности с Вашингтоном — об этом большое интервью с заместителем министра иностранных дел России Сергеем **Рябковым**.

Все авторы этого номера согласны с тем, что регулирование — как национальное, так и международное — отстает от развития технологий. Традиционные механизмы поддержания безопасности теряют эффективность или перестают работать, а других механизмов пока нет. В этих условиях не рано ли сбрасывать с пути

прогресса этику, особенно понятную и универсальную этику мировых религий, которые в России еще называют *традиционными*? Не совершаем ли мы ошибку, когда дискредитируем основы этой этики или ставим церковь в оппозицию научно-техническому развитию? В обществе, в котором модернизационная повестка, в общем-то, не очень популярна, нужно ли *инновационному сообществу* искать врага там, где можно найти друга и союзника? Эта мысль появилась после разговора с руководителем Синодального отдела по взаимоотношениям Церкви с обществом и СМИ Московского Патриархата Владимиром **Легойдой** об отношениях науки, технологического развития и религии. Комментарий на тему в номере.

В 2017 г., кроме прочих дат, будет отмечаться юбилей второй Гаагской конференции 1907 г., где были сформулированы ключевые нормы международного гуманитарного права. Первая конференция состоялась в 1899 г., — обе были созваны по инициативе России. У нашей страны есть опыт выдвижения гуманитарных инициатив, конкурентные преимущества по развитию новых технологий, есть и великая гуманистическая и миротворческая традиция. Борьба за глобальное технологическое лидерство не может быть без лидерства в осмыслении новых вызовов глобальной безопасности. Только тогда у нас будет шанс жить в комфортном и безопасном мире по правилам, которые нас устраивают[3].

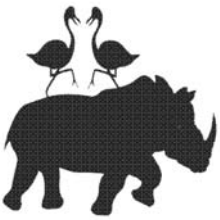
АЛЬБЕРТ ЗУЛЬХАРНЕЕВ,
директор ПИР-Центра

Примечания

1 Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. (проект). Сайт Совета безопасности РФ http://www.scrf.gov.ru/documents/6/136.html (последнее посещение — 20.01.2017).

2 Keep Trump's Finger Off The Button: Take Nuclear Missiles Off Hair-Trigger Alert https://www.change.org/p/president-obama-keep-trump-s-finger-off-the-button?recruiter=654845468&utm_source=share_petition&utm_medium=facebook&utm_campaign=share_facebook_responsive&utm_term=mob-xs-no_src-custom_msg (последнее посещение — 8.02.2017).

3 Существенная часть публикаций этого номера подготовлена по итогам международной конференции «Повестка XXI века — новые технологии и вызовы глобальной безопасности» и Международной школы по проблемам глобальной безопасности. Оба форума организованы в сентябре 2016 г. ПИР-Центром и Дипломатической академией МИД России в партнерстве с Фондом поддержки публичной дипломатии им. А. М. Горчакова, Фондом «Русский мир», Международным Комитетом Красного Креста, Корпорацией Карнеги в Нью-Йорке, Шведским управлением по радиационной безопасности, Федеральным департаментом обороны, гражданской защиты и спорта Швейцарии, Лабораторией Касперского и Робототехническим центром Сколково.



Отношения между Россией и США — ось глобальной безопасности. В Вашингтоне приступила к работе новая администрация во главе с Дональдом Трампом. Его заявления в ходе предвыборной кампании и в первые дни на президентском посту подают осторожные надежды на смену вектора двухсторонних отношений и возобновление полноценного диалога по глобальным и региональным проблемам. Москва воспринимает слова позитивно, но только в слова давно не верит.

Обречены ли Россия и США на противостояние? Результаты и уроки *перезагрузки*. С чего можно начать восстановление отношений, а что предлагать бессмысленно? Изменятся ли американские планы по ПРО и модернизации ядерной триады? Готова ли Москва скорректировать подходы к диалогу по стратегической стабильности? Каких практических шагов ждет Россия от новой американской администрации? Перспективы диалога по кибербезопасности, советы по *иранской ядерной сделке* и принципы выхода из ядерного тупика на Корейском полуострове.

Эти и другие вопросы осветил заместитель министра иностранных дел России Сергей Рябков на встрече с членами Международного клуба *Триалог* и в интервью директору ПИР-Центра Альберту Зульхарнееву.

Сергей Рябков:

«НИЧТО НЕ ПРЕДОПРЕДЕЛЕНО. ДАВАЙТЕ СУДИТЬ НЕ ПО СЛОВАМ, А ПО ДЕЙСТВИЯМ И КОНСТРУКТИВНО РАБОТАТЬ»

— Восемь лет назад, когда к власти пришла администрация Барака Обамы, ходила шутка о том, что Россия готова нанять телохранителя новому американскому президенту, лишь бы с ним ничего не случилось, — так высоки были ожидания от предстоящей работы с новой демократической администрацией. Причем ожидания были взаимные и в течение какого-то времени подтверждались на деле. Но, как мы видим, итоги восьмилетнего периода весьма неутешительны как для двусторонних отношений, так и для сотрудничества по проблемам глобальной безопасности. В чем причины такого развития событий?

— Подводя черту под восьмилетним периодом развития отношений при Обаме, нужно сказать, что, по сути дела, мы видели две разные администрации США под его руководством.

Первое четырехлетие прошло под лозунгом *перезагрузки*, при этом сам термин в ткань международного общения внедрили американцы. Автором, который отчеканил это слово-монету, на тот период был специальный помощник президента Обамы по российским делам, впоследствии посол США в Москве Майкл Макфол.

Это время ознаменовалось достижением некоторых важных договоренностей с Вашингтоном, которые и по сей день, мы в этом убеждены, оказывают положительное воздействие на международную безопасность и служат своего рода якорем в наших отношениях, не позволяющим этим отношениям совсем уплыть в неконтролируемое плавание по бурным водам. Среди этих договоренностей, конечно, на первом плане стоит Договор СНВ 2010 г., в соответствии с которым на основные уровни по боезарядам и носителям обе страны должны выйти к 5 февраля 2018 г., то есть фактически через год.

Однако во второй президентский срок Обамы американская сторона взяла курс на планомерное разрушение взаимодействия. На наш взгляд, это было связано с концептуальной проблемой. А именно с тем, что в вашингтонском политическом истеблишменте, несмотря на все данные нам ранее обещания и политические сигналы, так и не сумели признать Россию в качестве равного партнера, с мнением которого следует считаться. Более того, усмотрели серьезный вызов в укреплении российских позиций на международной арене, стали активнее использовать против нас различные инструменты давления.

Можно вспомнить, что еще задолго до украинского кризиса — я говорю об этом не случайно, потому что сейчас слово «санкции» в этом контексте настолько неразрывно связалось со словами *Минские соглашения*, что, по сути дела, наблюдается сознательное искажение того, что имело место не так давно — а происходило введение первого санкционного пакета в рамках так называемого *закона Магнитского* в 2012 г., то есть за два года до произошедшего на Украине и в Крыму.

Примерно в то же время администрация Обамы и ее правоохранительные органы развернули подлинную охоту на российских граждан по всему миру. Наиболее вопиющие, знаковые и резонансные случаи — это, конечно, ситуации с Виктором Бутом и Константином Ярошенко. Последний был просто похищен в стилистке «надеть черный мешок на голову» и затолкан в самолет агентами антинаркотической службы США, хотя он не имел и не мог иметь отношения ни к каким транспортировкам наркотиков через Либерию или где-либо еще.

Темп тотального сползания отношений к нынешнему состоянию — несомненно, худшему со времен холодной войны (здесь еще можно обсуждать, не хуже ли оно сейчас, чем в худшее время холодной войны) резко усилился после переворота в Киеве и последующих событий в Крыму, а затем и на Донбассе. Хотелось бы обратить внимание на то, что администрация Обамы, не дожидаясь того, что будет дальше, буквально в первые месяцы после крымских событий провозгласила курс на *системное сдерживание* России. И это включало не только ограничение двусторонних контактов, свертывание механизмов взаимодействия, но и резкое расширение санкционной политики, которая, по сути, превратилась в единственный

инструмент и единственное средство работы с Москвой на последующие два с половиной года.

В итоге, по состоянию на сегодня под американскими санкциями находятся 172 российских гражданина и 350 юридических лиц, включая разного рода компании, банки и организации. Я не буду утомлять вас статисткой по количеству недружественных и откровенно враждебных действий в различных сферах, не говоря уже о гигабайтах неприемлемой риторики, с которой приходилось и приходится знакомиться на протяжении всего этого времени.

— Президент Трамп приступает к работе. Ваши первые впечатления и прогнозы развития российско-американских отношений? Изменятся ли наши подходы к работе с американцами?

— Хотелось бы надеяться, что перемены в Белом доме позволят переломить опасную тенденцию деградации российско-американских связей. Мы, конечно, внимательно следили и следим за тем, что Трамп говорил и говорит о России, мы позитивно восприняли его слова о необходимости налаживания нормального диалога между нашими странами. Настроенность обеих сторон выправлять неудовлетворительную ситуацию в двусторонних делах была подтверждена в телефонных разговорах президентов Путина и Трампа.

Что касается нашего подхода, то Президент России не раз подчеркивал, что мы открыты для прагматичного взаимодействия с Вашингтоном по всем вопросам. Однако такое взаимодействие должно выстраиваться в русле баланса интересов, без попыток шантажа и навязывания своей воли. Но для далеко идущих выводов *исходных данных* пока недостаточно. Нужно отследить и проанализировать практические действия новой администрации. Первые шаги Трампа после вступления в должность являются весьма значимыми, далеко идущими, серьезными — они сейчас анализируются.

Чтобы окончательно определиться с внешнеполитическими приоритетами и подходами по конкретным вопросам, новому хозяину Белого дома, мы это понимаем, потребуется время, тем более что в Вашингтоне происходит очень глубокая, массированная, масштабная смена руководящего звена всех основных ведомств и других структур исполнительной власти.

При любом раскладе нам важно реалистично оценивать ситуацию в отношениях, не пытаться смотреть на будущий диалог «сквозь розовые очки». Уверяю вас, у нас нет подобного рода безосновательных иллюзий, что с приходом Трампа начинается «новая жизнь», или все перевернется, повернется на 180 градусов.

— Одно дело — риторика кандидата в президенты, другое — работа уже вступившего в должность президента, возможности которого велики, но все-таки ограничены и внутриполитической обстановкой, и отношениями с союзниками. Нет ли у Вас опасения, что, столкнувшись с такой реальностью, Трамп быстро изменит свой настрой в отношении России?

— Мы понимаем, что разгребать завалы, созданные в последние годы Белым домом, будет очень непросто. Никуда быстро не уйдет и прочно утвердившийся в вашингтонской элите межпартийный консенсус на антироссийской основе. Наверняка, мы увидим нескончаемые попытки «*образумить*» Дональда Трампа

и вернуть его в *мейнстрим* в том, что касается восприятия нашей страны и подхода к отношениям с Россией.

Эти попытки сейчас составляют основное содержание диалога многих европейских лидеров, лидеров Евросоюза и НАТО с новой администрацией США, когда обсуждают Россию и отношения с ней. Те европейские политики, которые сейчас с разной степенью увлеченности обсуждают перспективы *«российского вмешательства»* в предстоящие в некоторых европейских странах выборы, весь последний год сами занимались грубейшим вмешательством во внутренние дела США, продвигая Хиллари Клинтон на президентский пост. А когда ее победы не случилось, они решили настроить Трампа *по-клинтоновски* — по крайней мере, на российском направлении. Все это вызывает сожаление, но, по большому счету, ничего неожиданного в этом нет, и мы будем исходить из этой реальности в предстоящий период. Людей не переделаешь. Они свято верят в собственную непогрешимость.

Мы также обратили внимание на то, что в конгрессе США как раз в период пересменки в Белом доме активизировались силы, которые хотят *кодифицировать* все худшее, что было оставлено Обамой на российском направлении его внешней политики. Я, конечно, имею в виду законопроект, предусматривающий кодификацию санкций, введенных указами президента Обамы, и их существенное ужесточение. Дальнейший график прохождения этого законопроекта пока не ясен, тем более что в сенате есть одна его версия — известная версия Кардина, Менендеса, Маккейна, Рубио и других, а в палате представителей — несколько иная. И какова будет процедура — объединительная, либо пойдут по разным трекам — пока не совсем понятно, но факт есть факт. С учетом того уровня антироссийских настроений, о которых я уже говорил, мы исходим из того, что даже гипотетическое президентское вето на конечный *продукт* может быть преодолено.

— То есть надежд на возможность отмены санкций возлагать не стоит, и на повестке этот вопрос не стоит?

— Просить их отменить или даже обсуждать критерии их отмены мы не будем, как не делали этого и раньше.

— В одном популярном аккаунте в Твиттере промелькнула мысль о «снятии санкций в обмен на ядерные сокращения». Как Вам такая идея?

— Она совершенно неработоспособна. Во-первых, мы не обсуждаем санкции и не будем обсуждать. Это Вы можете воспринимать с улыбкой, можете серьезно, но это так и есть. А во-вторых, как можно «разменивать» отмену санкций на разоружение? Получается, что мы должны разоружаться в одностороннем порядке. Это вообще *non-starter*.

— Какими же могут быть первые шаги по восстановлению отношений?

— В практическом плане для начала нужно хотя бы восстановить механизмы коммуникации, которые в большинстве областей не работают после решения Вашингтона о заморозке деятельности президентской комиссии с марта 2014 г.

Понятно, что вряд ли речь пойдет о восстановлении всех рабочих групп (всего их было 21), но перезапуск контактов между министерствами и ведомствами в той или иной форме давно востребован.

— Какая повестка сегодня может быть в «общей корзине»?

— Конечно, хотелось бы надеяться, что получится сотрудничество в борьбе с международным терроризмом.

При Обаме Вашингтон нехотя, но все-таки стал воевать с ИГИЛ — после того как террористы совершили несколько ужасающих акций. Однако демократическая администрация до последнего дня прикрывала Джабхат ан-Нусру [организация запрещена в России. — *Ред.*] и явно рассчитывала использовать ее боевиков для смещения правительства в Дамаске. Но ведь «Нусра» — это сирийское отделение террористической группировки «Аль-Каида», которая устроила 11 сентября 2001 г. теракты в Нью-Йорке и в Вашингтоне, стоившие почти четырех тысяч жизней американцев. Получается, что администрация Барака Обамы поддерживала террористов, а это в самих США является уголовно наказуемым деянием.

Степень политического сюрреализма в последнее время и так превышает все, что раньше казалось невозможным, но это вообще выходящий из ряда вон «казус», который повторялся много лет.

Дональд Трамп, похоже, понимает ситуацию иначе, чем его предшественник. Во время предвыборной кампании Трамп говорил, что главная проблема в Сирии — международный терроризм, который свил там гнездо. Мы с этим согласны. Но что получится в реальности — пока большой вопрос.

В ходе телефонного разговора 28 января оба президента констатировали, что от наших стран немало зависит в плане поддержания глобальной безопасности, решения острых региональных проблем, противодействия опасным вызовам, особенно терроризму.

Москва готова к полноценной дискуссии по поддержанию глобальной безопасности, включая проблематику стратегической стабильности, и решению острых региональных проблем. Но эта дискуссия может стать продуктивной только в том случае, если США будут руководствоваться основополагающими принципами взаимного учета интересов и ненанесения ущерба безопасности другим.

При обоюдном конструктивном настрое могут открыться новые возможности для сотрудничества в инвестиционной и технологической сферах, а также в вопросах торговли. Товарооборот в прошлом году продолжал снижаться, но сейчас, по последней статистике, можно зафиксировать универсальный тренд — падение товарооборота приостановилось, начинается постепенный рост. Важно, что целый ряд значимых американских компаний не захотели уходить с российского рынка, несмотря на призывы и давление со стороны официального Вашингтона; они сохраняют настрой на взаимодействие с партнерами в нашей стране.

По-прежнему востребованы культурно-гуманитарные обмены и контакты между людьми. Кстати, на этот год выпадает ряд значимых дат, которые при наличии обоюдного интереса, можно было бы отметить проведением совместных мероприятий. Я имею в виду прежде всего 210-ю годовщину установления дипломатических отношений, 200-летие прибытия российской эскадры на Гавайи, 150-летие договора об Аляске, 80-летие легендарного чкаловского перелета.

Отношения с США сегодня оказались во многом на перепутье. Содержательное наполнение работы по конкретным направлениям будет вестись постепенно — по мере выстраивания диалога с новой республиканской администрацией

и в зависимости от ее готовности реализовать на практике некоторые предвыборные сигналы президента.

— Предлагаю подробнее остановиться на вопросах стратегической стабильности, нераспространения и контроля над вооружениями. Из опыта известно, что продвижение в российско-американском диалоге по этим вопросам намечается в том случае, когда отношения между странами на подъеме или когда они достигли опасной точки, как Карибский кризис. Сейчас есть шанс на улучшение отношений. Повлияет ли это на корректировку российских подходов?

— Хотел бы совершенно ответственно заявить, поскольку мне этим приходится заниматься постоянно и в полном объеме, что в связи со сменой администрации в Вашингтоне никакого изменения позиции РФ относительно того, что в ходе дальнейшего диалога по стратегической стабильности нужно учитывать все факторы, влияющие на нее, не произошло. А к этим факторам относятся и продолжение, которое, видимо, будет ускоряться, создания США глобальной ПРО, и развитие ими СНВ в неядерном оснащении в рамках концепции *молниеносного глобального удара*, проблемы с соблюдением США Договора о ракетах средней и меньшей дальности (РСМД), нарастающие угрозы попадания оружия в космос, сохранение и кое в чем усиление количественных и качественных дисбалансов в обычных вооружениях. Все эти элементы неотъемлемым образом должны учитываться в ходе диалога. Нам пока непонятно, как именно администрация Трампа будет выстраивать политику в данной сфере. Наверное, еще рано об этом говорить.

— Вы сказали о готовности к сотрудничеству с США по вопросам стратегической стабильности. Ожидаете ли Вы изменений в политике США по ПРО, в частности по европейскому сегменту этой системы? И вызывают ли озабоченность у Москвы анонсированные в ходе предвыборной кампании планы по серьезным финансовым вливаниям в модернизацию ядерной триады США?

— Я сказал, что мы готовы к продолжению диалога по стратегической стабильности при условии, что все эти вышеперечисленные факторы будут не просто приняты во внимание, но и учтены в любых возможных решениях по вопросам стратегической стабильности. Так что вопрос возможного сотрудничества лежит далеко за горизонтом, и такое сотрудничество даже трудно себе представить на нынешнем крайне проблемном отрезке в наших двусторонних отношениях.

В более широком смысле вопрос возможного пересмотра и модернизации, можно даже сказать, переконфигурирования, военной стратегии США в мире и особенно в Европе привлекает наше самое пристальное внимание. Необходимо аккумулировать больше информации и получить более точные оценки того, в каком направлении собираются двигаться США.

У нас пока складывается впечатление, что новая администрация не намерена что-либо кардинально менять в отношении планов развития противоракетной обороны. Возможно, будет сделан чуть больший акцент на территориальной обороне континентальной части США. Последствия этого еще предстоит понять и проанализировать. Но, в общем и целом, думаю, что республиканская администрация, следуя традиции предыдущих американских администраций, будет укреплять программу ПРО в плане ее потенциала, маневренности, скорости развертывания, морского компонента и всего остального. При этом возможно определен-

ное сотрудничество США по данному вопросу с другими странами, в том числе не являющимися членами НАТО.

Пока рано что-то определенно говорить о так называемом европейском сегменте. Как я уже отметил, в настоящее время эти вопросы с администрацией Трампа мы ни в каком формате не обсуждаем, и таких обсуждений не ведется уже давно — еще со времен предыдущей администрации.

США стоят на пороге начала значительных усилий по модернизации своей ядерной триады. Эти планы были заявлены ближе к концу второго срока Обамы. Не думаю, что есть какие-то основания ожидать, что при администрации Трампа эти планы подвергнутся серьезным изменениям. Скорее, наоборот: даже вызывавшие определенные противоречия элементы плана, объявленного при Обаме, будут финансироваться более эффективно, если можно так сказать.

Вам, конечно, известно, что новая администрация делает упор на эффективность бюджетного финансирования военных программ, но возможность урезать финансирование данного направления можно полностью исключить. Это лишь один пример. Спекулировать на данные темы и сложно, и безответственно с моей стороны, но это явно не та область, где Америка собирается концентрироваться на внутренних вопросах. Думаю, представление о том, что американскую безопасность можно гарантировать только в глобальном масштабе, в Америке разделяют все, и новый президент наверняка будет придерживаться аналогичного подхода.

Мне также кажется, что будет продолжение, а не отмена того, что страны НАТО согласовали на своих саммитах в Уэльсе и в Варшаве. Интересно будет посмотреть, какие решения примут на так называемом мини-саммите НАТО в этом году. Твердое решение о проведении такого саммита еще не принято, но, если он будет проведен, интересно будет понаблюдать, не добавит ли он тех или иных оттенков в общую картину или каких-то новых акцентов в определенных областях.

Это стало бы ранним сигналом о том, насколько администрация Трампа собирается придерживаться идеи, скажем так, изменения баланса в НАТО. Будут ли там с американской стороны повторяться многочисленные лозунги и заверения (на которые нам тоже следует обращать внимание) о «незаменимости» альянса, о том, что это «самый успешный альянс в истории человечества»? Именно такие заявления безостановочно тиражировали европейские лидеры в ходе их последних контактов с Трампом и его представителями. Раньше это называлось «стараются индоктринировать».

— В ходе предвыборной кампании Дональд Трамп критически высказывался о Совместном всеобъемлющем плане действий (СВПД) по иранской ядерной программе и заявлял, что по крайней мере попытается изменить условия соглашения. Также известно, что республиканцы, сохранившие большинство в Конгрессе, крайне недовольны заключением этого соглашения. Ожидаете ли Вы в этом контексте кризиса СВПД? И как следует на это реагировать России?

— Это одна из областей, где нынешняя администрация США собирается очень активно проводить новую политику. С ее стороны раздаются заявления и сигналы, которые не предвещают ничего хорошего для СВПД. Лично я не считаю, что у новой администрации есть намерение полностью выйти из соглашения и предложить взамен что-то совершенно новое, то есть предложить партнерам все

начать с чистого листа. Однако вполне возможны попытки «исправить» некоторые, с ее точки зрения, недостатки в СВПД, а также, коль уж зашла об этом речь, в Резолюции 2231 Совета Безопасности ООН. Мне кажется, упор может быть сделан на вопросах введения дополнительных, более интрузивных, мер контроля и мониторинга выполнения соглашения на разных иранских объектах.

Мой совет американским коллегам по иранской ядерной «сделке» очень простой: не пытайтесь чинить то, что не сломано. Если кто-то попытается «переписать» соглашение, он откроет ящик Пандоры. И дело даже не в том, что мы все вложили много политической воли, усилий и времени в достижение этого соглашения. У нас работа такая, так что мы не жалуемся. Но мне кажется, что просто было бы слишком рискованно пытаться запустить «новый процесс» по такому серьезному вопросу и добиваться новых условий соглашения. Вместе с тем нельзя исключить и того, что администрация попытается настоять на своих условиях, полностью отдавая себе отчет в том, какова будет реакция в Иране. Это был бы нежелательный и негативный вариант развития событий, который лишь подлил бы масла в огонь на Ближнем Востоке.

— Благодаря достигнутому соглашению, тема иранской ядерной программы вызывает меньшее беспокойство, чем ситуация на Корейском полуострове. Новый президент США заявил, что готов провести прямые переговоры с северокорейским лидером. КНДР провела очередное ядерное испытание в сентябре 2016 г., и это событие не вызвало большого общественного резонанса. Ситуация, похоже, зашла в тупик. Каково Ваше видение ситуации и перспектив решения проблемы? Применим ли к северокорейскому вопросу опыт работы по выработке СВПД?

— По-моему, ничего подобного Резолюции 2270 Совет Безопасности ООН раньше никогда не принимал. Это в очередной раз показывает прочность консенсуса в международном сообществе относительно того, что проведение ядерных испытаний Северной Кореей не приемлемо, что оно наносит ущерб международной безопасности и подрывает международный режим нераспространения ОМУ и усилия по укреплению этого режима.

С политической и дипломатической точек зрения можно сказать, что пример СВПД не применим к северокорейской ситуации. И на то есть несколько причин. Во-первых, стартовые условия для подготовки соглашения в случае с Ираном были совсем другими: степень прогресса в ядерной области, которая уже достигнута КНДР, не сравнима с иранской. Этот факт следует принимать во внимание всем, кто участвует в обсуждении.

Во-вторых, подписание СВПД стало возможно благодаря двум факторам: приходу к власти нового руководства исполнительной ветви и появлению новой команды переговорщиков в Исламской Республике, а также открывшемуся «окну возможностей» со стороны администрации Обамы, которая тогда еще не имела статуса *хромой утки*, но при этом сделать ставку на достижение подобного соглашения для нее уже было менее рискованно, чем раньше. В случае с КНДР подобных «стимулирующих» факторов попросту нет.

И в-третьих, говоря несколько упрощенно, нужно учитывать региональную обстановку. Мы полагаем, что северокорейское руководство стремится к подписанию мирного договора с США. Но, для того чтобы добиться прогресса на дипломатическом и политическом фронте, нужна ситуация относительного мира и спокой-

ствия на полуострове. Это, в свою очередь, требует крайней степени сдержанности со стороны тех игроков в регионе, которые после серии шагов со стороны КНДР резко нарастили свою военную активность в различных областях, в том числе в плане проведения учений на море, в воздухе и на суше, развертывания противоракетной системы THAAD и т. д. Мы это обсуждаем со всеми в регионе, в том числе с самой КНДР и, разумеется, с Китаем, а также с Японией, с представителями Южной Кореи.

Продолжение шестисторонних переговоров или работа в каком-то другом формате — вопрос на мой взгляд, вторичный. Надеемся, что вне зависимости от конфигурации будет соблюдено ключевое условие: отсутствие каких-либо провокаций и эскалации, что необходимо для поиска решения путем диалога и мирных средств. Не так давно российская сторона предложила определенные идеи насчет того, как со временем добиться принятия первичных мер по укреплению доверия и транспарентности, на которые в этом регионе, откровенно говоря, не особо высок спрос. Мы свои предложения внесли, работаем по ним, посмотрим, что будет дальше.

Опять же, как и по вопросу сирийского урегулирования, нужно будет понять, кто этим будет заниматься в практическом плане в Вашингтоне. Но мы готовы взять на себя свою часть этой ноши наряду со всеми остальными участниками, включая новую администрацию США и, конечно, наших китайских друзей и японских коллег.

— К вопросу обвинений в кибератаках на США со стороны якобы российских хакеров. Видятся ли Вам какие-то перспективы для сотрудничества с новой администрацией в сфере кибербезопасности? В первые годы администрации Обамы в этой области намечался определенный прогресс. Каким Вам видится дальнейшее развитие событий?

— Наше предложение заключается в том, чтобы по-деловому провести экспертные консультации на межведомственном уровне с участием всех заинтересованных сторон, постаравшись таким образом внести ясность в этот тревожный вопрос. Несомненно, здесь есть определенные аспекты, вызывающие обеспокоенность. Особенно это относится к киберпреступности, похищению данных, а также к нарушениям прав интеллектуальной собственности. Кроме того, аспекты, которые имеют серьезную политическую окраску, — их тоже можно обсудить, и мы не раз заявляли, что готовы к такому обсуждению. Но делать это нужно не путем бесконечных дебатов — это даже не дебаты, а мегафонная дипломатия в самом худшем смысле слова. Так что наше предложение остается в силе, и мы его не собираемся снимать.

У нас немало вопросов, которые мы хотели бы задать американской стороне. Вы наверняка знакомы с заявлениями наших высокопоставленных официальных лиц, в том числе Николая Патрушева, Дмитрия Пескова и других, об атаках извне на российские сайты и российские интернет-ресурсы. Мы пытаемся не допустить превращения этого сюжета в очередную политическую проблему. Мы деструктивную политику в отношении США не ведем, и наше предложение остается в силе, мы будем продолжать работать по этой теме.

— Мы обсудили конкретные вопросы, хотел бы задать более философский. Вы упомянули о наличии антироссийского консенсуса в Вашингтоне, но, надо признать, и у нас в России имеется аналогичный консенсус в отношении США. Многие политологи утверждают, что нормальные отношения между Россией и США — это отношения* легкого противостояния*, которое важно контролировать и не допускать его эскалации. Иначе говоря, когда

Россия слаба — отношения могут быть хорошими, а когда Россия находится в сильной позиции, такого рода соперничество неизбежно. Насколько обоснованной Вы считаете такую теорию? Предопределена ли логика российско-американских отношений долгосрочными историческими или геополитическими факторами?

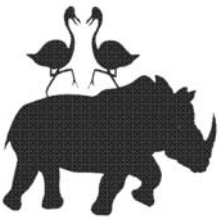
— Я искренне считаю, что здесь ничто не предопределено. Невозможно делать такие выводы из истории наших отношений или утверждать, что в нынешней ситуации есть сходство с ситуацией многолетней давности. В некоторых элементах можно, конечно, уловить такое сходство, и тем не менее. Например, в области контроля над вооружениями всегда считалось, что для России легче иметь дело с республиканскими администрациями, чем с администрациями демократов. Но при этом новый договор СНВ, подписанный в 2010 г., — стержневой на сегодняшний день двусторонний договор в области стратегических ядерных вооружений — был заключен с администрацией демократов, а не республиканцев. Или взять те результаты, которые администрация Обамы числила среди главных внешнеполитических достижений своего восьмилетнего пребывания у власти: СВПД, сирийское химическое разоружение — опять же, Россия сыграла очень весомую роль в достижении этих результатов, и они были достигнуты при администрации демократов, а не республиканцев.

Мне кажется, что с администрацией Трампа у нас есть возможность через какое-то время как минимум выйти на некое плато стабильности. Насколько высокий или низкий уровень будет у этого плато, посмотрим. Но после периода крайне серьезных пертурбаций и резкого ухудшения наших двусторонних отношений для начала нам нужен период осмысления возможностей, а затем размеренный и обдуманный конструктивный период, который тоже вполне может в определенный момент закончиться. Однако это не повод для пессимизма.

Я бы сказал, что мы открыты ко многому в той степени, в которой на это готова противоположная сторона, но только на принципах равноправия и взаимного уважения интересов друг друга. Это обязательный компонент. Некоторые комментаторы, особенно те, кто уже десятилетиями отслеживает российско-американские отношения, полагают, что взлеты и падения в наших отношениях вполне естественны, что время все лечит и что колебания градуса в российско-американских делах неизбежны. Им кажется, что отношения наших двух стран просто следуют законам природы, за которыми физики могут наблюдать на экранах своих осциллографов, где кривая движется по синусоиде. Думаю, что в таком суждении есть доля истины. Но правда и в том, что после каждого падения, после каждого нового спада выйти на новую восходящую траекторию в наших отношениях становится труднее и политически, и психологически.

Тем не менее мы полны решимости пройти свою часть этого пути и дойти до момента, когда можно будет сказать, что американский подход серьезно изменился по сравнению с 2015-м и 2016-м годами. Не знаю, когда это произойдет и произойдет ли это вообще. Однако борьба с терроризмом, ближневосточные вопросы, двустороннее взаимодействие в областях, представляющих взаимный интерес, и все остальное, что можно упомянуть в этом ряду, настраивают на рабочий лад. Есть несколько многообещающих сегментов, где по очевидным причинам мы и так уже упустили много времени.

Так что давайте не будем предаваться иллюзиям и разговорам, а займемся делом, вот в чем смысл моего комментария. Давайте подходить к этому вопросу размеренно и обдуманно, судить не по словам, а по действиям и конструктивно работать.



Связь, навигация, синхронизация по сигналам точного времени, дистанционное зондирование Земли и масса других космических услуг — то, без чего современное общество не сможет функционировать. Боевые действия в космосе или реализация других угроз мирной комической деятельности к концу света не приведут, но могут отбросить человечество далеко назад. Между тем есть планы освоения Луны и Марса — ведущие космические державы могут реализовать эти проекты самостоятельно, но стоит ли проводить границы там, где их нет.

Насколько обоснованы страхи потери мирного космоса, опасен ли уже сегодня космический мусор, что является оружием в космосе, перспективы соперничества и сотрудничества в космосе, подходы России к отношениям с другими комическими игроками — эти и другие вопросы обсудил директор программы ПИР-Центра «Россия и ядерное нераспространение» Андрей Баклицкий с заместителем генерального директора по международному сотрудничеству Государственной корпорации по космической деятельности *Роскосмос* Сергеем Савельевым.

Сергей Савельев:

«СТРАХОВЩИКИ РАБОТАЮТ С РЕАЛЬНЫМИ РИСКАМИ, А ДО ВОЕННЫХ ДЕЙСТВИЙ В КОСМОСЕ ПОКА НЕ ДОХОДИЛО...»

— Насколько Россия сегодня зависит от устойчивой работы спутников? Какая критическая инфраструктура окажется под ударом, в случае выхода из строя спутниковой группировки?

— На глобальном уровне сейчас любое государство, не только Россия, зависит от космических услуг. Они исключительно плотно переплетены с нашей повседневной жизнью. Давайте рассмотрим наиболее заметные примеры.

Связь — существенная часть потока данных в сети Интернет — идет через спутниковые порталы. Практически все удаленные и труднодоступные районы не имеют иной альтернативы в области связи, вне зависимости от того, о чем идет речь — о ретрансляции телесигнала или спутниковой телефонии.

Навигация — подавляющее большинство смартфонов сейчас имеет функцию навигации с использованием спутниковых систем. Наверное, все крупные транспортно-логистические компании пользуются плодами прикладной навигации, когда диспетчеры могут в режиме реального времени отслеживать перемещения машин и их использование. В настоящее время базовая комплектация многих автомобилей включает навигаторы, а с начала текущего года в России средства передвижения должны оснащаться *тревожными кнопками* ЭРА-ГЛОНАСС, которые позволяют экстренным службам сразу локализовать место ДТП.

Другое, менее известное использование спутниковых навигационных систем — это синхронизация банковских транзакций по сигналам точного времени, получаемым со спутников. Наконец дистанционное зондирование Земли также связано с работой спутников. Оно обеспечивает нас широким спектром прикладных применений: картографирование и районирование местностей, поиск полезных ископаемых и археологических объектов, мониторинг ледовой и экологической обстановки, природных бедствий и чрезвычайных ситуаций.

Если всего этого не станет, конечно, нам всем будет очень тяжело. По сути, по ряду направлений нам придется откатиться к технологиям 1960–1970-х годов. В том, что касается национальной безопасности, наиболее чувствительной для нас, скорее всего, окажется область управления и связи. Придется опираться на наземные линии связи и прямую трансляцию, возможно, даже возрождать телекс-связь.

В любом случае такой сценарий не представляется катастрофическим, а его последствия — непреодолимыми. Однако, безусловно, нашей задачей в плане международного сотрудничества — и мы над ней работаем — является недопущение реализации подобного сценария.

— Насколько критична на сегодняшний день ситуация с космическим мусором на низкой околоземной и геостационарной орбитах? Что планирует делать Роскосмос для уменьшения угроз, вызванных космическим мусором?

— Представляется, что угроза, связанная с космическим мусором, в ряде СМИ сильно преувеличена. В настоящее время вероятность столкновения двух космических объектов на орбите примерно равна возможности попасть под автомобиль на Красной площади. Вместе с тем угроза реально существует, поэтому мы держим ее под контролем. Создана и развивается система контроля околоземного пространства. Также реализуется проект создания АСПОС ОКП — автоматизированной системы предупреждения об опасных сближениях в околоземном космическом пространстве. В международном плане огромная работа ведется на площадке ООН и в рамках Межагентского координационного комитета по космическому мусору. Вырабатываются рекомендации и руководства к действию, направленные на снижение «мусорной» угрозы и снижение загрязнения околоземного пространства в результате космической деятельности. Внимание также уделяется повышению ситуационной информированности о критически важных частях околоземно-

го пространства, например, геостационарной орбиты или орбиты МКС. Ряд этих рекомендаций оформляется в международные отраслевые стандарты, в связи с чем налажено плотное взаимодействие с ISO — международной организацией по стандартизации.

Без ложной скромности можно утверждать, что Россия является одним из наиболее активных и ответственных участников этого процесса. Так, нами уже давно приняты меры технологического характера, призванные уменьшить количество космического мусора, который производится на этапе выведения на орбиту и отделения космических аппаратов. Разгонные блоки и отработавшие свое спутники в зависимости от остаточных объемов топлива, либо сводятся с орбиты и сгорают в атмосфере Земли, либо уводятся на орбиты — это могут быть орбиты с низким сроком орбитального существования или орбиты захоронения с последующей пассивизацией, то есть сбросом всех жидкостей и газов, которые могли бы способствовать разрушению космических объектов.

Вместе с тем еще многое остается сделать. Например, Россия выдвинула инициативу о создании международного информационного центра при ООН, что позволит свести воедино массивы информации об обстановке в околоземном пространстве, которые получает каждое государство. В результате мы существенно улучшим всеобщую ситуационную осведомленность, а также наши возможности по орбитальному планированию и снижению рисков опасного сближения космических объектов. К сожалению, некоторые наши партнеры пока сопротивляются этой инициативе, мотивируя свое нежелание присоединиться к ней соображениями национальной безопасности.

— Неоднократно озвучивались опасения, что средства по утилизации космического мусора могут использоваться как оружие против спутников других государств. Насколько подобные страхи обоснованы?

— Вполне обоснованы. Для того чтобы специализированный космический аппарат удалил космический мусор, он должен приблизиться к нему, определить, что объект действительно является мусором, а не действующим космическим аппаратом, захватить его тем или иным приспособлением и свести с орбиты (или увести на орбиту захоронения). В военной терминологии такой аппарат называется *спутником-инспектором*. Соответственно, любой *спутник-мусорщик* может быть потенциально использован в военных целях, то есть имеет двойное назначение.

Также в военном лексиконе существует термин *удаление некооперирующего/нефункционального объекта*. А это может быть как действительно мусор, так и космический аппарат некой недружественной державы. По большому счету в международном праве сейчас нет четко сформулированного механизма, который позволил бы иметь защиту от такой ситуации, когда вам скажут: «Мы считаем, что ваш спутник не работает по назначению, поэтому мы уничтожили его, как космический мусор». Да еще и предложат заплатить за оказанную «услугу».

— В начале декабря 2016 г. западные СМИ в очередной раз обвинили Россию в том, что под видом испытания системы ПРО Москва тестировала противоспутниковое оружие. Существует ли теоретическая возможность

провести разделение между противоспутниковыми системами и другими типами вооружений или пока это нереализуемая задача?

— Процитированные Вами заявления относятся, скорее, к политической сфере, поскольку при желании противоспутниковым оружием может быть объявлен любой спутник — ведь потенциально он может быть использован в качестве перехватчика. Про спутники-инспекторы я уже говорил. Противоспутниковым оружием также можно объявить любые детали, отделяющиеся от ракет-носителей при запуске, поскольку они также теоретически могут поразить чужой космический аппарат, тем более что четкие и признанные на международном уровне критерии определения преднамеренности или непреднамеренности выведения спутника из строя на настоящий момент фактически отсутствуют.

Что касается разделения систем вооружений на различные подкатегории — эта задача выглядит крайне сложной в связи с тем, что границы между вооружениями различного назначения подчас сильно размыты. Приведу пример. 21 февраля 2008 г. США осуществили перехват своего нерабочего спутника, применив стандартную морскую зенитную ракету *SM-3*, которая поставлена на вооружение в США и Японии, а в свое время предлагалась на экспорт в Турцию. Иными словами, мы имеем фактическое подтверждение, что, вероятно, любая зенитная ракета дальнего действия теоретически может быть использована в качестве противоспутникового оружия.

— В случае превращения околоземного пространства в поле боя спутниковые системы неизбежно понесут серьезные потери. Учитывается ли такая возможность при оценке рисков той или иной программы? Включается ли риск преднамеренного уничтожения космических аппаратов в их страховку?

— Наверное, этот вопрос следовало бы задать представителям военного ведомства. В любом случае представляется, что все космические державы исходят из вполне вероятной потери значительной части своих спутников в силу тех или иных обстоятельств. Для компенсации этих потерь они располагают резервами производственных мощностей, а также заделами по конкретной номенклатуре спутников высокой степени готовности. Страхование — это другое дело, страховщики работают преимущественно с реальными и подтверждаемыми рисками, а у нас, к счастью, до военных действий в космосе пока не доходило.

— Каковы, на Ваш взгляд, главные расхождения между Россией и западными странами в подходах к обеспечению безопасности космического пространства?

— В настоящее время, как нам представляется, наши западные партнеры делают ставку на запретительный подход — назначить кого-нибудь главным надсмотрщиком (или он сам себя назначит), навесить повсюду запретов, хватать и не пущать. В этом отношении наша позиция более гибкая — она основывается на принципе равноправного доступа в космос. Нельзя загонять себя и других в ситуацию, откуда есть только два выхода: отказаться от национального суверенитета или пойти на открытый конфликт с международным сообществом. Пространство для диалога должно оставаться всегда. Мы также считаем неконструктивными попытки ввести выборочные запреты, а также формирование и противопоставление элитных клубов и всех остальных. Согласитесь, требования наказывать за разработки

космических вооружений со стороны государства, которое уже само имеет такие боевые системы, выглядят по меньшей мере ханжеством.

— В некоторых экспертных сообществах приходилось слышать, что отрасль могла бы лучше справиться с выработкой международных норм и правил, чем военные и дипломаты. Если бы удалось собрать за столом переговоров представителей Роскосмоса, НАСА и Европейского космического агентства (ЕКА), получилось бы договориться, например, о неразмещении оружия в космосе?

— Мы бы с удовольствием сели за стол переговоров с нашими партнерами из НАСА, ЕКА и других агентств. Но, к сожалению, такие вопросы нельзя решать в отрыве от политических интересов руководства космических держав, а также от геополитической обстановки.

— Планы России по освоению Луны и Марса — это, скорее, нацеленность на соперничество или на сотрудничество с другими космическими державами?

— Однозначно понимаем такие проекты в качестве основы для сотрудничества. Конечно, Россия, США, Китай и, возможно, Япония теоретически обладают возможностями реализовать лунный или марсианский проект в одиночку. Однако риски, связанные с его выполнением — финансовые, организационные, технологические, будут слишком велики. На данном этапе межпланетный полет — проект настолько комплексный, сложный и ресурсоемкий, что гораздо рациональнее реализовывать его в широкой международной кооперации, объединяя воедино опыт и ноу-хау разных стран, а также распределяя сопутствующие риски более равномерно.

Валерий Бычков

КАК ОСУЩЕСТВЛЯТЬ КОНТРОЛЬ ЗА НЕРАСПРОСТРАНЕНИЕМ ЯДЕРНОГО ОРУЖИЯ? В ПОИСКАХ ПУТЕЙ РАЗВИТИЯ СИСТЕМЫ ГАРАНТИЙ МАГАТЭ

Современную систему гарантий МАГАТЭ можно охарактеризовать как международную систему контроля выполнения государствами своих обязательств по мирному использованию ядерной энергии. С момента ее установления в 1961 г. система находится в развитии, отвечая на вызовы времени и ожидания государств. В настоящее время система гарантий МАГАТЭ является важным элементом ДНЯО. Государства — участники ДНЯО, не обладающие ядерным оружием, обязаны заключить соглашение о всеобъемлющих гарантиях с МАГАТЭ, то есть поставить под гарантии МАГАТЭ весь ядерный материал во всей своей мирной ядерной деятельности. Высокая действенность (англ. effectiveness) контроля, или, что то же самое, высокий доверительный уровень (англ. credibility) заключений агентства по результатам его контрольной деятельности, является ключевым фактором современного режима нераспространения. Повышение действенности и эффективности (англ. efficiency) контроля было и остается движущим мотивом совершенствования и развития системы гарантий.

В 1990-х гг. были разработаны меры по укреплению системы гарантий, включающие Дополнительный протокол к соглашению по гарантиям. Усилия по внедрению этих мер были начаты в конце 1990-х — начале 2000-х гг. и продолжаются по настоящее время. В данной статье обсуждается современное состояние системы гарантий МАГАТЭ, рассматривается концепция осуществления гарантий на уровне государства и освещается дискуссия 2012–2014 гг. вокруг этой концепции, а также анализируются перспективы дальнейшего развития системы гарантий.

Современные проблемы развития гарантий во многом являются проблемами концептуального характера. Имеются трудности, связанные с интерпретацией положений тех или иных документов по гарантиям. Это ярко проявилось в дискуссии на Генеральной конференции и Совете управляющих МАГАТЭ в 2012–2014 гг. вокруг концепции осуществления гарантий на уровне государства. Преодолеть эти трудности помогает рассмотрение системы гарантий в ее развитии.[1] В данной работе дана более широкая трактовка концепции гарантий на уровне государства, чем та, что вытекает из современного определения концепции секретариатом МАГАТЭ.

Еще одна сложность в исследовании системы заключается в том, что часть документации по гарантиям имеет ограниченное распространение и не доступна

широкой общественности. Поэтому в некоторых случаях мы обращаемся к тем публикациям сотрудников МАГАТЭ, размещенным в открытой печати, где разъясняются те или иные внутренние документы агентства.

НА УРОВНЕ УСТАНОВКИ — СИСТЕМА ГАРАНТИЙ В 1981–1991 гг.

Для понимания концепции гарантий на уровне государства (англ. State level concept) нам необходимо проанализировать систему гарантий 1981–1991 гг. Гарантии МАГАТЭ того периода иногда называют традиционными или классическими гарантиями, но с точки зрения осуществляемой концепции их следует называть гарантиями на уровне ядерной установки. В указанный период инспекционная деятельность в рамках всех трех существующих типов соглашений[2] проводилась на основе процедур, описанных в документе «Структура и содержание соглашений между Агентством и государствами, требуемые в связи с Договором о нераспространении ядерного оружия» (INFCIRC/153). Хотя в целом это документ высокого качества, некоторые его параграфы сформулированы недостаточно четко, что приводит к трудностям в его интерпретации.

Первая часть документа содержит основные положения соглашения, а вторая часть — процедуры, которые должны применяться для осуществления этих положений. Во втором параграфе первой части документа сформулирована обязанность Агентства «… обеспечить применение… гарантий ко всему исходному или специальному расщепляющемуся материалу [то есть ко всему ядерному материалу. — пояснение *В. Б.*]) во всей мирной ядерной деятельности… государства… исключительно с целью проверки того, чтобы такой материал не переключался на ядерное оружие…»[3].

Во второй части документа, раздел «Цель гарантий» содержит три параграфа: 28, 29 и 30. Параграф 28 определяет, что «…цель гарантий состоит в своевременном обнаружении переключения значимых количеств ядерного материала с мирной ядерной деятельности на производство ядерного оружия…». В тексте типового соглашения[4] аналог параграфа 28 имеет следующую формулировку: «…цель процедур гарантий, изложенных в настоящем соглашении, состоит в своевременном обнаружении переключения…». Далее нам нужно уточнить о переключении чего и откуда идет речь в параграфе 28. Параграфы, определяющие процедуры учета ядерного материала (то есть параграфы 31, 32, 35, 41, 59 и 62) оперируют термином «ядерный материал, подлежащий гарантиям». Это неточный термин, который следовало бы уточнить как «ядерный материал, подлежащий процедурам учета и инспектирования». Согласно параграфу 7, государство должно вести учет и контроль такого материала в рамках национальных систем учета и контроля и декларировать МАГАТЭ инвентарные количества и потоки такого материала с помощью процедур, определенных в соглашении.

Параграф 34 в разделе «Начало применения гарантий» определяет стадию ядерного топливного цикла, начиная с которой ядерный материал подлежит процедурам учета. Это та стадия, на которой состав и чистота материала делают его пригодным для изготовления топлива или для изотопного обогащения. Примерами такого материала являются двуокись урана и гексафторид урана. Примером материала, не достигшего описанной выше стадии топливного цикла, является концентрат урана (например, желтый кек). Концентрат урана не подлежит процедурам

учета и инспектирования, изложенным в соглашении, государство обязано лишь уведомлять агентство об экспорте и импорте такого материала. Таким образом, во второй части соглашения речь идет об обнаружении переключения материала, подлежащего учету и заявленного государством в соответствии с установленными процедурами. Процедуры учета основаны на концепции зон баланса материала на каждой заявленной установке. Техническое заключение агентства по результатам проверки делается согласно параграфу 30, для каждой установки[5] в отношении количества неучтенного материала за период материального баланса (в среднем за один год).

С учетом вышеприведенного анализа уточненная формулировка цели процедур проверки выглядит следующим образом: «...своевременное обнаружение переключения значимых количеств заявленного ядерного материала на установках, поставленных под гарантии». Таким образом, цель процедур проверки ядерного материала формулируется на уровне установки, поставленной под гарантии.

Сопоставление цели и процедур проверки, изложенных во второй части соглашения, с положениями второй статьи соглашения показывает, что задача проверки полноты декларации государства не адресована в явном виде. Лишь некоторые процедуры, такие как специальная инспекция и проверка информации о конструкции установки, могут быть использованы для подтверждения отсутствия незаявленных ядерного материала и деятельности.

Важную роль в концепции гарантий на уровне установки играют критерии гарантий, которые представляют стандартные инспекционные процедуры, разработанные секретариатом агентства для каждого типа установок, поставленных под гарантии, то есть для исследовательских и энергетических реакторов, для заводов по изготовлению топлива и др. Стандартные процедуры отвечают «своевременному обнаружению переключения значимых количеств заявленного ядерного материала на установке, поставленной под гарантии». Эта цель была принята для всех типов соглашений по гарантиям; небольшие отличия в стандартных процедурах инспекций были сделаны лишь для установок, поставленных под гарантии в рамках соглашений по типу INFCIRC/66. Критерии служат как для планирования инспекционной деятельности, так и для оценки достижения инспекционных целей для ежегодного Доклада об осуществлении гарантий (ДОГ)[6]. Кроме того, критерии обеспечивают прозрачность инспекционных целей и процедур, создавая платформу для обсуждения результатов по каждой установке между секретариатом агентства с одной стороны и оператором установки и госорганом, отвечающим за гарантии, с другой стороны.

Хотя в целом критерии основаны на концепции осуществления гарантий на уровне установки, они содержат некоторые черты будущей концепции гарантий на уровне государства. Это процедуры проверки потоков ядерного материала между установками и процедуры проверки отсутствия заимствования материала между установками с целью сокрытия его несанкционированного изъятия.

Типовое заключение по гарантиям, публиковавшееся в ДОГ в 1981–1991 гг., выглядело следующим образом: «Секретариат... не обнаружил признаков переключения ядерного материала, поставленного под гарантии, или несанкционированного использования установок, оборудования или неядерного материала, поставленных под гарантии. На этом основании секретариат заключает, что ядерный мате-

риал и другие предметы, поставленные под гарантии, оставались в мирной ядерной деятельности…».

В заключение этого раздела несколько подробнее остановимся на анализе формулы «своевременное обнаружение переключения значимых количеств заявленного ядерного материала на установке, поставленной под гарантии».

Начнем с анализа термина «переключение». Во втором параграфе документа INFCIRC/153 говорится о переключении ядерного материала на «ядерное оружие или другие ядерные взрывные устройства». В параграфе 28 этот перечень дополнен словами «или на неизвестные цели». Дело в том, что, используя процедуры контроля, изложенные в соглашении, секретариат сумеет лишь обнаружить недостачу заявленного ядерного материала, но не сможет определить, на какие цели он был переключен. Поэтому в концепции осуществления гарантий на уровне установки, термин «переключение» понимается как недостача или физическое исчезновение определенного количества заявленного материала.

Далее, с учетом того, что производство ядерного взрывного устройства требует порогового количества ядерного материала, вводится понятие значимого количества. Инспекционные планы проверки наличия заявленного материала составляются исходя из требуемой вероятности обнаружения недостачи как минимум одного значимого количества материала. При этом предполагается, что в стране могут существовать незаявленные установки, необходимые для перевода переключаемого материала в то изотопное, химическое и физическое состояние, которое необходимо для производства ядерного оружия. Эта гипотеза служит для определения своевременности обнаружения. Например, инспектор должен обнаружить признаки переключения облученного ядерного топлива на реакторной установке не позже чем в трехмесячный срок со дня события. Этот критерий своевременности обнаружения базируется на постулате о том, что для извлечения одного значимого количества плутония на штатной радиохимической установке требуется три месяца.

Признаком переключения, о котором говорится в заключении по гарантиям, является аномалия в учетных данных, декларированных государством, которая включает одно или больше значимых количеств ядерного материала. Признаком переключения может являться также аномальная ситуация, возникшая при выполнении процедур гарантий, например, непредоставление доступа инспектору для физической проверки материала. Последнее приведет к заявлению секретариата о невозможности сделать заключение о непереключении ядерного материала.

КОНЦЕПЦИЯ ОСУЩЕСТВЛЕНИЯ ГАРАНТИЙ НА УРОВНЕ ГОСУДАРСТВА

В 1993 г., после обнаружения секретной ядерной деятельности в Ираке, направленной на получение ядерного оружия, агентство инициировало программу укрепления гарантий под названием «Программа 93+2». Ее основной задачей была разработка мер по обеспечению полноты декларации государства в рамках соглашения о всеобъемлющих гарантиях (СВГ). Новые меры должны были агентству дать возможность обнаруживать незаявленные ядерный материал и деятельность. Основой для них послужил опыт, приобретенный агентством в Ираке.

Программа была реализована в два этапа. На первом этапе были разработаны меры, которые могли применяться в рамках существующих соглашений. На втором этапе были разработаны меры, для осуществления которых агентству требовался дополнительный юридический инструмент: для этого был предложен Дополнительный протокол (ДП) к соглашению о гарантиях. Типовой ДП был одобрен Советом управляющих в 1997 г. Подробное описание новых мер гарантий и начального этапа их осуществления дано в фундаментальном обзоре[7], опубликованном агентством в 1999 г. Трудность этого этапа заключалась в том, что цель процедур, изложенных в ДП, формулируется на глобальном уровне, «с тем, чтобы повысить действенность и эффективность системы гарантий в качестве содействия целям глобального ядерного нераспространения». Соответственно, ДП не имеет конкретной привязки к положениям того или иного типа соглашений. Поэтому возникает необходимость разрабатывать концепцию или подход к осуществлению ДП в рамках конкретного типа соглашения[8].

Первым шагом к разработке такого подхода в рамках соглашения о всеобъемлющих гарантиях стал документ «Концептуальные основы интегрированных гарантий»[9], подготовленный секретариатом в 2002 г. Идея интегрированных гарантий (ИГ) заключается в том, что, применив меры ДП в государстве с СВГ и сделав заключение об отсутствии незаявленных ядерного материала и ядерной деятельности, агентство может сократить инспекционные усилия по проверке заявленного материала.

Концепция ИГ имеет в своей основе упрощенную интерпретацию положений второй статьи соглашения: «проверка достоверности и полноты деклараций государства». На базе этой формулы постулируются две независимые цели проверки: «обнаружение переключения заявленного ядерного материала» (для проверки достоверности деклараций) и «обнаружение незаявленных ядерного материала и деятельности» (для проверки полноты деклараций). Для достижения первой цели используются инспекционные процедуры, изложенные в критериях. Для достижения второй цели используются процедуры Дополнительного протокола.

Выполнив все необходимые процедуры проверки, секретариат делает заключение об отсутствии переключения заявленного ядерного материала и об отсутствии в стране незаявленных ядерного материала и ядерной деятельности. На основе этих двух заключений секретариат делает общее, так называемое расширенное заключение о том, что за отчетный период весь ядерный материал в стране оставался в мирной ядерной деятельности.

Предполагается, что, сделав раз расширенное заключение для конкретной страны, секретариат в дальнейшем будет ежегодно подтверждать это заключение. Для этого разрабатывается подход по осуществлению ИГ на уровне государства (англ. State-level approach). По определению секретариата, такой подход представляет оптимальную комбинацию всех мер гарантий в рамках СВГ и ДП с целью достижения максимальной эффективности и действенности осуществления гарантий. Для ежегодного осуществления подхода по ИГ в конкретном государстве секретариат для него разрабатывает годовой план осуществления подхода (англ. Annual implementation plan).

Таким образом, концепция ИГ включает уже новые по отношению к традиционным гарантиям элементы. В частности к ним относятся подход по разработке целей

и процедур контроля для государства в целом, разработка взамен критериев годового плана осуществления подхода по гарантиям и, что самое важное, заключение по результатам осуществления гарантий для государства в целом. Эти элементы являются признаками общей концепции гарантий на уровне государства (англ. State-level concept); термин был впервые употреблен секретариатом в ДОГ за 2004 г.

Прежде чем перейти к обсуждению общей концепции гарантий на уровне государства, остановимся на недостатках концепции ИГ.

Во-первых, данная концепция относится только к странам с СВГ, заключившим ДП, и только к тем из них, для которых было сделано расширенное заключение. Она не включает в рассмотрение страны с СВГ, которые не заключили ДП, и страны с другими типами соглашений по гарантиям.

Во-вторых, есть определенные трудности с промежуточными заключениями по результатам осуществления гарантий. Так, заключение об отсутствии в стране незаявленных ядерного материала и ядерной деятельности имеет непреложный, или детерминистический характер, в то время как вся контрольная деятельность в рамках системы гарантий основана на вероятностном подходе. Сделать заключение об отсутствии незаявленного материала в стране весьма непросто, но еще сложнее определить уровень достоверности такого заключения.

В-третьих, несмотря на свое название — ИГ — упомянутые выше цели процедур не связаны между собой, поэтому процедуры ДП на уровне государства не связаны или не интегрированы с процедурами проверки ядерного материала на уровне установки. Поэтому оптимизация деятельности по проверке адресована на формальной основе, за счет стандартных правил по уменьшению инспекционных усилий на заявленных установках. Например, вышеупомянутый критерий своевременности обнаружения для облученного топлива был увеличен с 3 до 12 месяцев, что значительно уменьшило количество инспекций на реакторных установках.

Фактически концепция ИГ отражает ранние представления о том, что в результате укрепления гарантий в рамках «Программы 93+2» система гарантий будет состоять из двух частей. Одна часть — это так называемые традиционные гарантии, с критериями, усовершенствованными на основе результатов первого этапа этой программы, а вторая часть — это ИГ, где традиционные гарантии интегрированы с ДП. Это представление, очевидно, повлияло на позицию отдельных государств во время дискуссии 2012–1024 гг., в отношении того, относится требование проверки полноты деклараций ко всем государствам с СВГ или только к тем из них, которые заключили ДП.

Недостатки ИГ были преодолены в более общей концепции осуществления гарантий на уровне государства (КУГ). Основные черты этой концепции были сформулированы при подготовке Докладов об осуществлении гарантий за 2004 и 205 гг. Рубежом перехода от концепции на уровне установки к КУГ стал ДОГ за 2003 г., в котором заключение по результатам осуществления гарантий впервые было разбито по типам соглашений и сделано на уровне государств, а не на уровне установок, как прежде. Новая структура заключения потребовала переосмысления целей и формулировок заключений по гарантиям в зависимости от типа соглашений и наличия ДП.

Новая концепция была сначала сформулирована для СВГ. В частности в ДОГ за 2005 г. было сделано важное пояснение: хотя полномочия агентства по проверке достоверности и полноты декларации государства вытекают из самого соглашения о всеобъемлющих гарантиях, инструменты соглашения, предоставляемые для решения этой задачи, ограничены. Поэтому заключение ДП с государством дает возможность агентству наиболее полно выполнить свои права и обязанности, прописанные во второй статье соглашения.

Для СВГ цели контрольной деятельности МАГАТЭ были сформулированы в соответствии со второй статьей соглашения. В отличие от концепции на уровне установки в КУГ термин «переключение ядерного материала» трактуется именно как переключение на ядерное взрывное устройство. При этом учитывается, что путь переключения (англ. acquisition path) может включать несанкционированное изъятие заявленного ядерного материала, несанкционированное использование заявленных установок, а также использование незаявленных ядерного материала и деятельности. Например, путь переключения плутония, который содержится в отработавших сборках ядерного реактора, может включать несанкционированное изъятие заявленных сборок на реакторной установке, несанкционированное извлечение плутония из этих сборок на заявленной радиохимической установке и конверсия плутония в металлическую форму на незаявленной установке.

Таким образом, цели контрольной деятельности на уровне государства в рамках СВГ:

a) обнаружить несанкционированное изъятие (переключение) заявленного ядерного материала;

b) обнаружить несанкционированное использование заявленных установок;

c) обнаружить незаявленные ядерный материал и деятельность.

Эти цели, равно как и относящиеся к ним процедуры проверки, взаимосвязаны через рассматриваемый путь возможного переключения. Они вытекают из второй статьи соглашения и не зависят от наличия или отсутствия ДП. Для достижения целей (a) и (b) совсем не обязательна ежегодная инспекция всех установок в государстве, как это требуется в концепции гарантий на уровне установки. Частота и интенсивность инспекций на установках определяются в результате анализа способов возможного получения материала, пригодного для ядерного оружия, исходя из конкретного ядерного топливного цикла государства. Частота и интенсивность инспекций зависят также от действенности процедур для достижения цели (c), то есть от того, заключило ли государство ДП с МАГАТЭ.

Для государства, заключившего СВГ и ДП с агентством, расширенное заключение по гарантиям выглядит следующим образом: «Секретариат не обнаружил признаков переключения заявленного ядерного материала из мирной ядерной деятельности и признаков присутствия незаявленных ядерного материала или деятельности. На этом основании секретариат заключает, что ядерный материал в государстве оставался в мирной деятельности».

Проведем сравнительный анализ осуществления гарантий в рамках концепции на уровне установки (КУУ) и концепции на уровне государства (КУГ). Анализ проведем для СВГ, рассматривая ситуации с ДП и без него.

1. Концепция на уровне установки.

a. Действенность и эффективность гарантий.

Применяются стандартные процедуры инспекций для обнаружения переключения ядерного материала на установке; процедуры основаны на мерах учета и контроля материала, подкрепленных мерами сохранения и наблюдения. Частота и интенсивность инспекций, а также сами процедуры проверки, определены в критериях для каждой установки ядерного топливного цикла. Действенность проверки адекватна задаче обнаружения переключения заявленного материала на установке. Задача проверки полноты декларации в этой концепции не поставлена, соответственно действенность контроля недостаточна для полного выполнения положений второй статьи соглашения. Оптимизация инспекционных усилий осуществляется за счет их концентрации на тех установках ядерного топливного цикла, которые содержат ядерный материал, пригодный для производства ядерного оружия.

b. Осуществление гарантий в государствах, заключивших Протокол о малых количествах (ПМК)[10].

В рамках КУУ в государствах с ПМК отсутствует сам объект гарантий, поскольку отсутствуют заявленные установки и зоны баланса материала[11]. Поэтому Доклады об осуществлении гарантий в 1981–1991 гг. не содержат информации о государствах с ПМК. Рассматривается только осуществление гарантий в странах, поставивших под гарантии ядерный материал на установках, а также в местах нахождения вне установок (порядка 70 стран).

c. Прозрачность планирования и осуществление деятельности по проверке; прозрачность выводов и заключений.

Критерии гарантий обеспечивают прозрачность планирования и осуществления контрольной деятельности для инспектора, оператора установки и представителя государственного органа, отвечающего за гарантии. Результаты оценки достижения инспекционных целей для каждой установки, поставленной под гарантии, дают основу для управления качеством осуществления процедур гарантий как агентством, так и государством. Заключение об отсутствии переключения делается в том случае, если в результате контрольной деятельности не были обнаружены признаки переключения, то есть серьезные аномалии в учете ядерного материала или в осуществлении других процедур гарантий. Ключевым моментом является анализ обнаруженных аномалий.

2. Концепция на уровне государства.

a. Действенность и эффективность гарантий.

Концепция включает цель проверки полноты декларации государства. Даже в случае отсутствия ДП действенность и эффективность гарантий выше, чем в концепции на уровне установки, за счет рассмотрения ядерного топливного цикла в целом и осуществления мер, разработанных на первом этапе «Программы 93+2». Эти меры включают прежде всего анализ на непротиворечивость всей доступной информации, имеющей отношение к гарантиям. Для государств, заключивших ДП, агентство достигает наивысшего уровня действенности и эффективности гарантий благодаря осуществлению мер ДП:

декларации государства о его ядерном топливном цикле и дополнительном доступе инспекторов в места, связанные с топливным циклом и определенные в декларации. Интегрированные гарантии являются частным случаем осуществления этой концепции.

b. Осуществление гарантий в государствах, заключивших ПМК.

   В рамках КУГ объектом гарантий является выполнение государством его обязательств в соответствии с положениями соглашения. Для государства с ПМК цель процедур проверки — подтвердить заявленный государством ядерный статус, то есть подтвердить отсутствие ядерного материала в количестве, превышающем установленный лимит, и подтвердить отсутствие незаявленной ядерной деятельности. Фактически это цель (c), приведенная выше. В государствах с ПМК, не заключивших ДП, единственной доступной мерой для частичного достижения этой цели является анализ всей информации, имеющей отношение к гарантиям. Полностью цель может быть достигнута только для государств с ДП (Интегрированные гарантии). Информация об осуществлении гарантий в государствах с ПМК (около 100 стран) включена в рассмотрение в Докладе об осуществлении гарантий (ДОГ) начиная с 2003 г.

c. Прозрачность планирования и осуществление деятельности по проверке; прозрачность выводов и заключений.

   Планирование и осуществление контрольной деятельности менее прозрачны, чем в КУУ. Современные подходы по гарантиям для государства в целом, а также ежегодные планы по их осуществлению разрабатываются секретариатом отдельно для каждого государства. В настоящее время этот процесс недостаточно прозрачен с точки зрения государств. Кроме того, нет системы оценки достижения целей контрольной деятельности, подобной оценке достижения инспекционных целей в традиционных гарантиях. Заключения по гарантиям делаются на основе всей доступной информации, относящейся к ним. Ключевым моментом является анализ признаков переключения заявленного материала и наличия незаявленных ядерного материала и деятельности. Недостаточная прозрачность в осуществлении концепции стала одной из причин ее критики во время дискуссии 2012–2014 гг.

Как уже отмечалось выше, наиболее значимый шаг от КУУ к КУГ был сделан в ДОГ за 2003 г., когда агентство перешло от заключения, не зависящего от типа соглашений и сформулированного на уровне поставленных под гарантии установок, к заключению, сформулированному на уровне государств, с учетом их обязательств по соглашениям о гарантиях. Иными словами, рубеж между КУУ и КУГ был перейден в ДОГ за 2003 г. Однако этот шаг никак не отразился на деятельности специалистов, работающих в области международных гарантий. Секретариат агентства также не уделил этому должного внимания, сконцентрировав свои усилия на разработке внутренних руководств по подходу к осуществлению гарантий на уровне государства в рамках СВГ. Новая концепция не была должным образом документирована и не была своевременно доложена Совету управляющих. Даже современное определение КУГ секретариатом размытое и узконаправленное: «Способ осуществления гарантий путем рассмотрения в рамках соглашения о гарантиях, ядерной — и примыкающей к ядерной — деятельности государства и его возможностей в целом»[12]. В результате в ходе дискуссии 2012–2014 гг. кри-

тика государств оказалась направлена на саму концепцию, хотя, по сути, объектом критики было практическое осуществление концепции.

ДИСКУССИЯ О КОНЦЕПЦИИ ОСУЩЕСТВЛЕНИЯ ГАРАНТИЙ НА УРОВНЕ ГОСУДАРСТВА В 2012–2014 гг.

Основная часть дискуссии проходила на заседаниях Совета управляющих и Генеральной конференции МАГАТЭ и отражена во внутренних документах агентства. Суть дискуссии и ее результаты приводятся на основе докладов на симпозиуме МАГАТЭ по гарантиям[13], заявления представителя РФ при международных организациях в Вене, сделанном на симпозиуме по гарантиям[14], публикации[15] и резолюции по гарантиям Генеральной конференции МАГАТЭ 2014 г.[16].

В 2012 г. Российская Федерация и ряд других стран выступили с критикой КУГ. Критика включала следующие позиции:

- Концепция не была официально доложена Совету управляющих и не получила его одобрения.
- Отсутствует описание основных принципов и элементов концепции, которые были бы понятны государствам.
- Практическое осуществление концепции может приводить к субъективным и политически мотивированным заключениям.

В ходе дискуссии некоторые государства поставили под сомнение трактовку положений второй статьи СВГ и, соответственно, полномочия секретариата проверять полноту декларации государств, не заключивших ДП с агентством. Кроме того, секретариат обвинили в желании осуществлять процедуры ДП в тех странах, которые не ввели протокол в действие.

Генеральная конференция 2012 г. обязала гендиректора МАГАТЭ предоставить отчет Совету управляющих о развитии КУГ. Такой отчет был подготовлен и рассмотрен на сентябрьском заседании Совета управляющих 2013 г. Отчет объяснял, каким образом секретариат разрабатывает подходы по осуществлению гарантий для государства в целом и как такие подходы осуществляются в государствах с СВГ. Однако не все члены совета были удовлетворены объяснениями секретариата. Было решено, что секретариат подготовит дополнение к отчету для рассмотрения его перед Генеральной конференцией 2014 г. Параллельно с подготовкой дополнения к отчету секретариат провел в 2014 г. семь технических совещаний с представителями государств с целью обсуждения концепции и учета сделанных замечаний.

Это дополнение к отчету было рассмотрено в 2014 г. на сентябрьском заседании Совета управляющих и на Генеральной конференции. На этот раз Совет управляющих в целом был удовлетворен разъяснениями секретариата. Результаты обсуждения были отражены в резолюции Генконференции. В предваряющей части резолюции отмечалось, что при осуществлении гарантий в рамках СВГ агентство должно проверять достоверность и полноту заявлений государства и что ДП является важным инструментом повышения способности агентства формулировать выводы в отношении отсутствия незаявленных ядерного материала и деятельности. В постановляющей части приветствовались разъ-

яснения секретариата о том, что осуществление концепции будет проводиться строго в рамках существующих соглашений, что разработка и осуществление подхода для государства в целом будет проводиться в режиме консультаций с самим государством и что информация, относящаяся к гарантиям, будет применяться только для целей гарантий, а не для каких-то иных целей. Отмечалось, что секретариат будет продолжать информировать Совет управляющих о разработке и применении гарантий в контексте КУГ.

В своем заявлении на симпозиуме по гарантиям 2014 г. глава делегации РФ подчеркнул, что, несмотря на проделанную работу, разработка основ для применения КУГ не завершена. В частности он отметил три важных элемента, работа над которыми должна быть продолжена с тем, чтобы не допустить дискриминации в отношении отдельных государств:

- При использовании информации, полученной от сторон, не являющихся субъектами соглашения о гарантиях, секретариат должен указать источник информации и защитить ее достоверность на Совете управляющих.
- Следует разработать процедуру для ограничения произвольного увеличения секретариатом интенсивности проверок при обнаружении возможных признаков незаявленной ядерной деятельности в государстве с СВГ, но без ДП.

Страновые факторы (англ. State-specific factors), используемые секретариатом для подхода по гарантиям к государству в целом, должны быть объективными, а их набор — полным.

Дискуссия 2012–2014 гг. была своевременной и полезной для развития КУГ. Она продемонстрировала, что гарантии МАГАТЭ являются совместным предприятием агентства и государств. Важным итогом стало понимание необходимости продолжить диалог.

НА ПУТИ К СИСТЕМЕ ГАРАНТИЙ НА ГЛОБАЛЬНОМ УРОВНЕ?

В настоящее время гарантии применяются в государствах, заключивших соглашение о гарантиях с МАГАТЭ по одному из трех типов: соглашение о всеобъемлющих гарантиях (СВГ) в рамках ДНЯО для стран, не обладающих ядерным оружием; соглашение на добровольной основе для стран — членов ДНЯО, обладающих ядерным оружием; и соглашение по типу INFCIRC/66 для стран, не являющихся членами ДНЯО или какого-либо регионального договора, требующего отказа от ядерного оружия (Израиль, Индия, Пакистан).

ДОГ за 2015 г. содержит следующие данные о применении гарантий на 31 декабря 2015 г.:

- гарантии применялись в отношении 181 государства;
- в 173 государствах гарантии осуществлялись в рамках СВГ, в 5 государствах — в рамках соглашения на добровольной основе, в 3 государствах — в рамках соглашений по типу INFCIRC/66;
- 121 государство имело действующие СВГ и ДП, в 54 из них осуществлялись интегрированные гарантии;

- 52 государства с действующими СВГ еще не заключили ДП;
- 12 государств — участников ДНЯО еще не ввели в действие СВГ, как это требует статья III Договора;
- в настоящее время агентство не имеет возможности осуществлять контрольную деятельность в КНДР.

Основной вызов системе гарантий, а фактически — режиму нераспространения в целом, представляет противоречие между глобальной природой ядерных технологий и национальной природой ответственности и контроля[17]. С развитием инновационных технологий и их большей доступностью задачи режима нераспространения усложняются. Все больше новых стран становится обладателями ядерных технологий. Происходит постоянное увеличение инвентарных количеств и потоков ядерного материала в мире. Ответ этим вызовам состоит в работе над повышением действенности и эффективности системы гарантий.

КУГ обеспечивает существенное повышение действенности и эффективности гарантий и в среднесрочной перспективе будет, по-видимому, играть ведущую роль. Однако предстоит еще много сделать для ее развития. Есть проблемы с прозрачностью осуществления концепции и подготовки расширенных заключений. Концепция не проработана для соглашений на добровольной основе и для соглашений по типу INFCIRC/66.

Остановимся подробнее на проблеме прозрачности.

КУГ характеризуется тем, что формирует цели процедур проверки исходя из обязательств, взятых государством в соглашении о гарантиях. Для случая СВГ цели процедур проверки сформированы исходя из положений второй статьи соглашения. Здесь ключевым положением является задача обнаружения переключения ядерного материала из мирной деятельности на ядерное взрывное устройство. В рамках КУГ рассматриваются все промежуточные этапы возможных путей переключения ядерного материала, такие как конверсия, трансмутация, радиохимическая переработка и так далее. Иначе говоря, рассматриваются все стадии ядерного топливного цикла, необходимые для получения материала, пригодного для изготовления ядерного оружия. В ядерном топливном цикле конкретного государства, планирующего переключение, некоторые эти стадии уже могут существовать, а недостающие будут введены в строй, скорее всего, как незаявленные установки. Сам факт существования незаявленных ядерного материала и установок может быть интерпретирован как часть актуализированного пути переключения, поскольку этот материал и установки не находятся в заявленной **мирной деятельности**. Подход по гарантиям в рамках КУГ для данного государства будет содержать оптимальный набор мер по обнаружению путей переключения, характерных для ядерного топливного цикла государства.

Для стран с СВГ и ДП расширенное заключение формулируется следующим образом: «Секретариат не обнаружил признаков переключения заявленного ядерного материала из мирной ядерной деятельности и признаков присутствия незаявленных ядерного материала или деятельности. На этом основании секретариат заключает, что ядерный материал в государстве оставался в мирной деятельности». Ключевым фактором является то, что секретариат в результате своей контрольной деятельности не обнаружил признаков переключения и присутствия.

Вопрос сводится к тому, какие действия секретариат провел по проверкам в поле и по анализу доступной информации, для того чтобы прийти к такому заключению. Эти действия перечислены в подходе по гарантиям для каждого конкретного государства и в ежегодном плане по осуществлению подхода. Вместо рассмотрения индивидуальных подходов и планов по их осуществлению, было бы целесообразно подготовить стандартизованные подходы и планы для каждого типичного ядерного топливного цикла. Так, все страны с ПМК были бы объединены в одну группу, страны, имеющие только исследовательские установки — в следующую группу и далее. Такой подход значительно улучшил бы прозрачность осуществления КУГ секретариатом. Стандартизованные подходы для типичных ядерных топливных циклов дали бы возможность, по аналогии с критериями, проводить оценку достижения целей гарантий для каждого государства и управлять качеством осуществления подходов по гарантиям.

В долгосрочной перспективе вектор развития системы гарантий связан с будущим ДНЯО и зависит от прогресса в области ядерного разоружения (статья VI ДНЯО) и от обязательств стран, обладающих ядерным оружием, но не являющихся членами ДНЯО. В очень далекой перспективе можно было бы рассматривать ситуацию полного ядерного разоружения, когда СВГ и ДП или их будущие эквиваленты стали бы нормой для всех стран. И тогда уже или даже на более ранней стадии встал бы вопрос о концепции осуществления гарантий на глобальном уровне. Эта концепция рассматривала бы ядерные топливные циклы на региональных и мировом уровнях. Возможно, для этого потребуется новая редакция юридических инструментов системы. Однако путь в будущее и далек, и труден, а современное состояние вопросов ядерного разоружения и путей разрешения региональных конфликтов пока не дает оснований для оптимизма. Поэтому обсуждать эту перспективу, по-видимому, преждевременно.

Примечания

1 Такой подход был осуществлен в статье автора «Система гарантий МАГАТЭ: эволюция концепции» (*Ядерный клуб*. 2013. № 1–2), ставшей попыткой осмысления результатов эволюции системы за все время ее существования. Этот же подход продолжен и в настоящей работе, которая опирается на результаты предыдущей статьи. См. также: Бычков Валерий. Система гарантий МАГАТЭ: эволюция концепции. Сайт Центра энергетики и безопасности http://ceness-russia.org/data/doc/13-09-06%20IAEA%20Safegurds%20Evolution%20RUS.pdf (последнее посещение 22 декабря 2016 г.).

2 Соглашение о всеобъемлющих гарантиях, соглашение по типу INFCIRC/66 и соглашение на добровольной основе для ядерных стран — участников ДНЯО.

3 В начале 1990-х гг. в процессе разработки мер по укреплению гарантий Совет управляющих МАГАТЭ подтвердил, что в соответствии с параграфом 2 документа INFCIRC/153 агентство имеет право и обязанность не только проверить, что декларации государств о ядерном материале, подлежащем гарантиям, являются достоверными, но что они являются также полными. Laura Rockwood. Legal framework for IAEA safeguards. IAEA. P. 30–31. https://ola.iaea.org/ola/documents/pub1608_web-final.pdf (последнее посещение 22 декабря 2016 г.).

4 Документ INFCIRC/153 не представляет текст типового соглашения; текст типового соглашения содержится во внутреннем документе Агентства GOV/INF/276. С формулировкой аналога параграфа 28 можно ознакомиться, обратившись к любому действующему соглашению этого типа, например, к соглашению с Республикой Беларусь, INFCIRC/495. https://www.iaea.org/sites/default/files/infcirc495_rus.pdf (последнее посещение 22 декабря 2016 г.).

5 Каждая установка содержит одну или более зон баланса; из практических соображений нам удобнее рассматривать установки, а не зоны баланса, — этот подход использован в критериях по гаран-

тиям, которые будут рассмотрены ниже; чтобы упростить обсуждение мы не рассматриваем здесь заявленный материал, находящийся вне установок.

6 Ежегодный доклад генерального директора МАГАТЭ Совету управляющих. Первая часть доклада, содержащая заявление об осуществлении гарантий, а также общие сведения в связи с заявлением об осуществлении гарантий, доступна на сайте агентства.

7 Голдшмидт Пьер. Система гарантий МАГАТЭ вступает в XXI век. Приложение к *Бюллетеню МАГАТЭ*, 1999, декабрь. Т. 41, № 4.

8 ДП может быть заключен на добровольной основе с любым государством, имеющим соглашение о гарантиях с МАГАТЭ. В статье рассматривается осуществление ДП только для соглашений о всеобъемлющих гарантиях. Применение ДП для соглашений типа INFCIRC/66 и соглашений на добровольной основе требует отдельного рассмотрения, которое выходит за рамки данной статьи.

9 Внутренний документ Агентства GOV/2002/8. Концепция описана в публикации: Cooley Jill. Integrated nuclear safeguards: genesis and evolution. *Verification Yearbook* 2003. Center for security studies, ETH Zürich. https://www.files.ethz.ch/isn/13412/VY03_FULL.pdf (последнее посещение 22 декабря 2016 г.).

10 Государство и МАГАТЭ заключают Протокол о малых количествах (ПМК) к соглашению о всеобъемлющих гарантиях, если, согласно заявлению государства, количество имеющегося в государстве ядерного материала, подлежащего учету, не превышает установленного лимита. ПМК приостанавливает действие большинства процедур соглашения, в том числе процедур учета материала и инспекций. В 2005 г. Совет управляющих утвердил новую редакцию ПМК, которая содержит обязательство государства заявлять имеющийся ядерный материал и предоставлять в этом случае агентству возможность для проведения инспекций.

11 Это утверждение справедливо для ПМК, заключенных до 2005 года и для тех случаев в рамках ПМК в новой редакции, в которых государство заявляет об отсутствии любых количеств ядерного материала, подлежащего учету.

12 Jill N. Cooley. Overview of the development and discussion on evolving safeguards implementation. Symposium on International Safeguards: Linking Strategy, Implementation and People. October 2014, Vienna, Austria.

13 Symposium on International Safeguards: Linking Strategy, Implementation and People. Session SO1: Evolving Safeguards Implementation. October 2014, Vienna, Austria. Presentations by: J. Cooley, P. Burton, N. Kozlova, and D. Trimble.

14 Statement by the head of the delegation of the Russian Federation, Ambassador-at-large Grigory Berdennikov at the Symposium on International Safeguards: Linking Strategy, Implementation and People. October 2014, Vienna, Austria. https://www.iaea.org/safeguards/symposium/2014/images/pdfs/Russian_Statement.pdf (последнее посещение 22 декабря 2016 г.).

15 Rockwood Laura. The IAEA's State-level Concept and the Law of Unintended Consequences. Arms Control Today. September, 2014. https://www.armscontrol.org/act/2014_09/Features/The-IAEAs-State-Level-Concept-and-the-Law-of-Unintended-Consequences (последнее посещение 22 декабря 2016 г.).

16 Strengthening the Effectiveness and Improving the Efficiency of Agency Safeguards. Resolution adopted on 26 September 2014 during the tenth plenary meeting. GC (58)/RES/14/September 2014. https://www.iaea.org/About/Policy/GC/GC58/GC58Resolutions/English/gc58res-14_en.pdf (последнее посещение 22 декабря 2016 г.).

17 Culture of nuclear nonproliferation: multiple-author monograph / Ed.: V. Murogov. — Moscow: NRNU MEPhI, 2014. P. 50.

Станислав Кувалдин*

АТОМНАЯ ЭНЕРГЕТИКА И ПРОТИВОДЕЙСТВИЕ ИЗМЕНЕНИЮ КЛИМАТА В КОНТЕКСТЕ ПАРИЖСКОГО КЛИМАТИЧЕСКОГО СОГЛАШЕНИЯ

Парижское соглашение, принятое под эгидой Рамочной конвенции ООН об изменении климата, было заключено в 2015 г. и вступило в силу 4 ноября 2016 г. По состоянию на конец декабря 2016 г. соглашение ратифицировано 118 странами мира и является ключевым документом, призванным регулировать проводимую странами мира климатическую политику. Действие документа должно начаться после 2020 г., а его главной целью является реализация участниками совокупности мер, которая позволит до конца 21 века не допустить повышения температуры атмосферы Земли более чем на два градуса Цельсия по сравнению с доиндустриальным периодом. Также должны быть минимизированы отрицательные последствия неизбежного потепления (подъем уровня мирового океана вследствие таяния полярных льдов и теплового расширения воды, увеличение зоны пустынь, разрушение многолетней мерзлоты и др.) для жителей уязвимых регионов планеты.

Для достижения заявленных целей странам мира необходимо снизить антропогенное воздействие на климат и прежде всего добиться значительного сокращения эмиссии парниковых газов (углекислого газа, метана и ряда других) мировой экономикой. Увеличение концентрации парниковых газов, способных поглощать и повторно излучать инфракрасное излучение, приводит к увеличению температуры атмосферы, океана и изменению климата Земли. Одной из ключевых задач в этом отношении является снижение использования ископаемого топлива, сжигание которого приводит к поступлению в атмосферу больших объемов диоксида углерода (CO_2).

По данным Международного энергетического агентства (МЭА), наибольшая доля потребления ископаемого топлива в мире приходится на электроэнергетический сектор и теплоэнергетику. По оценкам МЭА, эти сектора в 2013 г. были ответственны за 42% объемов эмиссии парниковых газов, связанных с использованием ископаемого топлива[1]. Альтернативой этому топливу в энергетике могут служить источники энергии, использование которых не связано с эмиссией парниковых газов. К их числу, помимо возобновляемых источников энергии (ВИЭ), таких как солнечное излучение, энергия ветра, океанских приливов, тока речной воды и других, относится и энергия атома.

АТОМНЫЙ ВКЛАД

Усилия каждой страны в выполнении целей Парижского соглашения по удержанию роста глобальной температуры в пределах по сравнению с доиндустриальным периодом до конца 21 века, заявляются в добровольных национальных целях, которые каждая страна определяет самостоятельно, информируя об этом секретариат Рамочной конвенции ООН по изменению климата. Эти обязательства получили название Предполагаемых определяемых на национальном уровне вкладов[2] (в англоязычном варианте — Intended nationally determined contributions, или INDC). INDC составлялись в произвольном порядке без каких-либо указаний со стороны ООН о желательной форме и характере обязательств. После ратификации Парижского соглашения странами, подписавшими договор, их вклады перестают считаться предполагаемыми и определяются просто как Вклады на национальном уровне (в английской аббревиатуре NDC).

Поскольку каждая страна могла указывать на собственные способы достижения цели по снижению выбросов парниковых газов, атомная энергетика также могла быть указана в качестве одного из вариантов. Этот выбор предпочли сделать 9 стран. Среди уже ратифицировавших Парижское соглашение государств упоминание о роли атомных электростанций (АЭС) в решении национальных задач по снижению выбросов парниковых газов имеется у Аргентины, Белоруссии, Индии, Иордании, Китая, Нигера, Объединенных Арабских Эмиратов (ОАЭ) и Японии. Среди еще не ратифицировавших Парижское соглашение стран упоминание о роли атомной энергетики содержится в INDC Турции и Ирана.

Учитывая достаточно свободный порядок составления документа с формулированием национальных вкладов, оценить роль, которую атомная энергетика призвана играть в климатической политике, по ним непросто. Тем не менее можно отметить, что некоторые страны просто упомянули об имеющихся у них планах развития атомных проектов, в том числе в новом контексте снижения выбросов парниковых газов. Подобное краткое упоминание о развитии атомной энергетики содержится, в частности, у Турции, Ирана и Иордании. Минск, в свою очередь, в своих NDC отмечает, что даже с учетом ввода в строй Белорусской АЭС национальной экономике в ближайшие годы не удастся выполнить задачу по абсолютному снижению текущего объема выбросов[3].

ОАЭ в своем документе более четко указывают на то, что поставленная цель по увеличению доли чистых (в данном случае углеродно-нейтральных) источников энергии в энергобалансе страны до 24% в 2021 г. (по сравнению с 0,2% в 2014 г.) будет достигнута не в последнюю очередь за счет ввода в строй АЭС *Барака*[4]. Последнее вполне объяснимо с учетом того, что реализуемые сейчас в ОАЭ планы по развитию солнечной и ветряной генерации и производства электроэнергии из отходов предусматривают ввод 2,6 гигаватт (ГВт) мощностей на возобновляемых источниках энергии до 2030 г., тогда как АЭС Барака к 2020 г. должна обеспечить дополнительные 5,6 ГВт, причем с более высоким коэффициентом использования установленной мощности, чем у ВИЭ[5].

Во всех перечисленных случаях, кроме Ирана, речь идет о странах, лишь планирующих возведение АЭС на своей территории. Япония, также упоминающая

об атомной энергетике в своем NDC, напротив, имеет развитую сеть АЭС. Поэтому она посчитала важным упомянуть, что не планирует отказываться от использования атомной энергии в ближайшем будущем. Учитывая, что последний всплеск обеспокоенности общественного мнения в Японии и в мире в целом по поводу рисков использования атомной энергетики был связан с аварией на японской АЭС *Фукусима* в 2011 г., эти пояснения зафиксировали принципиальное отношение японских властей к атомной энергии. В частности в своем NDC Япония указывает, что АЭС в энергетическом балансе в 2030 г. будут отвечать примерно за 20–22% вырабатываемой электроэнергии[6]. Следует отметить, что по сравнению с периодом, предшествовавшим аварии на *Фукусиме*, доля энергии, вырабатываемой на АЭС должна сократиться (в 2011 г., по данным, приводимым Всемирной ядерной ассоциацией, Япония получала от АЭС 30% вырабатываемой электроэнергии[7]). Однако с учетом того, что вскоре после аварии 2011 г. Япония вывела из эксплуатации все действующие АЭС и начала сложный процесс проверки безопасности действующих реакторов, данные DNC фактически отражают возвращение прежней роли АЭС в качестве важного источника энергии для национальной экономики. В настоящее время реакторы, признанные безопасными после проведенной проверки, заново запускаются в эксплуатацию. Сохранение доли электроэнергии, вырабатываемой на АЭС на уровне 20–22% в энергобалансе страны, зафиксировано в Четвертом базовом энергетическом плане страны, принятом кабинетом министров в 2014 г. Среди последствий временного отказа Японии от ядерной энергии в этом документе упоминается о росте выбросов парниковых газов японской экономикой в связи с необходимостью вырабатывать энергию из ископаемого топлива[8].

Наиболее твердо о роли атомной энергии в своих планах по реализации Парижского соглашения заявил Дели. В NDC Индии упоминается о намерении резко увеличить мощность собственных атомных электростанций. К 2032 г. АЭС Индии должны иметь мощность 63 ГВт электроэнергии по сравнению с примерно 5,8 ГВт в настоящее время[9]. Пожалуй, это один из самых амбициозных планов по развитию атомной энергетики, реализуемых в настоящее время в мире. Тем не менее следует заметить, что реалистичность данного плана вызывает определенные сомнения. В частности Всемирная ядерная ассоциация ссылается на результаты запроса парламента Индии 2011 г., согласно которому к 2032 г. реалистичнее ожидать увеличение мощности АЭС Индии до 27,5 ГВт[10]. В самом NDC Индии планы по доведению мощностей АЭС страны до 63 ГВт также формулируются в несколько гипотетическом ключе. Говорится лишь о предпринимаемых усилиях по достижению этих показателей. Кроме того, сами показатели ставятся в зависимость от достижения договоренности об обеспечении поставок ядерного топлива на новые АЭС[11]. Следует отметить, что с учетом роста энергопотребления в стране фактически роль АЭС в энергобалансе останется достаточно скромной. В настоящее время АЭС обеспечивают чуть больше 2% вырабатываемого в Индии электричества. При этом, согласно докладу Комиссии по планированию правительства Индии, составленному в 2006 г. и анализирующему различные сценарии решения проблем энергетического обеспечения, даже самые масштабные планы строительства АЭС (в 2006 г. аналитики Комиссии по планированию рассматривали вариант с 20-кратным увеличением мощностей индийских АЭС) с учетом роста энергопотребления позволят расширить

долю АЭС в энергобалансе страны чуть менее чем до 6,5%[12]. Стоит заметить, что планы Индии по развитию других видов чистой энергии выглядят еще более амбициозными. В частности уже в 2022 г. Индия планирует довести мощности своей солнечной генерации до 100 ГВт. Эти показатели являются частью плана «Solar Mission», провозглашенного правительством Нарендра Моди как ответ Индии на проблему изменения климата.

Китай также упоминает о планах развития атомной энергетики как одной из мер по декарбонизации экономики. В NDC Китая дается обзор достижений страны по снижению углеродоемкости национальной экономики, среди которых также упомянуто увеличение к 2014 г. мощностей АЭС почти в три раза по сравнению с 2005 г. и доведение их до 19,88 ГВт[13]. В собственных INDC Китай не приводит подробностей дальнейшего развития атомной энергетики (хотя считает нужным упомянуть о том, какие мощности солнечной и ветряной генерации планируется ввести в строй в ближайшие годы). Тем не менее известно, что согласно 13-му 5-летнему плану Китая мощность генерации АЭС к 2020 г. планируется довести почти до 58 ГВт[14]. При этом, согласно некоторым авторитетным расчетам, для выполнения Китаем взятых на себя обязательств в рамках Парижского соглашения по доведению к 2030 г. доли неископаемых источников энергии в энергетическом балансе страны до 20%, а также по достижению к этому времени пика выбросов парниковых газов национальной экономикой, мощность АЭС Китая (наряду с развитием возобновляемых источников энергии) к 2030 г. должна быть доведена до 150 ГВт. Впрочем, планы развития мощностей ветряной и солнечной энергетики до этого же периода должны быть еще выше: 400 и 350 ГВт соответственно[15].

Россия подписала Парижское соглашение в апреле 2016 г., а процесс его ратификации начнется не раньше 2019 г.[16]. Несмотря на то что атомная энергетика отвечает за 18,6% электрической генерации в России[17], Москва не заявляла о роли мирного атома в своих INDC[18]. При этом Государственная корпорация «Росатом» активно участвует в сессиях Конференции сторон Рамочной конвенции ООН об изменении климата. 17 ноября 2016 г. в рамках 22-й сессии в Марракеше российская делегация организовала специальное мероприятие, одной из тем которого стало развитие атомной энергетики в качестве возможного ответа на климатические изменения. Участие в мероприятии принял первый заместитель генерального директора ГК «Росатом». По оценкам ряда участников, в Марракеше Россия была главным сторонником атомной энергетики.

Таким образом, атомная энергетика занимает свое место в реализации целей Парижского соглашения, поставленных рядом стран. При этом в таких странах, как Китай и Индия, развитие атомной энергетики составляет существенный элемент национальных планов снижения углеродоемкости наряду с планами увеличения солнечной и ветряной генерации. Само упоминание атомной энергетики в INDC некоторых стран не превращает развитие атомной энергетики в предпочтительную стратегию снижения углеродоемкости национальных экономик (хотя в некоторых странах, в частности в ОАЭ, возможное появление АЭС станет существенным вкладом в снижение эмиссии парниковых газов). Учитывая невы-

сокое количество стран, заявивших об атомной энергетике в своих NDC, ее роль в реализации Парижского соглашения, очевидно, останется ограниченной, хотя и важной для некоторых стран.

ПОЙМАТЬ ВЕТЕР ПАРИЖА

Учитывая свой низкоуглеродный статус, атомная отрасль заинтересована в том, чтобы отразить свои интересы в рамках Парижского соглашения. Международное агентство по атомной энергии (МАГАТЭ) — международная организация, координирующая использование атома в мирных целях, принимает участие в конференциях Рамочной конвенции ООН по изменению климата, в том числе в переговорах 2015 г., приведших к заключению Парижского соглашения. Тем не менее роль МАГАТЭ на подобных переговорах остается достаточно скромной. Наряду с другими участниками, предлагающими собственные решения для снижения выбросов парниковых газов, МАГАТЭ проводит мероприятия и распространяет информационные материалы о вкладе, который могут внести в решение этого вопроса АЭС и другие виды использования мирного атома. В этом смысле влияние организации и приводимых ею доводов на ход переговоров достаточно ограниченно. Всемирная ядерная ассоциация — организация, официально занимающаяся продвижением интересов атомной индустрии, также принимает участие в климатических переговорах. Не стала исключением и последняя конференция ООН по изменению климата, проходившая в Марракеше в ноябре 2016 г. Выступая на пресс-конференции на полях конференции председатель Всемирной ядерной ассоциации Агнета Райзинг озвучила цель возвести до 2050 г. 1000 ГВт новых мощностей атомной энергетики[19]. Отчасти она согласуется с расчетами МАГАТЭ, согласно которым для удовлетворения мировых энергетических потребностей и достижения планируемых странами мира целей по снижению эмиссии парниковых газов мировую ядерную генерацию к 2050 г. необходимо увеличить до 900 ГВт[20]. Тем не менее с учетом нынешнего уровня заказов на новые АЭС в мире подобные планы не выглядят реалистичными.

Как бы то ни было Парижское климатическое соглашение не содержит прямых запретов на использование атомной энергетики для решения поставленных задач по удержанию повышения глобальной температуры в пределах двух градусов Цельсия по сравнению с доиндустриальным периодом. В этом заключается коренное различие Парижского соглашения с механизмом реализации предыдущего климатического соглашения, формально продолжающего свое действие до 2020 г. — Киотского протокола. Киотский протокол является особым дополнением к Рамочной конвенции об изменении климата ООН, принятым в 1997 г. и вступившим в силу в 2005 г. Согласно положениям Киотского протокола, присоединившиеся к данному соглашению развитые страны брали на себя обязательства снизить общее поступление парниковых газов в атмосферу на 5% по сравнению с 1990 г. При этом цели по снижению эмиссии должны быть достигнуты не только за счет действий внутри стран, но и с помощью различных рыночных мер, таких, как торговля углеродными квотами, а также так называемых *механизмов гибкости*, то есть вариантов сотрудничества между развитыми и разви-

вающимися странами, позволяющих развитым странам осуществлять проекты, направленные на снижение выбросов парниковых газов в других государствах.

Марракешские соглашения 2001 г. (не путать с Марракешской климатической конференцией, состоявшейся в 2016 г.), определившие правила применения предусмотренных Киотским протоколом механизмов, содержат указание на то, что развитые страны должны воздерживаться от использования в торговле углеродными квотами тех углеродных единиц, которые получены в результате реализации атомных проектов на чужой территории. Иными словами, строительство странами, обладающими ядерной технологией, АЭС в развивающейся стране или финансирование такого строительства, несмотря на достигаемое в результате реализации подобного проекта прямое или косвенное (то есть в сравнении с альтернативными энергетическими проектами) снижение выбросов парниковых газов, не могло стать основанием для выпуска дополнительных углеродных квот. Само по себе подобное правило не являлось ограничением для развития атомной энергетики, оно лишь не включало атомные проекты в систему рыночного поощрения «зеленых инвестиций», таких как механизм чистого развития и проекты совместного осуществления.

Впрочем, наличие рыночных механизмов регулирования климатической политики было отличительной особенностью Киотского протокола. Парижское соглашение охватывает более широкий круг стран по сравнению с Киотским протоколом, предусматривает более широкий набор мер реализуемой политики и состоит из добровольно принимаемых на себя странами-участницами обязательств. Это, в том числе, не дает возможность как-либо ограничивать страны в достижении заявленных мер. Статья 6 Парижского соглашения предусматривает возможность создания добровольного рынка странами-участницами, для реализации которого также предполагается создание отдельного механизма, получившего название механизм устойчивого развития. Конкретные правила реализации подобного механизма еще не выработаны, однако фактически в данном случае речь идет о вмонтировании элементов углеродного регулирования и международной кооперации в логику Парижского соглашения. В настоящее время никаких признаков, указывающих на то, что в этом механизме могут быть устранены введенные Киотским протоколом ограничения и реализация атомных проектов вне собственных стран может быть зачтена в качестве части национального вклада в Парижское соглашение, нет.

Впрочем, главным финансовым механизмом Парижского соглашения должно стать предусмотренное документом в соответствии со статьей 9 предоставление развитыми странами различных видов помощи развивающимся странам, направленных на содействие адаптации к климатическим изменениям и осуществление мероприятий по смягчению роста глобальной температуры (то есть снижению выбросов парниковых газов). При этом в преамбуле соглашения фиксируется ориентировочный объем такой помощи со стороны развитых стран в размере 100 млрд долларов в год начиная с 2020 г. Именно налаживание подобного финансового, а значит, и технологического потока из развитых стран в адрес развивающихся должно стать главным фактором, создающим новые постпарижские реалии. И, очевидно, именно за эти солидные *климатические*

финансы развернется основная конкуренция между различными технологическими проектами.

Интересно задаться вопросом о том, можно ли часть этих финансовых потоков будет направить в том числе на финансирование строительства АЭС. Положительный ответ именно на этот вопрос может сделать Парижское соглашение фактором стимулирования атомной энергетики. Хотя действие Парижского соглашения еще не началось, на последней сессии конференции сторон Рамочной конвенции ООН об изменении климата в Марракеше были рассмотрены и помещены в официальные документы расчеты потока климатического финансирования в 2013–2014 гг. В этом потоке были учтены прямая помощь развивающимся странам из бюджетов развитых стран, средства, проходящие через различные банки развития и частные инвестиции, мобилизованные правительствами развитых стран. Такой поток оценен в 53 млрд долларов в 2013 г. и 61 млрд долларов в 2014 г. Среди планов распределения этих средств атомная энергетика отсутствует. Ориентируясь на существующую динамику, можно предположить, что планируемая цель по аккумуляции 100 млрд долларов на «климатические» цели в 2020 г. будет достигнута без учета атомных проектов и атомная энергетика не войдет в методики подсчета «климатических» инвестиций.

Одним из инструментов финансирования подобных проектов, хотя и далеко не крупнейшим из них, станет Зеленый климатический фонд ООН, учрежденный в 2010 г. специально для финансирования проектов, направленных на снижение эмиссии парниковых газов. Пока сумма объявленных взносов в фонд составляет 10,3 млрд долларов. Общая сумма средств, направленных на финансирование пилотных климатических проектов на весну 2016 г. составляла 168 млн долларов. Кроме того, объявлено о том, что 200 млн долларов из средств Зеленого климатического фонда ООН будут направлены на поддержку инициатив малого и среднего бизнеса развивающихся стран, еще 200 млн долларов будут предоставлены различным институтам развивающихся стран как национального, так и регионального уровня на реализацию 10 пилотных проектов[21]. В целом, характер финансирования, осуществляющийся фондом на сегодняшний день, также не позволяет говорить о том, что его средства могут достаться атомным проектам. Теоретически такая вероятность существует, однако деятельность фонда находится под столь внимательным и критическим взглядом экологических организаций, что фактически возможность подобных инвестиций представляется почти невероятной.

ОБЪЕКТИВНЫЕ ТРУДНОСТИ

На достаточно ограниченное позиционирование атомной энергетики в качестве инструмента снижения выбросов парниковых газов влияет целый ряд факторов. Одним из них, безусловно, служит репутация. Аварии на АЭС *Три-Майл-Айленд* в США в 1979 г., на *Чернобыльской* АЭС в СССР в 1986 г. и на АЭС *Фукусима-1* в 2011 г. повлияли на то, что атомная энергетика имеет крайне неоднозначную репутацию в общественном мнении многих стран. Авторитетные неправительственные организации, а также политические партии с экологической повесткой в течение многих десятилетий проводили кампании против активного исполь-

зования атомной энергетики. Учитывая же, что поддержка этих структур крайне важна для реализации Парижского соглашения, вряд ли можно рассчитывать на то, что продвижение атомной энергии в качестве инструмента средства снижения выбросов, не встретит серьезных препятствий.

Ряд экологически ориентированных некоммерческих организаций (НКО) уже высказывали опасения, что устав Зеленого климатического фонда прописан не вполне четко и допускает финансирования «грязных» и небезопасных с их точки зрения, в том числе низкоуглеродных, проектов, связанных с использованием ископаемого топлива, а также ядерных технологий[22]. Организация Germanwatch в своем обзоре текущей деятельности фонда также призывает к сохранению постоянного контроля структур гражданского общества за реализуемыми фондом проектами, для того чтобы предотвратить направление средств фонда на противоречивые инициативы, к каковым организация относит и поддержку строительства АЭС[23].

Стоит отметить, что проект стратегического плана Зеленого климатического фонда, получивший одобрение на климатической конференции в Марракеше содержит упоминание о том, что Фонд должен финансировать «инновационные проекты и программы, в том числе способствующие применению и распространению новейших климатических технологий, характеризующихся высочайшим уровнем целей и задач, направленных на предотвращение изменения климата и адаптацию, которые могут быть масштабированы и/или воспроизведены, либо привести к фундаментальным изменениям в <…> направлениях инвестиций»[24]. Но рассчитывать на данную отсылку атомной энергетике стоит едва ли из-за противодействия вышеупомянутых экологических организаций.

Постоянное давление со стороны НКО и экологических организаций видится важным фактором и для определения перспектив возможного направления на атомные проекты и других средств в рамках помощи развивающимся странам на адаптацию к климатическим изменениям и предотвращение изменений климата. Главными донорами в рамках реализации планов Парижского соглашения должны стать развитые страны, причем во многих из них настороженно относятся к атомным проектам, во всяком случае к включению строительства новых АЭС в число проектов, направленных на предотвращение изменения климата. Поэтому с подключением атомных проектов к климатическим финансовым потокам в обозримом будущем видятся малопреодолимые сложности.

Впрочем, необходимо заметить, что подобный подход характерен и для других международных механизмов. В 2013 г. о своем отказе от финансирования строительства АЭС от имени Всемирного банка объявил президент этого финансового института Джим Ен Ким, мотивируя это тем, что «атомная энергетика является очень чувствительным политическим вопросом, ответ на который меняется от страны к стране»[25]. Воздерживается от финансирования атомных проектов и Международная финансовая корпорация. В подобных условиях рассчитывать на возможность направления климатических ресурсов на атомные проекты затруднительно.

РАБОЧАЯ РОЛЬ В ПРОЦЕССЕ ДЕКАРБОНИЗАЦИИ

Тем не менее вряд ли можно говорить о том, что снижение углеродоемкости мировой энергетики может произойти без учета фактора атомной энергии. Так или иначе атомная энергетика занимает свою долю в мировом энергетическом балансе, это проверенная и эффективная технология с практически нулевой эмиссией парниковых газов. Поэтому не учитывать данный фактор при расчете практических путей снижения эмиссии парниковых газов мировой экономикой практически невозможно. В частности учет атомной энергетики присутствует в расчетах сценариев декарбонизации мировой экономики, производимых созданной под эгидой ООН исследовательской организации Sustainable Development Solutions Network[26]. В опубликованной в 2014 г. группой исследователей под руководством Питера Лофтуса научной статье было проведено исследование 17 возможных сценариев декарбонизации мировой экономики, предложенных разными группами специалистов. Исследователи пришли к выводу, что сценарии, предполагавшие полностью игнорировать атомную энергетику и полагавшиеся исключительно на возобновляемые источники энергии, требовали беспрецедентного с учетом тенденций последних десятилетий увеличения энергоэффективности мировой экономики и соответствующих технологий, а потому они вряд ли могут считаться обоснованными[27].

МЭА, регулярно оценивающее перспективы развития различных энергетических секторов и в частности вероятные способы реализации различных климатических сценариев в докладе, выпущенном в 2016 г., предполагает, что для снижения выбросов парниковых газов в том объеме, в каком это необходимо для предотвращения повышения земной атмосферы выше двух градусов по сравнению с доиндустриальным периодом, необходимо учитывать и роль атомной энергетики. Впрочем, сейчас эта роль видится агентству довольно ограниченной, и общий вклад атомного сектора в объемы снижения выбросов с учетом современных тенденций развития мировой энергетики до 2050 г. оценивается на уровне 7%[28].

Ряд расчетов, показывают, что, комбинируя атомную энергетику с генерацией возобновляемых источников энергии, можно получить удачный вариант практически безуглеродного энергобаланса[29]. Инициатива Росатома по поддержке проектов ветряной генерации[30], по-видимому, показывает, что подобные вычисления до некоторой степени признаны перспективными и в России.

Оценивая возможную роль атомной энергетики в выполнении целей Парижского соглашения, следует отметить два связанных между собой обстоятельства. Первое — несмотря на то что атомная энергетика остается *фигурой умолчания* во многих широко обсуждаемых планах снижения эмиссии парниковых газов мировой экономикой, тем не менее атомные проекты являются составной частью планов декарбонизации энергетики ряда стран мира; кроме того, реализация мировых сценариев декарбонизации, полностью игнорирующих атомную энергетику, в обозримом будущем представляется маловероятной.

Второе — по ряду причин (в том числе из-за высокой стоимости атомных проектов и настороженного отношения мирового общественного мнения к развитию атомной энергетики) большинство стран не будет считать строительство АЭС предпочтительным направлением решения задач по снижению эмиссии парниковых газов, кроме того, подобные проекты почти наверняка не смогут претендовать на финансирование за счет международных ресурсов направляемых в рамках Парижского соглашения на поддержку усилий развивающихся стран по снижению углеродоемкости их экономик.

Атомная энергетика, безусловно, соответствует задачам снижения эмиссии парниковых газов мировой экономикой, которые намерены решить страны, подписавшие Парижское соглашение, но в ближайшие годы АЭС будет отведена своя рабочая, но не ключевая роль в процессе декарбонизации энергетики, при этом атомные проекты в нынешних обстоятельствах едва ли смогут рассчитывать на привлечение климатического финансирования.

Примечания

* Автор выражает благодарность А. Кокорину за оказанные консультации.

1 Подробнее см. CO2 Emissons From Fuel Combustion Highlights, IEA, 2015 https://www.iea.org/publications/freepublications/publication/CO2EmissionsFromFuelCombustionHighlights2015.pdf (последнее посещение 22 декабря 2016 г.).

2 Парижское соглашение. Статья 3. http://unfccc.int/files/essential_background/convention/application/pdf/russian_paris_agreement.pdf (последнее посещение 22 декабря 2016 г.).

3 Подробнее см. Предполагаемые национально-определяемые вклады Республики Беларусь. Министерство природных ресурсов и охраны окружающей среды Республики Беларусь http://www.minpriroda.gov.by/uploads/files/Belarus-INDC-v4-4-r-1.pdf (последнее посещение 22 декабря 2016 г.).

4 Подробнее см. Intended Nationally Determined Contribution of the United Arab Emirates. UN Climate Change Newsroom. http://www4.unfccc.int/ndcregistry/PublishedDocuments/United%20Arab%20Emirates%20First/UAE%20INDC%20-%2022%20October.pdf (последнее посещение 22 декабря 2016 г.).

5 Данные из совместного доклада агентства IRENA, Масдарского института науки и технологии и Министерства иностранных дел ОАЭ Renewable Energy Prospects: United Arab Emirates http://www.irena.org/remap/irena_remap_uae_report_2015.pdf (последнее посещение 22 декабря 2016 г.).

6 Подробнее см. Submission of Japan's Intended Nationally Determined Contribution. UN Climate Change Newsroom. http://www4.unfccc.int/submissions/INDC/Published%20Documents/Japan/1/20150717_Japan's%20INDC.pdf (последнее посещение 22 декабря 2016 г.).

7 См. в частности: Nuclear Power in Japan. World Nuclear Association. http://www.world-nuclear.org/information-library/country-profiles/countries-g-n/japan-nuclear-power.aspx (последнее посещение 22 декабря 2016 г.).

8 Англоязычная версия плана представлена здесь: Strategic Energy Plan. Agency for Natural Resources and Energy. April, 2014. http://www.enecho.meti.go.jp/en/category/others/basic_plan/pdf/4th_strategic_energy_plan.pdf, see page 9 (последнее посещение 22 декабря 2016 г.).

9 Подробнее см. India's Intended Nationally Determined Contribution. UN Climate Change Newsroom. http://www4.unfccc.int/submissions/INDC/Published%20Documents/India/1/INDIA%20INDC%20TO%20UNFCCC.pdf (последнее посещение 22 декабря 2016 г.).

10 См. в частности: Nuclear Power in India. World Nuclear Association. http://www.world-nuclear.org/information-library/country-profiles/countries-g-n/india.aspx (последнее посещение 22 декабря 2016 г.).

11 India's Intended Nationally Determined Contribution. UN Climate Change Newsroom. http://www4.unfccc.int/submissions/INDC/Published%20Documents/India/1/INDIA%20INDC%20TO%20UNFCCC.pdf (последнее посещение 22 декабря 2016 г.).

12 Integrated Energy Policy. Report of the Expert Committee. Government of India, 2006. P. xxii http://planningcommission.nic.in/reports/genrep/rep_intengy.pdf (последнее посещение 22 декабря 2016 г.).

13 Подробнее см. China' S Intended Nationally Determined Contributions. UN Climate Change Newsroom. http://www4.unfccc.int/Submissions/INDC/Published%20Documents/China/1/China's%20INDC%20-%20on%2030%20June%202015.pdf (последнее посещение 22 декабря 2016 г.).

14 Краткий обзор энергетических планов Китая в XIII 5-летнем плане взят здесь: China's 13th Five Year Plan offers no hope for coal markets, further suppressing CO2 emissions. Carbon Tracker. http://www.carbontracker.org/china-five-year-plan-coal-co2-emissions-renewables (последнее посещение 22 декабря 2016 г.).

15 Jian-Kun He, China's INDC and non-fossil energy development. Advances in Climate Change Research. Volume 6, Issues 3–4 http://www.sciencedirect.com/science/article/pii/S1674927815300058 (последнее посещение 22 декабря 2016 г.).

16 Распоряжение № 2344-р от 3 ноября 2016 г. Правительства Российской Федерации. http://www.pravo.gov.ru/laws/acts/85/50515252451088.html (последнее посещение 22 декабря 2016 г.).

17 Russian Federation. IAEA Power Reactor Information System. https://www.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=RU (последнее посещение 22 декабря 2016 г.).

18 Intended Nationally Determined Contribution submitted by the Russian Federation. UN Climate Change Newsroom.http://www4.unfccc.int/submissions/INDC/Published%20Documents/Russia/1/Russian%20Submission%20INDC_eng_rev1.doc (последнее посещение 22 декабря 2016 г.).

19 См. в частности: Nuclear must be part of the international response to climate change. World Nuclear Association. http://www.world-nuclear.org/press/press-statements/nuclear-must-be-part-of-the-international-response.aspx (последнее посещение 22 декабря 2016 г.).

20 Подробнее см. Nuclear Power and Paris Agreement, IAEA. 2015 https://www.iaea.org/sites/default/files/16/11/np-parisagreement.pdf (последнее посещение 22 декабря 2016 г.).

21 См. в частности обзор https://germanwatch.org/de/download/16139.pdf (последнее посещение 22 декабря 2016 г.).

22 См. в частности Dirty energy financed by the Green Climate Fund? Should we worry? Friends of Earth. April 24, 2015 http://www.foe.org/news/archives/2015-04-dirty-energy-financed-by-the-green-climate-fund (последнее посещение 22 декабря 2016 г.).

23 Green Climate Fund: The Basics. Germanwatch. May, 2016. https://germanwatch.org/de/download/16139.pdf (последнее посещение 22 декабря 2016 г.).

24 С текстом плана можно ознакомиться здесь: Report on the development of the Draft Strategic Plan for the Green Climate Fund. Submission from the ad hoc group of Board/Alternate members. P.3 March 3, 2016. https://www.greenclimate.fund/documents/20182/184476/GCF_B.12_06_-_Report_on_the_development_of_the_Draft_Strategic_Plan_for_the_Green_Climate_Fund_Submission_from_the_ad_hoc_group_of_Board_Alternate_members.pdf/9f3e48d5-a8bd-4a4d-91d2-31a841f98bfa (последнее посещение 22 декабря 2016 г.).

25 См. в частности: World Bank says no money for nuclear power. Phys. November 27, 2013. http://phys.org/news/2013-11-world-bank-money-nuclear-power.html (последнее посещение 22 декабря 2016 г.).

26 С последним докладом организации можно ознакомиться здесь: Pathways to deep decarbonization. SDSN — IDDRI. December, 2015. http://deepdecarbonization.org/wp-content/uploads/2015/12/DDPP_2015_REPORT.pdf (последнее посещение 22 декабря 2016 г.).

27 Подробнее см. Peter J. Loftus, Armond M. Cohen, Jane C. S. Long, Jesse D. Jenkins, A critical review of global decarbonization scenarios: what do they tell us about feasibility?, WIREs Clim Change, 6: 93–112. 2014. http://onlinelibrary.wiley.com/doi/10.1002/wcc.324/abstract (последнее посещение 22 декабря 2016 г.).

28 Подробнее см. Energy Technology Perspective 2016. IEA. https://www.iea.org/publications/freepublications/publication/EnergyTechnologyPerspectives2016_ExecutiveSummary_EnglishVersion.pdf (последнее посещение 22 декабря 2016 г.).

29 См. в частности: Charles W. Forsberg, Sustainability by combining nuclear, fossil, and renewable energy sources, Prog. Nucl. Energy, 2008. http://web.mit.edu/ans/www/documents/seminar/F08/forsbergpaper.pdf.

30 См. в частности: Анастасия Фомичева. Атомный ветер. Коммерсант, 03.06.2016. http://kommersant.ru/doc/3002870 (последнее посещение 22 декабря 2016 г.).

Тереза Хитченс

ПРАВА И СВОБОДЫ НА ОРБИТЕ — КАК ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ КОСМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Космическое пространство продолжает все активнее использоваться в военных, гражданских и коммерческих целях, в космической деятельности участвует все больше заинтересованных сторон, а возможность применять спутниковые технологии становится критической для нормального функционирования общества. Космические технологии находятся на подъеме: страны уже начали использовать сверхмалые спутники типа *CubeSat* и созвездия спутников. Добыча полезных ископаемых на астероидах и массовый космический туризм перестали быть фантастикой — живущие сегодня поколения вполне смогут застать эти новшества. Но новые возможности несут в себе и риски — соперничество в космосе может стать причиной межстрановых конфликтов. При этом к двум традиционным космическим сверхдержавам — России и США — присоединилось много новых игроков: в космосе сегодня представлены не только страны, но и, например, университеты и некоммерческие организации.

Быстрое развитие технологий также означает, что национальные и международные институты, призванные их регулировать, не успевают за их развитием. Наконец международные институты и международное право, созданные в годы холодной войны, давно устарели; это видно, в частности, на примере того, что вопросы мирного и военного использования космического пространства необоснованно разграничиваются.

Вся деятельность, которая ведется в космическом пространстве, регулируется на двух уровнях законодательства: международном и национальном. Первый уровень основан на международных договорах, а также на общепринятых практиках и нормах, относящихся к области *мягкого права*. Второй включает законы и подзаконные акты отдельных государств, а также регулятивные документы и правила различных организаций. Основными задачами правового регулирования космической деятельности на данном этапе являются обеспечение **безопасности** (англ. — *security*) в военном аспекте, **защищенности** (англ. — *safety*) людей и природной среды и достижение **устойчивости** (англ. — *sustainability*) в использова-

нии космического пространства в долгосрочной перспективе. Все три задачи взаимосвязаны и дополняют друг друга.

РЕГУЛИРОВАНИЕ КОСМИЧЕСКОГО МАСШТАБА

Существующая сегодня система международного космического права основывается на четырех соглашениях, принятых под эгидой ООН:

- Договор о космосе 1967 г.;
- Соглашение о спасании космонавтов, возвращении космонавтов и возвращении объектов, запущенных в космическое пространство 1967 г.;
- Конвенция о международной ответственности за ущерб, причиненный космическими объектами 1971 г.;
- Конвенция о регистрации объектов, запускаемых в космическое пространство 1974 г.

Пятый документ, принятый Генеральной ассамблеей ООН в 1979 г. — Соглашение о деятельности государств на Луне и других небесных телах, не был ратифицирован ведущими космическими державами и не имеет в настоящее время практического значения.

Кроме документов, принятых под эгидой ООН, важным элементом системы международного космического права является деятельность специализированного агентства ООН Международного союза электросвязи (МСЭ). К сожалению, усилия агентства зачастую игнорируются. В рамках своего мандата по развитию и регулированию информационно-коммуникационных технологий МСЭ распределяет между государствами спутниковые орбиты. Устоявшееся представление о космосе как о большом пустом пространстве является ложным — геостационарная и низкая околоземная орбиты используются очень активно. Доступ к околоземному пространству важно контролировать, с тем чтобы функционирование спутниковых систем тех или иных государств оставалось бесперебойным. Эту функцию и выполняет МСЭ.

Международные договоры, регулирующие космическую деятельность, дополняются нормами *мягкого права*. Среди них можно выделить пять ключевых политических договоренностей, принятых в рамках ООН, однако не являющихся юридически обязывающими:

- Декларация правовых принципов, регулирующих деятельность государств по исследованию и использованию космического пространства 1963 г.;
- Принципы использования государствами искусственных спутников Земли для международного непосредственного телевизионного вещания 1982 г.;
- Принципы, касающиеся дистанционного зондирования Земли из космического пространства, 1986 г.;
- Принципы, касающиеся использования ядерных источников энергии в космическом пространстве, 1992 г.;

- Декларация о международном сотрудничестве в исследовании и использовании космического пространства на благо и в интересах всех государств, с особым учетом потребностей развивающихся стран 1996 г.

Развитие международного *мягкого права* в космической сфере продолжается и сегодня, в частности в рамках Комитета ООН по использованию космического пространства в мирных целях. Особо следует отметить продолжающуюся работу над дополнением Руководящих принципов по предупреждению образования космического мусора (2007 г.). Термин «космический мусор» определить сложно, однако необходимо признать, что при каждом использовании космического пространства в космосе остается определенное количество мусора, представляющего серьезную опасность. Даже небольшой обломок вышедших из строя объектов может легко пробить обшивку спутника и уничтожить его.

Деятельность Рабочей группы по долгосрочной устойчивости космической деятельности также способствует развитию *мягкого права* в области освоения космоса. В 2016 г. был принят первый свод Руководящих принципов обеспечения долгосрочной устойчивости космической деятельности. Документ содержит полезные положения, но, что наиболее важно, его появление свидетельствует о том, что, несмотря на тяжелую геополитическую обстановку и конфликт между Россией и США, конструктивная совместная работа в сфере космической безопасности действительно возможна. Эта работа дает надежду на улучшение двухсторонних российско-американских отношений.

В 2013 г. Группа правительственных экспертов (ГПЭ) по выработке мер транспарентности и доверия в отношении космической деятельности выпустила доклад, посвященный вопросам безопасности в космическом пространстве. В докладе были проанализированы вопросы обеспечения безопасности и снижения вероятности конфликтов в космическом пространстве. Там же был представлен согласованный ряд мер по установлению и укреплению доверия, которые становятся все более необходимыми по мере усиления угрозы гонки вооружений в космическом пространстве. Государствам следовало бы присоединиться к реализации данных мер.

Говоря о мерах *мягкого права*, следует также упомянуть стандарты Международной организации по стандартизации (ISO), охватывающие большинство отраслей экономики и разработанные, в том числе для закрепления стандартов космической деятельности. Эти нормы вырабатываются непосредственно представителями космической отрасли, и, несмотря на то что меры не носят юридически обязывающий характер, эти стандарты соблюдаются. Кроме этого, развитию системы *мягкого права* способствует деятельность Межагентского координационного комитета по космическому мусору (МККМ) — результат сотрудничества космических агентств разных стран, занимающийся, в частности, анализом возможностей по сбору и удалению с орбиты космического мусора, а также разработкой руководства в данной сфере. Для большей эффективности норм *мягкого права* необходимы дальнейшее развитие и кодификация подобных стандартов и руководств.

Наконец набор стандартов и практик, применяемых национальными космическими операторами и государственными структурами, с течением времени также может стать нормой *мягкого права* или даже *жесткого* законодательства, в случае, если он будет принят на международном уровне.

Комментарий эксперта

Особую озабоченность в контексте обеспечения безопасности космической деятельности вызывает стремление отдельных государств установить международно-правовые режимы использования космического пространства, которые призваны обеспечить доминирование в нем отдельных участников или их групп. Проекты подобных международно-правовых документов призваны закрепить концепцию международного регулирования космической деятельности на основе юридически необязательных соглашений — она очень удобна некоторым государствам. Примером может служить проект Международного кодекса поведения в космическом пространстве, продвигаемый нашими европейскими партнерами при поддержке американских коллег.

Участники космической деятельности, обладающие такими действенными инструментами «конструктивного диалога» с партнерами как весомые экономический и военный потенциалы, напрямую заявляют о своей незаинтересованности в установлении обязательных международно-правовых норм, которые могли бы хоть в малейшей степени ограничить их в выборе методов и средств для достижения собственных целей. «Мягкое право» позволяет нашим западным партнерам игнорировать «неудобные» положения таких документов в отношении себя самих, но в то же время осуждать других участников космической деятельности — даже тех, которые не брали на себя соответствующих обязательств.

Ярким примером может служить ситуация, последовавшая за представлением Россией инициативы о неразмещении первыми оружия в космосе (НПОК). Значительное число государств признает действенность подобных политических обязательств в целях продолжения мирного использования космоса и присоединилось к НПОК. Апологеты же «мягкого права» поставили под вопрос толкование фразы «не выводить первыми», сделав вид, что не понимают смысла данного обязательства, которое заключается в предоставлении государством гарантий не начинать гонку вооружений в космосе, с сохранением права на ответные действия, если другое государство переступит эту черту.

Мы не отрицаем действенность отдельных инструментов «мягкой права» в области международного регулирования космической деятельности. Более того, порой это единственно приемлемый на международном уровне инструмент купирования серьезных проблем в этой сфере — особенно там, где в настоящее время технологически невозможно обеспечить достоверное подтверждение исполнения участниками космической деятельности взятых на себя обязательств. Кроме того, в ряде случаев для большинства государств с учетом их различий в экономическом и технологическом развитии наиболее приемлемым вариантом решения конкретных проблем в области космической деятельности является не использование, а именно отказ от использования некоторых методов и средств ее ведения.

Сейчас некоторые активные участники освоения космического пространства стремятся внести изменения в свои национальные законодательства — изменения касаются возможности исследования, разработки и использования природных ресурсов небесных тел. Наличие в отдельных государствах законодательства, призванного урегулировать в одностороннем порядке пробелы, не решенные на уровне международного космического права, только затруднит задачи мирового сообщества по разработке общепризнанных норм и спровоцирует напряженность в отношениях между участниками космической деятельности.

Василий Гуднов, начальник отдела международного сотрудничества, государственная корпорация «Роскосмос»

СВОЯ ОРБИТА БЛИЖЕ К ТЕЛУ

Несмотря на то что обеспечение безопасности в космическом пространстве невозможно в отсутствие глобальных правил, национальное законодательство критически важно для непосредственной реализации норм международного права в космической деятельности конкретного государства.

Согласно Договору о космосе 1967 г., государства несут ответственность за обеспечение безопасности при осуществлении космической деятельности и за соблюдение положений договора. Ключевым инструментом государств в этом деле выступает процедура лицензирования субъектов космической деятельности. Кроме этого, Устав и Конвенция МСЭ требуют внесения положений о выделении орбит в национальное законодательство. Конвенция о регистрации объектов, запускаемых в космическое пространство, обязывает государства создать национальные регистры и передавать базовую информацию об орбитах своих космических аппаратов в ООН. Некоторые государства на добровольной основе включают рекомендации ООН в национальные регулирующие документы (например, Руководящие принципы по предупреждению образования космического мусора).

Нормативные аспекты, которые не удается согласовать на международном уровне, могут быть имплементированы в национальное законодательство. Таким образом, определение «космического объекта» может стать обязательным в рамках законодательства каждой отдельной страны. В случае следования такому пути регулирования космической деятельности критически важным станет обмен информацией о том, какие именно нормы действуют в разных юрисдикциях. В отсутствие взаимной информированности странам будет сложно договариваться на международных форумах.

ТЕРНИИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА

Несмотря на сложную и солидную структуру, международное законодательство, призванное обеспечить безопасность космической деятельности, страдает от значительного количества пробелов.

Так, отсутствует международный договор, который бы запрещал размещение в космическом пространстве обычных вооружений. Существует российско-китайский проект юридически обязывающего договора о предотвращении размещения оружия в космическом пространстве, применения силы или угрозы силы в отношении космических объектов (ДПРОК), однако он не поддерживается США — по мнению американской стороны, договор излишне фокусируется на оружии, размещенном в космосе. При этом 99% объектов, которые в настоящее время находятся в космическом пространстве, теоретически могут использоваться в военных целях.

Кроме того, возникает ряд вопросов юридического характера: у международного сообщества нет согласованного определения терминов «космический мусор» и даже «космос», не говоря уже о понятии «космического оружия».

Американская сторона также считает открытым вопрос о том, будет ли противоракетная оборона (ПРО) нарушать ДПРОК, учитывая, что траектории баллистических ракет и противоракет могут проходить через космическое пространство. С точки

зрения Вашингтона, при разработке подобного договора необходимо учитывать наличие систем противоракетной обороны у Китая, России и Израиля. Важно понимать, что США относятся к вопросу ПРО очень трепетно — для американской стороны это не столько научный вопрос, сколько практически теологический.

Кроме того, в международном праве отсутствуют механизмы регулирования добычи полезных ископаемых на небесных телах. Оно также не содержит требований об устранении государствами произведенного ими космического мусора, притом что накапливание мусора угрожает самой возможности использования околоземного космического пространства.

Также, несмотря на свою ключевую роль, МСЭ не обладает механизмами юридического принуждения, которые бы заставили государства строго придерживаться использования выделенных им орбит.

Следует отметить и то, что на международную ситуацию в целом влияет отсутствие доверия между ведущими космическими державами. Действия США расцениваются Китаем и Россией как угрожающие, деятельность Москвы вызывает подозрения со стороны Вашингтона и Пекина, а поведение Китая не нравится двум другим углам этого треугольника государств. В таких условиях сложно обсуждать заключение договоров о предотвращении гонки космических вооружений.

Помимо этого, на международных площадках проявляются определенные расхождения в подходах к регулированию космической деятельности, а также по вопросам соблюдения норм международного права между традиционными космическими державами и новыми акторами.

ЛИФТЫ КОСМИЧЕСКОЙ ДИПЛОМАТИИ

Тем не менее ошибочно считать, что текущая международная ситуация исключает возможность достижения договоренностей, направленных на обеспечение безопасности использования космического пространства.

Одним из направлений деятельности мог бы стать процесс по согласованию того, как право вооруженных конфликтов (требование избирательности, пропорциональности, отсутствия сопутствующего ущерба) могло бы применяться в космическом пространстве. Эти нормы могли бы послужить основой для будущих договоров.

Другим потенциально привлекательным направлением могло бы стать введение запрета на испытания или использование противоспутникового оружия, которое ведет к появлению космического мусора. При этом следует учитывать, что вопросы, связанные с ПРО, и попытки связать космическое право с правом вооруженных конфликтов могут затруднить достижение договоренности в этой области.

Выработка механизмов исполнения решений МСЭ в случае, когда использование участков орбиты признано незаконным, отвечает интересам всех космических держав. Необходимые изменения в Регламент радиосвязи могут быть внесены в ходе очередной Всемирной конференции радиосвязи.

Следующим важным аспектом деятельности является кодификация национальных или региональных рекомендаций по устранению космического мусора, а также

реализация на национальном, региональном и глобальном уровне мер транспарентности и доверия, выработанных ГПЭ в 2013 г., включая улучшенный механизм уведомления, консультации и обмен информацией о космических объектах.

В обозримом будущем вряд ли можно ожидать заключения нового соглашения по контролю над вооружениями в космосе — слишком сильно недоверие между ключевыми игроками, однако прорыв может быть возможен на отдельных направлениях. Практически всеобщая обеспокоенность проблемой накопления космического мусора может способствовать заключению соглашения о запрете создания нового мусора. Эта сфера деятельности может стать неким трамплином для продвижения вперед. Некоторые другие вопросы (противоспутниковое оружие, вмешательство в работу спутников и применение права вооруженных конфликтов) также можно рассматривать в качестве предметов регулирования будущих международных договоров. Там же, где мировое сообщество не сможет достичь компромисса, положения *мягкого права* могут получить юридическую силу путем их включения в национальное законодательство.

Наконец критически важно продолжать дипломатические усилия по поиску взаимовыгодных соглашений для обеспечения космической безопасности. Зачастую в сфере безопасности первую скрипку играют военные, но, если мы хотим и дальше использовать космическое пространство в мирных целях, дипломатия должна выйти на первый план.

Комментарий эксперта

В 2004 г. Россия выступила с инициативой политического обязательства о неразмещении первыми оружия в космосе (НПОК). Год спустя такое же политическое обязательство взяли на себя остальные члены ОДКБ: Армения, Белоруссия, Казахстан, Киргизия, Таджикистан.

В 2012 г. Россия активизировала усилия по расширению количества подписантов обязательства по НПОК. В результате в 2012–2016 гг. обязательство по НПОК приняли еще 8 государств: Бразилия, Индонезия, Шри-Ланка, Аргентина, Куба, Венесуэла, Боливия и Никарагуа. Таким образом, общее число полноформатных участников НПОК достигло 14. Работа на этом направлении продолжается.

С целью придания инициативе глобального характера в 2014 г. российская делегация выдвинула проект резолюции ГА ООН по НПОК. Документ призвал космически значимые государства присоединиться к обязательствам по НПОК. К 2015 г. к России в число соавторов резолюции вошло 40 государств, а общая ее поддержка возросла до 130 стран. В стороне от общего тренда остаются лишь голосующие против резолюции по НПОК США и Израиль, а также поддерживающие их по политическим соображениям Грузия и Украина.

Являясь политическим обязательством, эта инициатива носит промежуточный и временный характер. Надобность в ней, разумеется, отпадет, когда будет согласован и принят Договор по предотвращению размещения оружия в космосе (ДПРОК). Пока же НПОК остается, по сути, единственной практической мерой, реализуемой в развитие резолюции ГА ООН «Предотвращение гонки вооружений в космическом пространстве» (ПГВК).

Основная проблема в согласовании международных подходов к обеспечению мирного использования космоса состоит в том, что со стороны США и их ближайших союзников ведется кампания по дискредитации российских усилий по ПГВК. В силу политических антироссийских установок США оказывают значительное давление на все без исключения государства. Тем не менее Россия намерена продолжать последовательную дипломатическую работу со всеми государствами для продвижения наших инициатив в области ПГВК, ДПРОК, НПОК.

Владимир Ермаков,
заместитель директора Департамента по вопросам нераспространения и контроля над вооружениями МИД России

КИБЕРБЕЗОПАСНОСТЬ ГРАЖДАНСКИХ ЯДЕРНЫХ ОБЪЕКТОВ: ОЦЕНКА УГРОЗЫ И ПУТИ ЕЕ ПРЕОДОЛЕНИЯ[1]

Доклад подготовлен ПИР-Центром в сотрудничестве с женевским Centre russe d'etudes politiques в 2016 г. Проект реализован в рамках Рабочего процесса по кибербезопасности ядерных установок при Совете по глобальной повестке Всемирного экономического форума.

Вызовы в сфере кибербезопасности стали одной из ключевых проблем для операторов критической инфраструктуры (КИ) во всех отраслях. Кибератаки способны нарушать критически важные бизнес-процессы и операции на физическом уровне, выводить из строя оборудование и угрожать потерей доступа к услугам и инфраструктурным сервисам первой необходимости. Общемировые тенденции использования информационно-коммуникационных технологий (ИКТ) делают КИ всех секторов более уязвимой для кибератак, однако возможности киберзащиты гражданских ядерных объектов (ГЯО) стоит рассматривать отдельно в силу уникальных особенностей этой области.

В докладе «Кибербезопасность гражданских ядерных объектов: оценка угрозы и пути ее преодоления» рассматриваются особенности сектора ГЯО с точки зрения обеспечения кибербезопасности его КИ, национальные и международные подходы к регулированию КИ ГЯО, попытки выработать классификацию киберугроз для ядерной отрасли, а также приоритетные направления деятельности для обеспечения кибербезопасности ГЯО на данном этапе.

КЛЮЧЕВЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ ГРАЖДАНСКИХ ЯДЕРНЫХ ОБЪЕКТОВ

Общемировые тенденции в использовании ИКТ делают критическую инфраструктуру всех секторов (электроэнергия, транспорт, нефтегазовый сектор, авиация и т. д.) более уязвимой для кибератак. К таким тенденциям относится масштабный и все еще продолжающийся переход на автоматизированные системы управления технологическими процессами (АСУ ТП) на критически важных объектах (КВО), а также практика подключения офисных и даже промышленных корпоративных сетей объектов КИ к интернету. Эта практика получает более широкое распространение по мере внедрения технологий Интернета вещей и Всеобъемлющего Интернета. Доступ объектов КИ к Сети идет параллельно с мобильной революю-

цией, благодаря которой в различные секторы КИ приходят концепции «приноси свое устройство» (BYOD) и «карманная АСУ ТП». Наконец, для большинства секторов КИ общей проблемой стала исключительная сложность трансконтинентальных цепочек поставок систем управления ТП, программного обеспечения (ПО) для контроля таких систем (включая автоматизированные системы управления и сбора данных SCADA), а также устройств нижнего уровня.

Эти тенденции проявляются по всех областях, и ядерная энергетика здесь не исключение, но в силу присущих ему особенностей, сектор ГЯО является наиболее консервативным в части некоторых из них: использование *больших данных*, применения Интернета вещей в промышленных процессах, удаленного мобильного управления системами управления и сбора данных, а также проведения политики «приноси свое устройство» среди сотрудников.

Сектор ГЯО обладает уникальными характеристиками и требует особого подхода к обеспечению кибербезопасности объектов. С одной стороны, гражданские ядерные установки практически повсюду защищаются глубоко проработанными и всеобъемлющими системами норм и правил физической ядерной безопасности (ФЯБ), которые позволяют принципиально устранить некоторые вопросы, связанные с кибербезопасностью. С другой стороны, уникальность сектора ГЯО создает *проблемные точки* и барьеры для эффективного противодействия киберугрозам. К таким особенностям относятся, в частности:

1. Уникальная инфраструктурная сложность сектора ГЯО

Объекты сектора ГЯО разнообразны и включают, например, малые исследовательские реакторы на базе университетов. Но в большинстве случаев, в частности когда в анализ включаются АЭС, речь идет об исключительно сложных, масштабных и опасных объектах. Соответственно, для поддержки функционирования АЭС требуется исключительно сложная ИТ-система. К примеру, на АЭС последнего поколения современная ИТ-инфраструктура включает как минимум четыре контура, причем корпоративная офисная сеть представляет собой лишь один контур — верхний. Каждый силовой блок на АЭС оснащен несколькими десятками подсистем АСУ ТП, которые необходимо интегрировать между собой, а также обеспечить их безопасность и совместимость с корпоративным ПО, отвечающим за управление и сбор данных. Общее количество поставщиков программного и аппаратного обеспечения для одной АЭС сегодня может превышать три сотни. Более того, каждый силовой блок оснащен более чем 10 тыс. датчиков, сенсоров и детекторов, отсылающих данные оператору на системы мониторинга. В общей сложности ИТ-системы современной АЭС регистрируют до 200 тыс. изменений параметров в секунду.

Такая сложность порождает ряд последствий и проблем, которые требуют продуманного решения:

Во-первых, для ГЯО **не существует универсальных стандартных решений по интеграции ИТ-подсистем объекта**. Так, каждая АЭС с точки зрения своей ИТ-инфраструктуры, ее архитектуры и топологии является уникальным объектом, на котором реализованы оригинальные решения по ИТ-интеграции. Соответственно, в каждом случае сетям и ИТ-системам такого объекта присущ уникальный набор уязвимостей кибербезопасности и брешей в защите сетевого периме-

тра. Это серьезно ограничивает возможности и практический смысл применения операторами ГЯО накопленного опыта и лучших практик.

Во-вторых, **проблема доверия к ИТ-поставщикам и необходимость обеспечения целостности цепочек поставок ИТ-продукции, особенно для АСУ ТП**. Операторы не располагают возможностями провести доскональную проверку тысяч контроллеров, дистанционных терминалов, маршрутизаторов, программных комплексов по управлению производственными процессами и т. д. на скрытый функционал, вредоносное ПО или ошибки. Это серьезная проблема, поскольку, как уже говорилось выше, каждый оператор АЭС вынужден зависеть от многих десятков и даже сотен поставщиков, а многие из них — транснациональные компании.

В-третьих, сложность внутренней ИТ-инфраструктуры ГЯО и интенсивность потоков данных в этой инфраструктуре требуют **комплексного и всеобъемлющего подхода к кибербезопасности, который принципиально выходит за рамки только лишь реагирования на инциденты**.

Можно наметить несколько элементов такого перспективного подхода:

- обеспечение кибербезопасности на этапе проектирования — концепция, которая имеет много общего с ядерной безопасностью на этапе проектирования;
- обнаружение сетевых событий, реагирование на них, а также мониторинг сетевого трафика в режиме реального времени для всех контуров ИТ-инфраструктуры ГЯО, включая АСУ ТП;
- введение новых требований к поставщикам критически важных комплектующих АСУ ТП. Например, обязать поставщика раскрывать оператору ГЯО исходный код прошивки программных логических контроллеров после подписания контракта на поставку;
- внедрение решений по криптографической защите информации, а также цифровых подписей и защищенных меток времени на нижних уровнях сетевой инфраструктуры ГЯО (уровень АСУ ТП) для более надежной защиты целостности и конфиденциальности данных.

2. *Неопределенность места и роли кибербезопасности ГЯО в физической ядерной безопасности*

Область кибербезопасности ГЯО формируется на пересечении промышленной безопасности АСУ ТП, физической ядерной безопасности (ФЯБ) и информационной безопасности (ИБ).

Задача ИБ — обеспечение триады «конфиденциальность–целостность–доступность» в отношении информации, которая обрабатывается, хранится и передается в информационных системах объекта. Эта задача распространяется как на информацию из баз данных офисного сегмента сети ГЯО, так и на данные, которые получает ПО для сбора и управления технологическими процессами от устройств нижнего уровня.

ФЯБ является уникальной составляющей экосистемы безопасности ГЯО, отсутствующей в прочих секторах КИ. Согласно определению МАГАТЭ, обеспечение ФЯБ заключается в предотвращении, обнаружении и реагировании на хищение, саботаж (диверсию), несанкционированный доступ, незаконную передачу или

другие злоумышленные действия в отношении ядерных материалов и других радиоактивных веществ, а также связанных с ними установок и пунктов хранения ядерных материалов.

Изначально ФЯБ не имела ничего общего с киберпространством. Однако по мере появления новых векторов угроз операторы ГЯО, технические специалисты и регуляторы были вынуждены работать над включением вопросов кибербезопасности в парадигму ФЯБ. На сегодняшний день интеграция кибербезопасности ГЯО и ФЯБ не завершена, и в некоторых случаях такая незавершенность представляет вызовы для обеспечения кибербезопасности ГЯО в силу следующих обстоятельств:

- нечеткое разведение функций и распределение ресурсов между структурными подразделениями ГЯО, отвечающими за ИБ/кибербезопасность, и подразделениями, ответственными за ФЯБ;
- взаимно противоречащие требования, стандарты и процедуры для обеспечения кибербезопасности с одной стороны и ФЯБ с другой;
- ограничения, которые могут накладываться требованиями и нормативами ФЯБ на значимые технологические нововведения, необходимые для более надежного обеспечения ИБ объекта (например, внедрение средств криптографической защиты информации на сетях передачи данных между АСУ ТП);
- терминологические и концептуальные расхождения между представителями подразделений, ответственных за кибербезопасность и за ФЯБ (что может затруднять совместную работу над нейтрализацией вызовов и реагированием на инциденты).

РЕГУЛИРОВАНИЕ В ГРАЖДАНСКОЙ ЯДЕРНОЙ ОТРАСЛИ: НАЦИОНАЛЬНЫЕ ПОДХОДЫ И МЕЖДУНАРОДНЫЕ ФОРМАТЫ

В большинстве стран кибербезопасность ГЯО только начинает формироваться в качестве отдельной повестки дня для регуляторов национального уровня. Ключевая сложность состоит в нечетком распределении регуляторных задач между государственными органами, которое влечет за собой пробелы в выполнении или, наоборот, дублирование функций регуляторов. Во многих государствах, особенно в развивающихся (Индия, Украина, Бразилия, ЮАР), связанные с кибербезопасностью ГЯО регуляторные полномочия рассредоточены между несколькими государственными агентствами и министерствами, что зачастую ведет к недостатку коммуникации между ними и отсутствию отлаженного механизма решения вопросов, которые попадают в сферу компетенций сразу нескольких регуляторов.

Следующей проблемой является отсутствие единого регулятора, который отвечал бы за весь комплекс вопросов, связанных с безопасностью ГЯО, а это часто ведет к слабой обратной связи от других участников: операторов ГЯО, их ИТ- и ИБ-поставщиков и подрядчиков. Более широко эта тенденция выражается в недостаточной обратной связи от частного сектора и экспертного сообщества, поскольку в некоторых случаях их представители не могут определить, какому регулятору следует адресовать те или иные вопросы.

Недостаточная гибкость подходов, на которые опираются национальные регуляторы, также может затормаживать развитие политики кибербезопасности ГЯО,

в том числе когда в основе таких подходов лежит развитая система норм и технических руководств по ФЯБ или законодательство в сфере защиты информации и кибербезопасности. Преемственность уже сформированного подхода иногда выступает барьером для выработки гибридного регулирования, которое бы охватывало специфические вопросы сектора ГЯО.

Наконец, имеет место недостаточно активная интеграция международных руководств, рекомендаций и лучших практик в национальные нормы и требования, которые во многих случаях ограничиваются сугубо техническими вопросами. Прежде всего это относится к рекомендациям и техническим руководствам МАГАТЭ, а также к документам и рекомендациям, выработанным в рамках других международных площадок и рабочих процессов (например, Всемирного института ядерной безопасности и Саммита по ядерной безопасности). Такая тенденция отмечается даже в государствах с развитой регуляторной политикой как в секторе ядерной энергетики, так и в сфере кибербезопасности (Россия, США, Франция).

Кибербезопасность ГЯО в национальном праве

Тем не менее с начала 2010-х гг. во многих юрисдикциях наблюдается постепенный прогресс. Один из заслуживающих упоминания индикаторов — заметно ускорившийся во многих государствах за последние пять лет процесс выработки и принятия отраслевого законодательства и обязательных требований по кибербезопасности ГЯО. В числе стран, которые с 2012 г. приняли или начали разрабатывать законодательство или подробные требования к кибербезопасности сектора ГЯО, — Австралия, Бельгия, Канада, Чехия, Франция, Венгрия, Нидерланды, Норвегия и Южная Корея. В 2016–2017 гг. этот список должен пополниться еще рядом государств, и многие из них ориентируются на рекомендации и технические руководства МАГАТЭ.

Кроме того, даже в тех государствах, где отсутствуют единый профильный регулятор для сектора ГЯО и соответствующее национальное законодательство, отмечается повышение активности регуляторов, сконцентрированной на ГЯО. В процесс выработки регулирующих норм все больше вовлекаются операторы таких объектов. Один из примеров — Россия, где в 2014 г. концерн *Росэнергоатом* начал активно адаптировать требования, содержащиеся в приказах о защите информации, принятые ранее Федеральной службой технического и экспортного контроля (ФСТЭК), для обеспечения ИБ при эксплуатации АЭС. Государства с развитой системой регуляторных норм для секторов ядерной энергетики и кибербезопасности активно переходят от регулирования отдельных вопросов ИБ ГЯО (защита информации в корпоративных сетях ядерных объектов, физическая изоляция таких сетей, лицензирование ИТ-поставщиков, обслуживающих ГЯО, и т. д.) к комплексным системам требований, которые бы обеспечивали гибридное регулирование вопросов на пересечении ФЯБ и кибербезопасности. Отдельного упоминания заслуживают США, где в 2010 г. были опубликованы всеобъемлющие и обязательные для всех операторов ГЯО требования Комиссии по ядерному регулированию NRC RG 5.71 *Программы кибербезопасности для ядерных установок*.

Наконец, прослеживается растущий интерес госорганов к участию в международных дискуссиях и разработке инициатив в сфере обеспечения кибербезопасности ГЯО. В июне 2015 г. 92 правительственные делегации приняли участие в первой

Международной конференции по компьютерной безопасности в ядерном мире, проведенной в штаб-квартире МАГАТЭ в Вене. Стоит отметить, что число участников конференции превысило число государств, имеющих гражданскую ядерную отрасль промышленности. Ряд инициатив и предложений, выдвинутых отдельными государствами, получили международную поддержку. Наконец, национальные научные и экспертные сообщества также демонстрируют растущий уровень активности в сфере кибербезопасности ГЯО.

Состояние международного сотрудничества в обеспечении кибербезопасности ГЯО

На международном уровне повестка дня в сфере обеспечения кибербезопасности ГЯО и противодействия актуальным киберугрозам развивается в условиях нормативного вакуума и отсутствия механизмов совместного управления инцидентами и их расследования. С одной стороны, такая ситуация типична для традиционных задач ФЯБ, когда угрозы локализованы, а необходимость обеспечивать безопасность и конфиденциальность превалирует над потребностью в тесном взаимодействии. Однако такой подход недостаточно эффективен, когда речь идет об обеспечении кибербезопасности ГЯО, поскольку зачастую киберугрозы имеют трансграничный характер. Даже если исходить из того, что какое-то конкретное государство способно обеспечить полную защиту своих мирных ядерных объектов от сетевых компьютерных атак, оно тем не менее останется зависимым от международных поставщиков и цепочек поставок ИТ-продуктов и сервисов, используемых на таких объектах. К примеру, в топ-3 поставщиков автоматизированных систем управления и сбора данных (SCADA) входят две компании из США и одна из Германии: Schneider Electric, Siemens и Rockwell Automation. Для большинства из сотен систем программного и аппаратного обеспечения, используемых на любом ГЯО, наиболее популярные решения поставляются крупными транснациональными компаниями. Полная локализация разработки и поставки ИТ-систем ГЯО невозможна. Поэтому операторам приходится мириться с тем, что в используемом им программном и аппаратном обеспечении могут присутствовать недоработки, дефекты и уязвимости, способные открыть дверь для кибератак. Тем не менее, несмотря на убедительные доводы в пользу необходимости международного сотрудничества в области кибербезопасности, в настоящее время уровень взаимодействия по ГЯО отстает от уровня взаимодействия по *традиционным* вопросам ядерной безопасности и противодействию *аналоговым* угрозам.

В частности, кибератаки против ГЯО не подпадают под действие существующих международных механизмов противодействия киберпреступлениям и их расследования. Наиболее известным механизмом такого рода является Будапештская конвенция о борьбе с компьютерными преступлениями, принятая Советом Европы в 2001 г. и открытая для подписания всеми странами. Схожая ситуация имеет место в отношении региональных соглашений в сфере кибербезопасности, например, межправительственного соглашения государств Шанхайской организации сотрудничества (ШОС) о сотрудничестве в области обеспечения международной информационной безопасности от 2009 г., а также двусторонних соглашений (российско-американская серия соглашений 2013 г., российско-китайское двустороннее соглашение 2015 г. и пр.).

Киберинциденты на ГЯО также не подпадают под действие необязывающих юридически трансграничных механизмов сотрудничества, таких как альянс Международного союза электросвязи (МСЭ) и международного государственно-частного партнерства ИМПАКТ или FIRST (международный Форум по взаимодействию между центрами реагирования на инциденты кибербезопасности). Более того, не выработана международная система стандартизации в отношении специфических ИТ-продуктов и сервисов, которые поставляются операторам ГЯО. Такая система могла бы включать набор требований по защите цепочек поставок особо важных ИТ-компонентов (программные и аппаратные комплектующие АСУ ТП АЭС), а также стандарты, описывающие надежную изоляцию промышленных сегментов сетей ГЯО от интернета, и т. д. Наконец, отсутствуют общие критерии и стандарты аудита кибербезопасности на ГЯО.

Кроме того, международные нормы и договоры по вопросам кибербезопасности ГЯО до сих пор отсутствуют. Существующие международные соглашения по ядерной безопасности и ядерному нераспространению были приняты раньше, чем на повестку дня вышли вопросы защиты объектов мирного атома от киберугроз. Обновление ранее принятых соглашений с учетом этой новой проблемы потребует долгосрочных усилий без гарантированного результата. Кроме того, отсутствие режима международного регулирования киберпространства в целом сказывается и на возможностях обеспечения кибербезопасности в секторе ГЯО.

Вместе с тем за последние годы был разработан ряд проектов соглашений и норм ответственного поведения в киберпространстве. В том числе такие проекты норм и правил поведения продвигала на международных площадках Россия — самостоятельно и вместе со своими партнерами по ШОС в 2011 и 2015 гг. Однако соблюдение предлагаемых норм может быть затруднено, поскольку позитивные и негативные механизмы для этого отсутствуют. Такое препятствие будет неизбежно возникать, пока не будут выработаны эффективные решения проблем атрибуции в киберпространстве и верификации предлагаемых мер. То же относится и к идеям о создании специального договора, который бы запрещал атаки на ГЯО и установки, содержащие опасные силы (включая АЭС), в соответствии с определениями статьи 56 Дополнительного протокола I к Женевским конвенциям 1949 г.

Тем не менее можно констатировать определенный прогресс и наличие открытого окна возможностей для выработки норм в связи с деятельностью Группы правительственных экспертов ООН (ГПЭ ООН) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. В июне 2015 г. четвертый созыв Группы завершил подготовку доклада Генерального секретаря ООН, в котором государствам — членам ООН был предложен список необязывающих добровольных норм, закладывающих основу для ответственного поведения в киберпространстве. Из числа этих норм как минимум две: запрет кибератак на КВО и обеспечение целостности цепочек поставок критически важной ИТ-продукции, — можно и нужно применить для обеспечения кибербезопасности сектора ГЯО.

Хотя эти нормы и не являются обязательными, если они будут приняты и поддержаны широким кругом государств, они могут стать основой для последующих, более конкретных и юридически обязательных международно-правовых документов. Кроме того, такие наработки ГПЭ ООН могут послужить механизмом укрепле-

ния международного взаимодействия с участием частного сектора, нацеленного на обеспечение целостности цепочек поставок ИТ-систем ГЯО, а также на решение других актуальных проблем.

Роль МАГАТЭ

Основополагающую роль в проработке вопросов кибербезопасности ГЯО до сих пор сохраняет за собой МАГАТЭ. Агентство начало поднимать эту тему на своих Генеральных конференциях с 2012 г., но поворот к систематической работе по обеспечению кибербезопасности ядерных установок произошел в 2013 г. Именно тогда была запущена Программа компьютерной и информационной безопасности при Управлении ядерной безопасности агентства. Цель программы — обеспечить государства — члены МАГАТЭ необходимыми рекомендациями, для того чтобы поддержать их деятельность по реагированию на трансграничные кибератаки, которые так или иначе затрагивают ядерные и другие радиоактивные материалы, а также связанные с ними объекты и виды деятельности. Программа включает шесть направлений деятельности МАГАТЭ в этой области, в том числе разработку технических руководств, организацию и поддержку форумов по обмену технической информацией, региональные тренинговые мероприятия, региональную и международную экспертную поддержку, предметную экспертизу по реагированию на инциденты, а также деятельность по повышению информационного охвата.

В настоящее время МАГАТЭ в своих рекомендациях по ядерной безопасности рассматривает кибербезопасность как фактор, способный повлиять на обеспечение должного уровня ФЯБ и, таким образом, подлежащий проработке и учету в контексте ФЯБ. Кроме того, в рекомендациях агентства, отмечается необходимость защиты от взлома компьютеризованных систем обеспечения ядерной безопасности (в том числе систем физической защиты и систем учета и контроля ядерных материалов).

Значимой инициативой, запущенной агентством в 2015 г., стала Международная конференция по компьютерной безопасности в ядерном мире, привлекшая широкий международный круг участников. В пятидневной конференции приняли участие представители 92 государств и 14 международных организаций. В общей сложности было представлено 172 доклада, в том числе доклады, содержащие проработанные сценарии возможных инцидентов на объектах ГЯО. Среди таких сценариев рассматривался и ход многоэтапных кибератак на АЭС. Конференция может стать важным каналом для повышения осведомленности о вызовах кибербезопасности ГЯО среди развивающихся стран, а также площадкой для обмена лучшими практиками. Несмотря на то что технические руководства и рекомендации МАГАТЭ по обеспечению компьютерной безопасности ядерных установок не являются обязательными для выполнения, они оказываются все более актуальными для тех стран, которые находятся на начальных этапах разработки собственной регуляторной базы в этой области. Также в отсутствие норм и трансграничных механизмов сотрудничества по предотвращению, расследованию и подготовке отчетности по киберинцидентам на ГЯО усилия МАГАТЭ по повышению осведомленности и наращиванию потенциала реагирования имеют особую ценность. Однако для более эффективной борьбы с киберугрозой агентству, возможно, имело бы смысл подтолкнуть государства-члены и международное сообщество

к диалогу по поводу формирования более практико-ориентированных механизмов и форматов трансграничного сотрудничества в данной сфере.

КИБЕРУГРОЗЫ ГЯО: БАЗОВАЯ МОДЕЛЬ КЛАССИФИКАЦИИ И ПРИМЕРЫ ИНЦИДЕНТОВ

На сегодняшний день не выработана универсальная классификация кибернетических воздействий на ядерные установки, равно как и на другие КВО.

Предлагаемая МАГАТЭ трехкомпонентная классификация позволяет выделить основные виды компьютерных инцидентов в зависимости от их последствий. Однако классификация агентства не позволяет установить источник и характер угрозы, а также определить базовые технические параметры для описания инцидентов. К таким параметрам относятся, в частности, затронутые атакой системы, возможные векторы угрозы, сценарии кибератаки и т. д. Существуют и более подробные классификации, описывающие виды инцидентов кибербезопасности на объектах КИ по признаку элементов информационных систем, которые могут выступать целью атаки. Одна из подобных широких классификаций для неядерных объектов КИ энергетической отрасли была разработана ОБСЕ в 2014 г.

За некоторыми оговорками, такой подход также применим к сектору ГЯО, поскольку информационные системы ядерных и неядерных объектов КИ по основным параметрам схожи. Подобную классификацию может использовать ИТ-департамент ГЯО в качестве полезного теоретического примера. Однако для принятия решений оператору ГЯО и структурному подразделению, отвечающему за обеспечение кибербезопасности на таком объекте, скорее необходима многомерная *ось координат*, позволяющая классифицировать инцидент по различным критериям. В частности оператору потребуется установить, чем вызван инцидент: действием человеческого фактора или технологическим сбоем; является нарушитель внутренним или внешним по отношению к системе; какова цель атакующего; какие системы могут быть затронуты инцидентом и т. д. Отсутствие такой *оси координат* — пробел, который следует закрыть совместными усилиями ИТ-отрасли, операторов и регуляторов. В качестве первого шага в этом направлении может быть предложена базовая модель классификации, позволяющая выстроить типологию инцидентов на ГЯО.

Надежная статистика инцидентов для сектора ГЯО не ведется, поскольку практика открытой отчетности об инцидентах отсутствует в силу соображений национальной безопасности и репутационных рисков для бизнеса. На основе открытых данных можно найти информацию как минимум о 14 серьезных инцидентах кибербезопасности на ГЯО за последние 25 лет. Тринадцать из них — инциденты на АЭС, а еще один инцидент связан с кампанией *Олимпийские игры*, которая велась против мирной ядерной инфраструктуры Ирана с использованием вирусов Stuxnet, DuQu, Flame и другого профессионального вредоносного ПО. Для того чтобы заложить базу дальнейшего исследования и сформулировать выводы на основе конкретных прецедентов, были изучены четыре инцидента. В частности были проанализированы инцидент на АЭС Дэвис-Бессе (США), кибероперация *Олимпийские игры*, кибератака на корпоративную сеть штаб-квартиры оператора южнокорейских АЭС KHNP и заражение сети АЭС Гундреммингen (Германия) в апреле 2016 г. Акцент был сделан на инцидентах, вызванных злоумышленными действиями, включая применение вредоносного ПО или других средств целенаправленного кибернетического воз-

действия. Хотя большинство из этих инцидентов хорошо известны, дополнительную ценность может иметь их анализ с точки зрения базовой модели классификации и описанной выше концепции комплексной среды кибербезопасности. Вместе с тем инциденты в корпоративной сети KHNP и в сети АЭС Гундремминген произошли относительно недавно, а их исследование может способствовать лучшему пониманию логики целенаправленных кибератак на ГЯО, что стало востребованной темой после кампании *Олимпийские игры*. При обобщении результатов проведенного анализа конкретных инцидентов в первую очередь нужно отметить, что было сформировано новое понимание ландшафта киберугроз в рассматриваемой области. Дальнейший углубленный анализ позволит развить и конкретизировать существующий ландшафт. Однако уже на этой стадии исследовательской работы несколько базовых тенденций выглядят неоспоримыми. Они требуют согласованной реакции от всех заинтересованных сторон, включая операторов ГЯО, ИТ-поставщиков, национальных регуляторов и международные площадки.

Во-первых, в отличие от 1990-х и 2000-х гг., сегодня в отношении ГЯО преимущественно используются киберугрозы повышенной опасности. Предположительно, они могут исходить от государственных игроков. Эти угрозы сочетают в себе средства кибершпионажа и киберсаботажа. При этом такие кибератаки тщательно спланированы: они нацелены на поражение критических систем и затрагивают сотрудников ядерных объектов. Наиболее серьезный вызов кибербезопасности ГЯО исходит от инцидентов, вызванных целенаправленным внешним человеческим вмешательством. Сегодня отсутствуют средства, которые позволяли бы комплексно и эффективно бороться с постоянными угрозами повышенной опасности, особенно в международном масштабе. Основными причинами этого являются неразрешенная проблема атрибуции и отсутствие международных норм и форматов для решения подобных вопросов.

Во-вторых, выявления и расследования инцидента может быть недостаточно для окончательного устранения угрозы. В случае с киберугрозами повышенной опасности, нацеленными конкретно на ГЯО, вредоносное ПО не является *одноразовым оружием*, как его зачастую описывают. Для атак используются комплексные пакеты ПО (тулкиты) и компьютерные черви с множеством модулей, которые легко подвергаются модификации и в каждой своей обновленной версии представляют новую угрозу кибербезопасности КВО.

Более того, как показывают примеры кампании *Олимпийские игры* и атаки на KHNP, однажды внедренное на объект вредоносное ПО начинает жить собственной жизнью независимо от планов своих создателей. Так, оно может превратиться во вредоносный проект с открытым исходным кодом, который доступен для модификации всем игрокам, обладающим необходимыми ресурсами и навыками. Ярким примером этого служит инцидент со Stuxnet. Спустя несколько лет после него производные версии ПО, использованного во время кампании *Олимпийские игры*, нарушили функционирование внутренней сети промышленного комплекса нефтедобывающей компании Saudi Aramco и заразили ряд КИ по всему миру, включая АЭС в России (хотя ущерба заражение не повлекло).

В-третьих, векторы угроз в рассмотренных примерах инцидентов на ГЯО смещаются в сторону от того спектра, который уже стал привычным в рамках концепции ядерной безопасности. Обеспечение безопасности внутреннего периметра

сетей ГЯО теперь идет рука об руку с интернет-безопасностью. Например, так было в случае кибератаки, когда целью номер один для ее авторов стали бывшие сотрудники южнокорейской АЭС. Борьба с кибершпионажем в отношении ГЯО также осложняется необходимостью разработки стратегии противодействия злоумышленникам в медиапространстве. Наконец, следует отметить, что угрозы не приходят поодиночке: кибершпионаж идет в связке с традиционным шпионажем и киберсаботажем. Сектор гражданской ядерной инфраструктуры теперь развивается в условиях постоянного наличия комплексных угроз, хотя они и пришли в сектор ГЯО позже, чем в другие сектора КИ. Кибератаки из краткосрочных спонтанных акций превратились в тщательно продуманные кампании — отныне их жизненный цикл может длиться годами. Соответственно, для эффективной борьбы с такими атаками требуется поддержание среды кибербезопасности с аналогичным по длительности жизненным циклом. Это вновь подчеркивает необходимость создания проактивной комплексной стратегии обеспечения кибербезопасности в режиме реального времени, которая должна прийти на смену подходу, основанному лишь на реагировании на уже случившиеся инциденты.

ПРЕОДОЛЕНИЕ УГРОЗЫ — ПЕРВЫЕ ШАГИ

Технический уровень

На техническом уровне необходимо внедрить новые подходы к обеспечению кибербезопасности ГЯО, прежде всего обеспечить взаимодействие операторов таких объектов с ИТ-вендорами. Необходимо свести к минимуму потенциальные риски скрытого функционала в критически важных ИТ-компонентах (АСУ ТП) за счет более интенсивного и обеспеченного ресурсами тестирования на проникновение (пентеста), анализа предельных значений (фаззинга) и глубокого сканирования прошивок программно-конфигурируемых устройств нижнего уровня.

Существенным шагом вперед мог бы стать консенсус о введении обязательства со стороны поставщиков раскрывать исходный код критически важных компонентов АСУ ТП при заключении контракта с оператором ГЯО. Сама отрасль АСУ ТП к такому требованию отнесется без энтузиазма — скорее, речь может идти о достижении компромисса по итогам длительного торга между отраслью и операторами ГЯО. Продуманное вмешательство со стороны регулятора могло бы дать поставщикам АСУ ТП стимул делиться с операторами исходными кодами своей продукции, не вынуждая их уходить с рынков отдельных государств, где могут быть введены такие требования.

Значимой составляющей нового подхода может стать и концепция обеспечения кибербезопасности на этапе проектирования объектов, особенно применительно к АЭС и другим крупным объектам гражданской ядерной инфраструктуры. Хотя принципы этой концепции известны и имеют общую основу с физической ядерной безопасностью на этапе проектирования, ее внедрение и подробное техническое видение пока по большей части находится в стадии разработки. Более тесный обмен опытом и лучшими практиками между ведущими ИТ-поставщиками и операторами ГЯО может помочь продвинуться вперед в решении этой задачи.

Наконец, необходимость защиты от внешних вторжений в АСУ ТП возвращает дискуссию к необходимости обеспечения не только доступности, но и конфиденци-

альности информации в критически важных ИТ-системах ГЯО. Для отрасли может оказаться целесообразным внедрение современных средств шифрования данных для обеспечения безопасности потоков межмашинных (M2M) данных между АСУ ТП. Как и в случае с раскрытием исходного кода прошивок ключевых продуктов, такой шаг будет непростым, поскольку внедрение криптографии создаст дополнительные издержки для операторов ГЯО. Однако, как показывают примеры недавних инцидентов, такие издержки могут оказаться меньшим из двух зол.

Уровень национальных регуляторов

На национальном уровне приоритетной целью является полная интеграция кибербезопасности ГЯО в концепцию ФЯБ, что позволит устранить функциональные бреши и дублирование функций между регуляторами, отвечающими за кибербезопасность и ядерную безопасность. Такая интеграция также необходима для разработки целостной стратегии обеспечения кибербезопасности на этапе проектирования объектов. Сегодня внимание этой задаче в основном уделяет МАГАТЭ, однако данная тема должна в первую очередь обсуждаться на национальном уровне в рамках диалога между регуляторами и получать должное внимание со стороны государственных органов.

Предпосылкой для успеха такого диалога может стать разработка комплексного законодательства, рассматривающего кибербезопасность ГЯО в качестве отдельного предмета. Развивающимся странам такое законодательство необходимо для того, чтобы определить ключевые приоритеты для государства и заполнить нормативный вакуум, который препятствует разработке операторами ГЯО собственных внутренних стандартов и технических руководств. МАГАТЭ и другие международные площадки сохраняют за собой определяющую роль при содействии такой работе на национальном уровне, поскольку именно они накапливают лучшие практики передовых стран и могут консультировать развивающиеся страны на предмет лучших образцов и моделей подходов.

Сближение парадигм кибербезопасности и ФЯБ также требует проведения масштабной работы над человеческим капиталом. Перед госорганами и операторами ГЯО стоит задача вырастить поколение специалистов с новым профессиональным видением, отличным от традиционного подхода к обеспечению ФЯБ, но при этом способным дополнить и обогатить его. На уровне внутригосударственной политики этому могут способствовать инновации в системе высшего образования и поддержка тренингов, семинаров и диалоговых форматов с участием представителей как сектора ядерной энергетики, так и ИТ-отрасли. Деятельность *мозговых центров* и неправительственных организаций по организации тренингов и повышению осведомленности об этих вопросах также должна получить поддержку. На международном уровне незаменимую роль играют тренинги, практические семинары и мероприятия по повышению осведомленности, организуемые МАГАТЭ.

Международный уровень

На уровне выработки международных норм и политик быстрого прогресса ждать не приходится. Юридически обязывающие межправительственные соглашения о борьбе с киберугрозами на объектах КИ еще долго могут не приниматься. В то же

время дебаты по вопросам адаптации существующих норм международного права к вызовам, исходящим из киберпространства, могут затянуться на десятилетия, но в итоге так и не привести к появлению применимых на практике механизмов сотрудничества. Действие существующих трансграничных механизмов противодействия киберпреступности практически не распространяется на сектор ГЯО из-за ограничений, связанных с национальной безопасностью. Тем не менее диалог в рамках всех перечисленных площадок и форматов целесообразен — имеет смысл вести его и далее, даже если он не принесет плоды в ближайшей перспективе.

Кроме того, некоторые возможности видятся в деятельности формата ГПЭ ООН. В августе 2016 г. стартовали встречи пятого созыва Группы, что дает шанс на достижение договоренностей и выработку добровольных норм ответственного поведения в конкретных секторах КИ. Решение о том, для каких секторов КИ в первую очередь следует разработать нормы, пока не принято, и в этом кроется возможность вынести вопросы обеспечения кибербезопасности ГЯО на самый верх повестки дня Группы. При таком развитии событий в следующий доклад, который готовит ГПЭ, могла бы войти добровольная норма, запрещающая государствам участвовать в кибератаках на ГЯО или предлагающая некий механизм добровольных самоограничений в части таких действий. Даже не имея юридически обязательной силы, такая норма помогла бы продвинуть дискуссию о кибербезопасности и приблизить появление будущего обязывающего межправительственного соглашения. Кроме того, работа ГПЭ может стать определяющей для разрешения вопросов формирования понятийного аппарата и классификации секторов КИ, а также классификации кибератак против объектов в этих секторах, включая ГЯО. Такая работа стала бы вкладом в достижение более широкой цели по разработке общего языка и общего видения для обсуждения вопроса кибербезопасности ГЯО на международном уровне. Наконец, некоторые более ранние предложения ГПЭ могли бы быть доработаны конкретно под сектор ГЯО. Примером может служить норма об обеспечении целостности цепочек поставок для критически важных ИТ-систем.

Помимо ГПЭ ООН, международные государственно-частные партнерства, такие как альянс ИМПАКТ-МСЭ, могут сыграть важную роль в обеспечении обмена данными о киберинцидентах на объектах ГЯО, накоплении лучших практик и создании баз данных уязвимостей, вредоносного ПО и скрытого функционала, используемых для кибератак на объекты ГЯО.

Список сокращений

BYOD — Bring your own device — «приноси свое устройство»

SCADA — Supervisory Control and Data Acquisition — автоматизированная система управления и сбора данных (конкретный вид АСУ ТП)

АСУ ТП — автоматизированные системы управления технологическими процессами

АЭС — атомная электростанция

ГПЭ ООН — Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

ГЯО — объект гражданской ядерной инфраструктуры

ИБ — информационная безопасность

ИТ — информационные технологии

КВО — критически важный объект

КИ — критическая инфраструктура

МАГАТЭ — Международное агентство по атомной энергии

ИМПАКТ-МСЭ — Альянс «Международное многостороннее партнерство по борьбе с киберугрозами — Международный союз электросвязи»

ОБСЕ — Организация по безопасности и сотрудничеству в Европе

ПО — программное обеспечение

ТП — технологические процессы

ФСТЭК — Федеральная служба технического и экспортного контроля

ФЯБ — физическая ядерная безопасность

ШОС — Шанхайская организация сотрудничества

КИБЕРБЕЗОПАСНОСТЬ АСУ ТП – КОММЕНТАРИИ ЭКСПЕРТОВ

Формирование рынка кибербезопасности АСУ ТП[2]

Процесс становления рынка защиты автоматизированных систем управления технологическими процессами (АСУ ТП) принципиально отличается от схожих процессов на сформированных ранее в России рынках, например, антивирусного рынка или рынка защиты от утечек. Это объясняется рядом предпосылок.

Во-первых, на рынке АСУ ТП существует большое количество конкурирующих поставщиков оборудования и различных технологических решений — рынок сильно зависит от оборудования (hardware). Это базовое отличие от рынка антивирусов, которые, как и вирусы, по большому счету создаются под пару основных операционных систем. Во-вторых, создание универсального программного обеспечения (software) для такого огромного количества систем представляется затруднительным. В-третьих, производители ведут себя закрыто — не стремятся делиться созданными протоколами. Наконец, подавляющее большинство систем, которые предлагаются на российском рынке, импортные. Нужно учитывать, что сотрудничество с иностранными производителями осложняется, потому что зачастую они представлены крупными корпорациями со сложной структурой принятия решений, к которым непросто обратиться с предложением, например, улучшить софт под решение конкретной проблемы конкретного предприятия.

Рынок АСУ ТП, формирующийся сейчас в России, имеет смысл рассматривать с позиций четырех групп. Первую группу представляют клиенты — крупные компании. Складывается интересная ситуация: с одной стороны, компании озабочены информационной безопасностью, собирают по этому поводу внутренние совещания. С другой — как только

речь заходит о внедрении конкретной системы или о проведении проверки, клиенты начинают приуменьшать риски, говоря, что у них все защищено. Позиция директоров по безопасности крупных компаний заключается в том, что вероятность внедрения злоумышленников в систему мала и несущественна, а потому на нее не стоит обращать внимания, то есть налицо массовое непризнание проблемы со стороны клиентов.

Вторая группа состоит из производителей средств АСУ ТП. Производители также не стремятся обсуждать существование проблемы и придавать значение уязвимостям в системах. Порой можно встретить следующее: представители компаний-производителей, рассказывая о том, что последствия от проникновения вируса в систему клиента были устранены за пять дней, позиционируют такой случай как успешный.

Третья группа представлена регуляторами. Первым ведомством в этом списке стоит поставить Федеральную службу по техническому и экспортному контролю (ФСТЭК) — в марте 2014 г. именно эта служба выпустила регулирующий документ как раз по защите критической инфраструктуры. Документ был подготовлен буквально за полгода, что говорит о действительном осознании проблемы. Однако, кроме регулирующих документов ФСТЭК, существуют еще отраслевые регламенты безопасности, а также международные регламенты безопасности — все они, строго говоря, противоречат друг другу. Различия этих регламентов касаются даже количества уровней безопасности, которые они выделяют — от четырех до семи.

Наконец, четвертая группа заинтересованных лиц на рынке состоит из компаний, которые занимаются разработкой средств информационной безопасности — систем, которые защищают от вирусов, от утечек, строят системы контроля доступа и т.д. Именно эти игроки заметили проблему, и именно они привлекают к ней внимание, потому что другие группы в этом менее заинтересованы.

Таким образом, получается, что единого взгляда на проблему у четырех заинтересованных групп нет, а это приводит к тому, что рынок развивается скачкообразно и довольно медленно.

В настоящее время заметно, что клиенты боятся ставить серьезные системы в разрыв, например, на атомной станции или на крупном транспортном узле. Существующие системы, в основном системы мониторинга, которые помогают лишь обнаружить проблему, но не решить ее. Именно поэтому сейчас рынок АСУ ТП в основном пытается проводить аудит безопасности и на основании этого предлагать решения, которые создаются, по сути, под каждого отдельного крупного клиента. Это объяснимо, потому что система, разработанная, скажем, под РЖД, будет отличаться от системы, созданной для защиты АЭС.

В силу закрытости рынка сложно определить, какие отрасли действительно являются наиболее уязвимыми, а какие — наименее. В целом же представляется, что те предприятия, которые стремятся внедрять у себя промышленный Интернет вещей, сейчас находятся в более уязвимом положении, чем те, которые подходят к этому вопросу консервативно. На мой взгляд, выгоды от более развитого уровня автоматизации промышленных систем меркнут перед возможными катастрофическими последствиями, если в эту систему через интернет проникнет вирус.

Наталья Касперская,
директор InfoWatch

Цифровые угрозы в физическом мире — дешевые и трансграничные[3]

В течение долгого времени физический и цифровой миры не пересекались — так было до появления систем АСУ ТП. Эти цифровые компьютерные системы непосредственно влияют на нашу жизнь, поскольку каждый завод сегодня управляется при помощи компьютерных систем, а также транспорт, электростанции и т. д.

Как мы знаем из опыта, компьютерные системы содержат уязвимости, они подвержены атакам. Таким образом, ситуация, когда два мира соприкасаются, приводит к переносу цифровых угроз в физическую реальность. Сегодня уже известны случаи, когда компьютерные инциденты приводили к нежелательным последствиям в физическом мире. Например, в декабре 2015 г. в шести областях Украины вследствие хакерской атаки произошло отключение электроэнергии — от сети были отключены 225 тыс. пользователей. В том же месяце на сталелитейном предприятии в Германии произошел киберинцидент, в результате которого была выведена из строя доменная печь.

Однако проблема переноса цифровых угроз в физический мир касается не только вмешательства в технологические процессы. Одна из тенденций последнего времени — распространение Интернета вещей. Под этим понятием подразумеваются те же самые устройства, но управляемые высокими технологиями. При этом воздействовать на подобные «умные вещи» можно удаленно, без физического контакта с ними. Также стоит помнить, что цифровые технологии характеризуются очень низкой стоимостью воспроизведения. Если высококвалифицированные исследователи нашли уязвимость и смогли использовать ее, повторение этого вслед за ними не требует высокой квалификации.

Компьютерные технологии трансграничны. Какие бы средства ни были разработаны для защиты от тех или иных компьютерных инцидентов и проблем, они должны согласованно применяться в разных странах мира. Сейчас уже сложилась хорошая практика международного сотрудничества в области расследования инцидентов на базе Интерпола и Европола, но этого недостаточно. В настоящее время отсутствуют соглашения между государствами даже об использовании интернета — практически отсутствует правовое регулирование интернета. Для регулирования отношений в этой новой для человечества области необходимо сотрудничество между государствами.

Андрей Духвалов,
руководитель Управления перспективных технологий,
Лаборатория Касперского

Примечания

1 Приложения к докладу, а также другие аналитические и информационные материалы по теме «Кибербезопасность объектов критической ядерной инфраструктуры» можно найти на сайте проекта http://cynuc.pircenter.org.

2 Текст комментария составлен на основе выступления Н.И. Касперской на международной конференции «Повестка XXI века — новые технологии и вызовы глобальной безопасности», проведенной ПИР-Центром и Дипломатической академией МИД России 29 сентября 2016 г.

3 Текст комментария составлен на основе выступления А.П. Духвалова на международной конференции «Повестка XXI века — новые технологии и вызовы глобальной безопасности», проведенной ПИР-Центром и Дипломатической академией МИД России 29 сентября 2016 г.

БОЕВЫЕ РОБОТЫ: УГРОЗЫ УЧТЕННЫЕ ИЛИ НЕПРЕДВИДЕННЫЕ?

Эволюция военного дела связана с развитием технологий так же тесно, как и любая другая сфера государственной или общественной жизни. Образ войны будущего уже довольно давно ассоциируется с участием роботов, вызывая горячие дискуссии в военно-политических кругах и гуманитарных организациях. Особенно острые обсуждения касаются перспектив использования в военных целях смертоносных автономных систем (САС) — боевых машин, в той или иной степени оснащенных искусственным интеллектом и в перспективе способных самостоятельно принимать решения. Вопрос о внедрении такого типа вооружений пока новый для международной повестки, он находится на стыке политических, правовых, технологических и этико-моральных соображений. Именно поэтому выработка единого подхода государств или международных организаций затрудняется.

Определение смертоносных автономных систем, важнейшие вызовы, связанные с их использованием, а также механизмы контроля над САС, существующие в международном праве, обсуждались на заседании круглого стола, который прошел в сентябре 2016 г. в рамках международной конференции ПИР-Центра и Дипломатической академии МИД России «Повестка 21 века — новые технологии и вызовы глобальной безопасности». И впервые такого рода международная дискуссия состоялась на российской площадке. Обсуждение проводилась до декабрьской Конференции о «негуманном» оружии, на которой было принято решение о формировании группы правительственных экспертов (ГПЭ). Модератором дискуссии выступил Вадим ***Козюлин****, старший научный сотрудник ПИР-Центра. Участниками мероприятия стали научный сотрудник Центра международного права им. Лаутерпахта при Кембриджском университете Том* ***Грант****, первый секретарь отдела многостороннего разоружения Департамента по вопросам нераспространения и контроля над вооружениями МИД России Андрей* ***Гребенщиков****, советник по правовым вопросам Международного Комитета Красного Креста (МККК) Жиль* ***Джиака****, руководитель робототехнического центра Фонда «Сколково» Альберт* ***Ефимов****, профессор Сианьской политической академии Синьпин* ***Сун*** *и координатор Кампании против роботов-убийц (Campaign to Stop Killer Robots) Мэри* ***Уорхэм****.*

РАЗУМНЫЕ БОЕВЫЕ РОБОТЫ: ГДЕ БЬЕТСЯ СЕРДЦЕ ПРОБЛЕМЫ?

ВАДИМ КОЗЮЛИН: Проблема боевых роботов и связанных с ними угроз относительно нова как для России, так и для всего мира. По этому поводу существует большое разнообразие мнений, хотя в целом передовые умы планеты согласны с тем, что человечеству необходимо заняться этой проблемой прежде, чем сама проблема займется человечеством. У боевых роботов есть много названий: их называют смертоносными автономными системами (САС) или боевыми автономными роботизированными системами (БАРС), российские военные предпочитают называть их робототехническими комплексами (РТК). Предлагаю разобраться, в чем заключается суть опасений, связанных с боевыми роботами, и обсудить, что в настоящее время делается в мире для решения этой проблемы, а также, что нужно сделать, чтобы снять опасения и ограничить (либо упорядочить) развитие технологий создания боевых роботов.

Предлагаю начать с определения того, о чем идет речь: что мы подразумеваем под этими названиями?

ЖИЛЬ ДЖИАКА: Что имеется в виду под понятием «смертоносные автономные системы»? Терминология, определения и подходы в данной области сильно варьируются. Согласованного международного определения пока нет; у каждого государства и у каждой международной организации есть свои терминология и подход, иногда довольно сильно различающиеся. Это создает серьезные трудности. Многие государства в ходе переговоров утверждают, что очень сложно продвинуться к достижению каких-то договоренностей в отсутствие общих понятийного аппарата и критериев. Под автономным оружием можно подразумевать любую боевую систему, которая работает автономно — в воздухе, на море или на земле. С точки зрения Международного Комитета Красного Креста (МККК), любое оружие может быть смертоносным, так что мы предпочитаем употреблять термин «автономное/автоматическое оружие», без упоминания его смертоносных свойств. Чтобы облегчить ведение дискуссии, мы постарались максимально упростить рабочее определение таких систем, чтобы можно было расширить рамки для принятия государствами решений в будущем. Мы считаем, что даже такое упрощенное определение может послужить хорошим началом. Итак, мы определяем автономное оружие как оружие, которое способно самостоятельно обнаружить, идентифицировать и поразить цель. Таким образом, в центре внимания находятся так называемые критические функции оружия: определение, отслеживание, выбор и поражение цели. Почему Красный Крест отдает приоритет именно этим аспектам оружейных технологий? Это связано с самой концепцией применения силы. Будучи организацией, которая стоит на страже МГП, МККК стремится применять это право таким образом, чтобы максимально защитить мирное население — именно поэтому нас интересуют вышеуказанные аспекты. Роботы в военном деле могут использоваться в самых разных целях, в том числе в качестве транспорта и т. д. Нас же интересует именно возможность применения ими силы. Конечно, это очень широкий подход и объемное определение; под него могут подпадать даже противопехотные мины. Тем не менее мы считаем, что на данном этапе определение автономного оружия должно быть достаточно широким.

Государствам следует предложить рабочее определение подобного рода оружия, но мы понимаем, что это сложная задача, поскольку нужно избежать одновременно

излишне широкой и излишне узкой трактовки. Если определение окажется слишком широким, под него подпадут некоторые уже существующие военные технологии, например, беспилотные летательные аппараты. А здесь стоит учитывать, что многие страны на политическом уровне выступают против включения в определение автономного оружия систем, уже поставленных у них на вооружение. В то же время определение может оказаться слишком узким, и тогда дискуссии перейдут в область научной фантастики, искусственного интеллекта и т. д. Соблюсти баланс действительно сложно.

СИНЬПИН СУН: Нам неизбежно придется двигаться в сторону достижения международных договоренностей, регулирующих разработку и применение САС, чтобы иметь возможность контролировать сферы их применения и придерживаться гуманитарных принципов. Для этого международное сообщество должно прийти к широкому консенсусу по трем вопросам: формулировке определения САС, созданию их классификации, а также выработке практических мер для контроля над подобными системами еще до принятия международного законодательства для данной сферы. Однако консенсус по этим вопросам пока не достигнут, а ведущихся в настоящее время исследований явно недостаточно.

Основные разногласия между экспертами и исследователями из разных стран по вопросу определения САС касаются достижения договоренности об уровне автономности аппарата, который будет под него подпадать, а также о необходимости ограничения смертоносности таких систем. На данный момент те автономные системы, которые уже применяются на поле боя, нуждаются в человеке-операторе, который осуществляет такие функции, как передвижение оружейной платформы, идентификация и выбор цели и т. д. По прогнозам экспертов, в будущем автономные системы смогут работать полностью автоматически, без участия человека-оператора. В процессе эволюции этих технологий возможно также сосуществование полностью автоматических систем, их полуавтоматических аналогов и систем, которые управляются человеком. В зависимости от ситуации на поле боя (на земле, в воздухе или на море), все три режима будут применяться одновременно для разведки, обороны и нападения. Именно поэтому достигнуть международных договоренностей в данной области будет непросто. Что касается определения уровня смертоносности, некоторые эксперты предлагают использовать в качестве критериев степень поражения и способ нанесения удара. Другие считают, что степень смертоносности самого аппарата определить невозможно и что летальный исход зависит от условий и способов применения боевых систем. Даже такой краткий анализ показывает, что дать четкое определение САС на основе современного международного законодательства и состояния военной науки очень сложно.

Важную роль в создании международного законодательства для регулирования автономных боевых систем будет также играть классификация САС. По уровню автономности такие системы можно разделить на 3 категории: управляемые дистанционно (например, боевые беспилотные летательные аппараты, которые полностью управляются человеком с земли); полуавтоматические (управляются человеком при взлете, заправке и загрузке боеприпасов) и полностью автоматические (интеллектуальные боевые роботы). От уровня автономности будет напрямую зависеть степень юридической ответственности за ущерб, нанесенный такими системами. Однако степень автономности не будет достаточным критерием для

классификации. В связи с различиями между оружейными платформами и уровнем развития технологий уровень автономности боевых систем, произведенных в разных странах, будет отличаться.

Другим критерием классификации САС может служить театр военных действий, для которого они предназначены — по этому критерию их можно разделить на воздушные, морские и наземные. Легитимность такого оружия должна определяться на международном уровне в рамках гуманитарного права и соответствующих договоров. Классификация САС очень важна для регулирования вопросов их боевого применения и юридической ответственности за ущерб, однако в настоящее время общепринятые стандарты и критерии в данной сфере отсутствуют.

АЛЬБЕРТ ЕФИМОВ: Мы очень много спорим о том, что такое смертоносные автономные системы, боевые автономные роботизированные системы — есть разные определения. Мое определение робота очень простое: роботом является то, что называет таковым эксперт. И в мире не существует другого определения, потому что это действительно сложная задача.

Теперь о состоянии робототехники и обоснованности опасений, связанных с возможностями САС: если кто-то боится роботов-убийц, ему стоит посмотреть в Интернете видеоролики про юношей, собирающих и разбирающих автоматы Калашникова и демонстрирующих при этом верх скорости. Роботам, с их текущим состоянием системы распознавания и реакции, еще очень далеко до этих юношей. Роботу намного проще разгадывать загадки, чем делать простые операции. Думаю, что продвинутость искусственного интеллекта можно сравнить с уровнем интеллекта насекомых.

Что касается состояния искусственного интеллекта и нейронных сетей: Ян Ликун, основатель школы нейронных сетей глубокого обучения, отмечал, если сравнить интеллект с тортом, те достижения (обучение без подкрепления), которые мы сейчас имеем по нейронным сетям, были бы лишь вишенкой на нем. К сожалению, науке пока неизвестно, как приготовить сам торт. Поэтому при нынешнем состоянии искусственного интеллекта сложно даже вообразить роботов-убийц, которые смогут самостоятельно выбирать цели, а значит, нынешние опасения экспертов несколько преждевременны.

МЭРИ УОРХЭМ: Нас часто спрашивают о нашем определении полностью автономного оружия или смертоносных автономных систем (САС), как они называются в Конвенции о «негуманном» оружии (КНО). Определения имеют большое значение, поскольку они определяют, что именно подпадает под действие договора, и тем самым играют большую роль в определении того, насколько сильным или слабым будет договор с точки зрения регулирующего потенциала. Именно поэтому определения всегда согласовываются на финальной стадии переговоров, а не с самого начала.

Мы считаем, что САС — это системы вооружений будущего, которые благодаря датчикам и искусственному интеллекту смогут работать без значимого контроля со стороны человека. Они смогут выбирать и поражать цели самостоятельно, без участия человека в наведении оружия на цель и принятии решения о поражении цели для каждой отдельной атаки.

Полной ясности по поводу некоторых аспектов, что могут представлять собой САС, пока нет. Но после более трех лет обсуждений можно сказать, что уже сложилось твердое понимание концепции автономного оружия — она была четко сформулирована многими экспертами.

Возможно, тот факт, что кампания не сосредотачивается на работе с конкретной системой оружия, раздражает критиков. Но наша деятельность выходит за рамки попыток регулировать или даже запрещать определенные типы вооружений. Мы требуем, чтобы правительства оперативно реагировали на потенциальные изменения в логике ведения боевых действий, которые выводят человека из механизма управления вооружением. Машины уже давно служат в качестве орудий войны, но на протяжении истории ими управляли люди.

Можно привести много примеров того, как автономность проявляется в функционировании систем вооружений. В первый доклад Human Rights Watch (HRW) на эту тему, опубликованный в ноябре 2012 г., мы включили описание «предшественников» полностью автономного оружия, к которым мы отнесли вооруженные дроны и беспилотные самолеты, боевые стационарные сторожевые роботы, автоматические боевые комплексы, барражирующие боеприпасы и другое оружие. Также мы назвали шесть стран, которые ведут разработку автономных видов вооружений: США, Китай, Израиль, Южная Корея, Россия и Великобритания.

Другие организации также проводили исследования состояния НИОКР в сфере разработки автономного оружия. В 2016 г. в докладе МККК были представлены списки создаваемых или используемых систем оружия с определенной степенью автономности. Кроме указанных выше стран, САС также разрабатываются и используются в Австралии, Франции, Германии, Индии, Нидерландах, Норвегии, Южной Африке, Швеции и Украине.

Опубликованная информация демонстрирует, что количество стран, заинтересованных в разработке или приобретении автономных систем вооружения, растет. Вооружения-предшественники, названные HRW, а также системы, перечисленные в докладе МККК, не должны рассматриваться как полностью автономные вооружения или боевые автономные системы вооружения. В цикле принятия решений этих машин все еще присутствует человек — он контролирует процесс выбора цели и принятия решения о применении силы. Но с достижением полной автономности роботов человек будет исключен из этого цикла.

По нашему мнению, государства согласны с тем, что смертоносных автономных систем вооружений пока не существует. Представители нескольких стран, в том числе России, делали заявления по этому вопросу на третьем заседании участников Конвенции ООН об обычных вооружениях по САС, которое состоялось в Женеве в апреле 2016 г. Представители большинства стран заявили, что не планируют развивать данный тип вооружений, однако обещания будет сложно соблюсти, если появится аргумент: «Если другая сторона приобретает их, нам лучше сделать то же самое».

Мы видим несоответствия между тем, что государства утверждают, и тем, что они делают на практике по мере развития технологий. Например, в этом году мы наблюдали, как чиновники Пентагона активно продвигали концепцию третьей

стратегии сдерживания, направленной на достижение большей автономности оружия, в том числе на создание полностью автономного оружия.

АНДРЕЙ ГРЕБЕНЩИКОВ: Следует констатировать, что проведенные дискуссии по определению сути САС существенно не продвинули наше понимание подобных систем как предмета возможных договоренностей. К тому же они не сняли имеющиеся у нас сомнения и озабоченность в отношении того, насколько эта тема вообще поддается глубокой проработке. Она по-прежнему остается весьма сырой и противоречивой. Об этом, в частности, свидетельствует то, что дискуссии по САС продолжают носить сугубо академический и не всегда простой для восприятия характер. Прежде всего все упирается в согласование рабочего определения подобных систем. Для нас это важный момент — мы не хотели бы, чтобы переговорная работа по этой теме, если она вообще будет иметь место, оставляла этот вопрос «на потом». К сожалению, в переговорной практике есть примеры, когда ключевые определения вырабатывались не в первую очередь, в частности это было с Ословской конвенцией по кассетным боеприпасам (ККБ). Определение кассетных боеприпасов в этом документе, как известно, разделило эти вооружения на «плохие» и «хорошие» и оставило целый ряд высокотехнологичных образцов вне охвата конвенции. Для многих государств это впоследствии стало сдерживающим фактором для присоединения к ККБ.

Кроме того, на определении САС завязана дальнейшая работа по обсуждению ключевых аспектов этого оружия: понятий автономии/автономности, критических функций, значимого человеческого контроля, предсказуемости и т. д. И каких-то существенных подвижек на этом направлении мы пока не зафиксировали.

В целом, мы исходим из того, что, если серьезно заниматься данной темой, необходимо прежде пройти весь круг подготовки. Для начала следует разработать рабочее определение САС, согласовать ключевые параметры и сферу его охвата, субстантивно проработать имеющиеся концепции и определить те из них, которые имеют непосредственное отношение к предмету нашей дискуссии. Ничего из этого до сих пор не сделано, и нам представляется, что потенциал неформальных дискуссий до сих пор не задействован до конца.

Именно поэтому на последней неформальной встрече экспертов по САС российская делегация дистанцировалась от присоединения к согласованной государствами-участниками неофициальной рекомендации к Обзорной конференции КНО о создании группы правительственных экспертов (ГПЭ) по САС. Наша позиция была оформлена в виде особого мнения о целесообразности продолжения такой дискуссии в неофициальном формате.

Что касается дальнейших перспектив обсуждения САС, безусловно, окончательное решение по этому вопросу примет Обзорная конференция КНО в декабре 2016 г. Мы продолжаем анализировать ситуацию и со своей позицией окончательно определимся уже ближе к декабрьскому мероприятию[1].

[1] На Обзорной конференции КНО российская делегация не стала нарушать консенсус и при принятии итогового документа воздержалась от выступлений против учреждения группы правительственных экспертов открытого состава по САС.

МАШИНА НА ПОЛЕ БОЯ — РИСКИ ДОПУСТИМОЙ АВТОНОМНОСТИ

ВАДИМ КОЗЮЛИН: Известно, что беспилотная авиация применялась и в Первую, и во Вторую мировые войны. В послевоенный период на вооружении армий мира появилось множество боевых автономных систем в самых разных сферах: в частности ПВО, охрана границ. В чем суть проблем, связанных с САС, и почему эта тема возникла именно теперь?

ЖИЛЬ ДЖИАКА: Один из главных вопросов использования САС заключается в том, что будет означать утрата человеческого контроля над применением силы и каковы ее последствия.

С точки зрения МГП также существует ряд тревожных аспектов. Дело в том, что, судя по проведенным исследованиям, автономные боевые системы в определенном смысле уже существуют, хоть и в относительно простой форме. К примеру, существуют корабельные системы ПВО, которые автоматически открывают огонь по приближающимся целям, в частности по ракетам, без вмешательства оператора. При этом события на поле боя иногда развиваются так стремительно, что даже если бы систему постоянно контролировал оператор, он бы не успел отменить решение, принятое системой ПВО. Так что в определенном смысле такие системы уже существуют. Можно их называть высокоавтоматизированными, можно автономными — по большей части, это вопрос определений. Важно, что решения принимаются системой автономно, хотя эта автономия и ограничена параметрами, заданными оператором. Есть также разные типы систем в плане загрузки боеприпасов, применяемых типов ракет, однако после запуска они также функционируют автономно.

Опасения, связанные с САС, касаются и того, что результат в деле контроля над автономными вооружениями пока не достигнут. Опять же важно отметить, что, по мнению организации HRW, нам не следует включать в рамки этого обсуждения использование беспилотников или других систем, которые управляются оператором, поскольку они представляют отдельную категорию вооружений. Сконцентрироваться следует прежде всего на автономности в применении силы. И нас беспокоит еще, что на нынешнем этапе развития технологий именно автономные системы остаются за рамками обсуждения. Пока что обсуждается не вопрос контроля над полной автономностью, а вопрос о том, контролируются ли такие системы на расстоянии человеком-оператором.

Есть и другие типы современных наземных систем вооружений, которые имеют определенные черты автономности. Так что возникает много вопросов юридического и технического характера, и с этим сейчас связана актуальность темы. Разные государства могут быть участниками различных соглашений (например, некоторые страны подписали договор о кассетных боеприпасах, а другие нет), и в определенной степени их обязательства также различаются. Таковы реалии международного законодательства. Государства должны придерживаться своих международных обязательств, но решать, в чем конкретно заключаются эти обязательства, должны они сами.

АЛЬБЕРТ ЕФИМОВ: Внимание к теме, которое стало проявляться в последнее время, отчасти можно объяснить текущим состоянием робототехники. Многие называют его Кембрийским моментом робототехники — по аналогии с периодом,

когда у существ, которые вышли на землю, появились глаза. В этом смысле наука сейчас переживает взрывной момент развития робототехники, потому что у роботов появились «глаза» — сенсоры.

Кратко сравнивм солдата-человека и солдата-робота: робот — это 150 мегапикселей, человек — это 160 млн цветов. Человек может слышать звуки в диапазоне от 16 до 20 тысяч герц, у робота диапазон может быть больше. Пальцы человека могут чувствовать порядка 13 нанометров (уровень атома), а робот пока даже близко не обладает такой чувствительностью — в лучшем случае они различают материалы с точностью до миллиметра.

Уровень автономности машин в военной робототехнике на текущем этапе не стоит преувеличивать. В прошлом году я был свидетелем последнего испытания робота DARPA Robotics Challenge и могу сказать, если кто-то опасается роботов-убийц, он может в прямом смысле закрыть перед ними дверь; в ходе испытания роботы стояли по полчаса, пытаясь ее открыть.

На данный момент, для того чтобы остановить всех роботов-убийц, достаточно запустить станцию радиоэлектронной борьбы (РЭБ), а эти технологии известны еще с 1970-х гг. Воздействие радиоизлучения эффективно для вывода из строя даже очень продвинутых технологий, таких, как американский *RQ-170 Reaper*, который несколько лет назад иранцы посадили с помощью GPS-спуффинга. Подобная борьба сейчас ведется на Украине — сообщали, что в ДНР при помощи РЭБ недавно посадили украинский беспилотник.

При этом военная робототехника представляет достаточно значимый рынок, оцениваемый примерно в 7,5 млрд долларов. Он привлекает многих производителей и правительства. Возникает вопрос: стоит ли его запрещать? На текущий момент автоматизированные вооружения используются многими армиями мира. Можно привести пример американской систем *Phalanx* или аналогичной российской корабельной системы ПВО; подобные системы есть в армиях других стран. В комплексе многих таких систем человек уже не может быть полностью интегрирован в цикл принятия решений — это сложно и не гарантирует безопасности. Стоит вспомнить недавние события, когда американские самолеты разбомбили взвод сирийских солдат; человек в полной мере присутствовал в системе принятия решения, но тем не менее от жертв это не спасло. Если же оружие, которое обладает искусственным интеллектом, может сделать за человека опасную работу, у человечества есть моральное право его использовать, потому что таким образом государство защищает жизни своих солдат.

В то же время стоит вспомнить историю, которая произошла в 1988 г. с коммерческим пассажирским рейсом IR655 авиакомпании Iran Air. Авиалайнер был сбит ракетой *SM-2MR*, запущенной с американского крейсера Vincennes. Тогда этот комплекс действовал полностью в автоматическом режиме: автоматически засек цель (гражданский самолет с 290 пассажирами на борту), определил ее, как истребитель *F-14*, наносящий удар по этому фрегату, и сбил его. Хотя с того момента эти комплексы не используются в полностью автоматическом режиме, эта история показывает, что человечество уже несет потери от автоматического оружия, которое находится в строю многих стран мира.

Интересно проанализировать статистику точности современных вооружений. Во время Корейской войны 1950–1953 гг. человеческие потери США от «дружеского» огня составляли 8%. Во время войны во Вьетнаме 1965–1974 гг., а также в ходе недавних войн (Афганистан, Ирак, война с ИГИЛ) потери от «дружеского» огня составили примерно 19–21%. О какой эффективности высокоточного оружия может идти речь, если потери от «дружеского» огня возросли больше чем в два раза? Это сравнение явно не в пользу современных технологий.

МЭРИ УОРХЭМ: Чем опасно оружие, которое может выбирать и атаковать цели без вмешательства человека? Тем, что полностью автономные вооружения, вероятно, будут нарушать международное гуманитарное право и права человека, а также игнорировать ответственность за незаконные деяния с использованием оружия. Начиная с 2012 г. организация HRW публикует доклады по этому вопросу.

Суть проблемы в том, что полностью автономное оружие не будет обладать человеческой способностью к сопереживанию, которая может выступать в качестве ключа при принятии решения о совершении убийства. Уступить контроль над принятием решения о том, кому жить, а кому умирать — значит отнять у людей их неотъемлемое достоинство, поскольку неодушевленные машины не могут осознать ни ценность человеческой жизни, ни значимость ее потери.

В докладе 2013 г. профессор Кристоф Хейнс, специальный докладчик ООН по вопросу о внесудебных или произвольных казнях, показал, что проблема САС «поднимает обширные вопросы о защите жизни во время войны и мира». В докладе говорится, что «применение САС может быть неприемлемо, потому что адекватную систему правовой отчетности создать невозможно и потому что роботы не должны иметь власть над жизнью и смертью людей».

Хочется привести слова представителя РФ при Совете по правам человека, которые тот высказал на одном заседании: он отметил, что использование этого вида оружия может иметь «серьезные последствия для общественных устоев, в том числе привести к обесцениванию человеческой жизни. Представляется, что в перспективе такие машины могут значительно подорвать способность международно-правовой системы сохранять минимальный правовой порядок».

Полностью автономное оружие противоречит принципу гуманности и требованиям общественного сознания, закрепленным в «оговорке Мартенса», которая предлагает гражданским лицам и комбатантам в случаях, не оговоренных в международных соглашениях, руководствоваться установившимися обычаями, законами человечности и требованиями общественного сознания. Хотя у общественного сознания нет четкого определения, и общественное мнение, и мораль могут сыграть роль в его формировании. Перспектива делегировать принятие решений по вопросам жизни и смерти машинам глубоко тревожит многих людей и ставит серьезные нравственные вопросы.

Обсуждение способствует повышению транспарентности этой области и информированности населения, однако необходимо действовать быстро. Государствам следует начать обсуждение превентивного запрета на разработку, производство и использование полностью автономных систем вооружений. Это можно сделать, определив необходимую степень значимого человеческого контроля над клю-

чевыми боевыми функциями, в частности при принятии решении о совершении убийства по каждой отдельной атаке.

Начиная с 2012 г. многие известные личности поддержали эту идею, среди них более 20 лауреатов Нобелевской премии мира, более 150 религиозных лидеров и более 3000 специалистов по искусственному интеллекту. В июне мы видели пример поддержки запрета со стороны научного сообщества, когда компания Google DeepMind поддержала превентивный запрет на полностью автономное оружие на слушаниях в парламенте Великобритании.

Спустя почти четыре года с момента запуска Кампании против роботов-убийц в апреле 2013 г. мы видим, что тема роботов-убийц активнее обсуждается правительствами, а также экспертами по этическим, правовым, военным и техническим вопросам. Ученые, ранее игнорировавшие эту тему, теперь регулярно проводят по ней семинары и работают над публикациями.

СИНЬПИН СУН: По мере стремительного развития военных технологий САС привлекают все большее внимание со стороны международного сообщества. Старт разработке автономных роботизированных систем дала сама промышленность, и прогресс в данной сфере привел к революционным изменениям в таких областях, как транспорт, управление складами и т. д. В военной области тоже происходит революция. Разработка и появление таких автономных оружейных систем, которые сочетают в себе сбор информации, ее оценку, принятие решений и непосредственное осуществление действий, несомненно, приведет к очень серьезным и даже шокирующим изменениям на поле боя. Такие перемены вызывают огромные опасения и тревогу со стороны международного сообщества, особенно среди специалистов в сфере МГП.

АНДРЕЙ ГРЕБЕНЩИКОВ: МИД РФ отслеживает развитие этой темы с момента начала ее обсуждения в Совете по правам человека. В 2013 г., как известно, по предложению делегаций Бразилии и Франции, работа по САС была перенесена на площадку КНО, где в течение трех лет она обсуждалась в неофициальном формате. Были проведены три специализированные встречи экспертов по САС, в ходе которых сначала под председательством Франции, а затем и Германии были предприняты попытки провести всесторонний анализ этой проблематики: ее технических, международно-правовых, морально-этических и других аспектов.

Следует отметить, что с самого начала российская делегация не скрывала своего настороженного отношения к этому процессу и перспективам проработки этой непростой и противоречивой темы на площадке КНО. И связано это было с целым рядом обстоятельств.

Прежде всего мы отдавали себе отчет в том, что речь идет исключительно о виртуальной технике, пока не имеющей реально работающих образцов, о которой многие делегации имеют весьма приблизительное представление. Конечно, в международной практике есть прецеденты выработки договоренностей, установивших превентивный запрет в отношении перспективных видов вооружений, например Протокол IV КНО об ослепляющем лазерном оружии, запретивший не само лазерное оружие, а его применение, пагубно отражающееся на здоровье человека. Однако, очевидно, что САС представляют собой более сложный вид вооружений, которому сложно дать определение.

Следующее обстоятельство — трудность проведения четкого «водораздела» между гражданскими и военными разработками автономных систем. Очевидно, что будущее человечества стоит за автономными технологиями, и было бы ошибкой лишить себя возможности пользоваться их преимуществами.

Также у нас существовали сомнения по поводу утверждений о недостаточности существующих международно-правовых положений в отношении САС. На наш взгляд, международное гуманитарное право (МГП) в случае его строгого соблюдения уже налагает некоторые ограничения при разработке и использовании таких систем. В частности это относится к часто цитируемому Доппротоколу I 1977 г. к Женевским конвенциям 1949 г., установившему принципы избирательности, пропорциональности и принятия мер предосторожности для защиты гражданского населения. Этот протокол также обязал государства при изучении, разработке, приобретении или принятии на вооружение новых видов оружия удостоверяться в их соответствии нормам МГП.

Наконец нам не хотелось компрометировать нашу КНО. Очевидно, в условиях чересчур завышенных ожиданий со стороны международного сообщества неспособность государств — участников КНО прийти к консенсусу по данной теме могла бы навредить авторитету КНО как площадки. Не следует забывать о том, что уникальность нашей Конвенции заключается в сбалансированности, взвешенном учете как гуманитарных соображений, так и законных оборонных интересов государств. Рассмотрение новых тем должно проходить при строгом учете этого обстоятельства. В целом, мы исходим из того, что укрепление КНО должно производиться не через поиск новых тем, а прежде всего посредством дальнейшей универсализации этого документа, тем более что для этого есть большой потенциал — в настоящий момент участниками Конвенции являются 123 государства: из них 116 присоединились к Протоколу I о необнаруживаемых осколках, 102 — к Дополненному «минному» Протоколу 2 (ДП-2), 113 — к Протоколу 3 о запрещении или ограничении зажигательного оружия, 107 — к Протоколу 4 об ослепляющем лазерном оружии, 91 — к Протоколу 5 о взрывоопасных пережитках войны. Мы работаем в этом направлении с государствами ОДКБ — с находящими вне конвенции Арменией и Киргизией, а также с не участвующим в ДП-2 и Протоколе 5 Казахстаном. Подвижки достигаются — в Казахстане соответствующее решение находится на этапе ратификации.

Что касается наших оценок прошедших экспертных встреч по САС на площадке КНО, безусловно, они были весьма интересными. Особенно это касается последних двух дискуссий в апреле 2015 и 2016 гг., которые приобрели более структурированный характер при председательстве германского постпреда при Конференции по разоружению М. Бионтино. Одним из достижений последней встречи стало признание государствами применимости действующих положений МГП к САС и важности сохранения за ними контроля со стороны человека.

ПРАВИЛА ПОВЕДЕНИЯ ДЛЯ РОБОТОВ

ВАДИМ КОЗЮЛИН: Можно ли урегулировать проблему на международном уровне при отсутствии общепринятого определения, когда не достигнуто согласие о том, какие вооружения подпадают под определение смертоносных автономных систем?

СИНЬПИН СУН: Было бы необъективно утверждать, что существующее МГП никак не регулирует вопрос САС. Нормы, применяемые к регулированию использования вооружений в международном законодательстве, можно разделить на три группы:

1. Запреты и ограничения на конкретные виды оружия в рамках международных договоров. К примеру, существует запрет на употребление взрывчатых и зажигательных пуль весом менее 400 грамм в рамках Санкт-Петербургской декларации 1868 г. Гаагской декларацией 1899 г. введен запрет на применение пуль, которые расширяются или деформируются в теле человека, а также удушающих газов. Аналогичные запреты есть в Гаагской конвенции 1907 г., Женевской конвенции 1949 г. и в Дополнительном протоколе I 1977 г., а также в Конвенции ООН о запрещении и ограничении применения конкретных видов обычных вооружений от 1980 г.

2. Запреты и ограничения на конкретные виды оружия в рамках обычного международного права. По результатам исследования положений обычного международного права в гуманитарной сфере, проведенного МККК, использование ядов, оружия, содержащего яды, биологического и химического оружия противоречит международному обычаю.

3. Общие принципы, регулирующие применение оружия в рамках МГП. Основные принципы касаются ограничения поражающего воздействия, разграничения между комбатантами и некомбатантами, пропорциональности целей и средств, военной необходимости и т. д. В соответствии с этими принципами необходимо тщательно выбирать военные средства и методы, когда вопрос не регулируется договорным или обычным международным правом.

Среди этих принципов и международных обычаев особо стоит отметить «оговорку Мартенса», которая является юридически обязывающей при разработке и применении любых типов вооружений, в том числе САС. Такие автономные системы не будут легитимированы международным сообществом, если они не будут соответствовать гуманитарным принципам и требованиям общественной морали. «Оговорка Мартенса» содержится в преамбуле к Конвенции о законах и обычаях войны на суше от 1899 г. Она также была подтверждена в преамбуле Гаагской конвенции (IV) 1907 г., а также в Статье 1 (2) Дополнительного протокола I. В консультативном заключении Международного суда от 1996 г. говорится, что оговорка «показала себя эффективным механизмом решения вопросов, связанных с быстрым развитием военных технологий».

Тем не менее существующее МГП имеет явные недостатки в плане регулирования САС. Несмотря на дух и принципы международного права, конкретные положения, касающиеся САС, в нем отсутствуют. Даже статья 36, которая обязывает страны проводить анализ и оценку новых вооружений, не содержит конкретных мер и юридической ответственности за нарушение обязательств. Выполнение этих обязательств остается на совести каждого конкретного государства. В результате этого общее обязательство, касающееся оценки новых систем вооружений, скорее всего, не будет выполнено, особенно при наличии явной военной необходимости использовать САС.

ЖИЛЬ ЖИАКА: Основные разногласия по поводу применения положений права к регулированию технологий находятся в области толкования законов. Проводи-

мые дискуссии помогают дипломатам достигнуть прогресса в понимании того, не приведет ли развитие новой технологии к определенным проблемам. В дальнейшем нужно разрабатывать практические рекомендации и, возможно, в будущем мы сможем приступить к регулированию таких военных технологий на международном уровне с помощью международных договоров. На данном этапе, в рамках международных дебатов по поводу Конвенции о конкретных типах обычного оружия — и это отметил наш российский коллега — некоторые государства придерживаются более формального подхода. Красный Крест считает, что важно продолжать дискуссии и дебаты, даже если они заводят нас в тупик, ведь главное — это продолжать разговор с военными. Часто такие обсуждения помогают нам совершенствовать наш подход и сделать его более реалистичным. К примеру, благодаря этим дискуссиям нам стало ясно, что у военных нет желания разрабатывать автономные системы, которые они потом не смогут контролировать, так что в каком-то смысле главный вопрос заключается в обеспечении мер контроля над автономными системами. Каковы должны быть критерии такого контроля? Здесь, на наш взгляд, есть широкое поле для обмена мнениями между разными странами. Мы приглашаем государства, и, конечно, Российскую Федерацию, продолжать диалог и предлагать решения, которые позволят нам достигнуть прогресса. И мы в МККК надеемся, что дискуссия будет продолжена в более официальном формате, возможно, в формате заседания ГПЭ в декабре 2016 г.

МЭРИ УОРХЭМ: Даже в отсутствие единого определения САС, сохранив значимый контроль человека над применением смертоносной силы в каждой конкретной атаке, мы можем фактически запретить использование полностью автономного оружия и тем самым добиться превентивного запрета. Установление значимого контроля человека за применением оружия поможет защитить человеческое достоинство во время войны. Введение контроля вполне соответствовало бы принципам МГП, в частности принципам избирательности и соразмерности, и поощряло бы их соблюдение.

Человеческий контроль также важен для обеспечения прав человека. Как отмечали два специальных докладчика ООН в феврале 2016 г.: «Там, где используется передовая технология, сотрудники силовых ведомств должны лично контролировать фактическое применение силы».

Сохранение значимого человеческого контроля позволит избежать вакуума ответственности, который возникнет при использовании полностью автономного оружия. Это позволит гарантировать, что виновный за преступное деяние, вызванное использованием оружия, будет наказан. Юридическое требование соблюдения человеческого контроля обеспечит привлечение к уголовной ответственности командира за использование любого оружия без такого контроля.

Значимый человеческий контроль также поможет избежать угрозы для фундаментальных моральных принципов в связи с решением о применении силы.

Законодательство в сфере разоружения имеет долгую историю запрещения вооружений из-за опасений отсутствия контроля, и обеспечивает прямой прецедент для запрета оружия, над которым нет контроля человека. Международный запрет на биологическое и химическое оружие также частично был вызван опасениями об управляемости оружия — при его применении люди не могут контролировать, куда оно движется и кого убивает, а это ведет к непредвиденным жертвам. Ана-

логичным образом противопехотные мины и кассетные боеприпасы запрещены во всем мире из-за опасения по поводу их неизбирательной природы и недостатка контроля.

В некоторых областях права контроль является позитивным обязательством, налагаемым на государства, а не порогом, который влечет ответственность. Например, международное экологическое право требует от государств контроля над загрязнением и другим ущербом для окружающей среды в целях предотвращения и минимизации вреда природе.

АНДРЕЙ ГРЕБЕНЩИКОВ: Не стоит рассматривать осторожную позицию МИД РФ по САС как игнорирующую активные усилия гуманитарных НПО в этой области. Наоборот, мы очень внимательно следим за процессом и крайне уважительно относимся к работе сторонников дальнейшего рассмотрения этой темы, в частности таких авторитетных акторов, как Кампания против роботов-убийц и МККК. За нашей позицией стоит стремление обстоятельно разобраться во всех нюансах этой непростой темы и принять по ней осмысленное решение в соответствии с заложенным в КНО принципом баланса между гуманитарными аспектами и интересами оборонной безопасности.

При этом я хотел бы напомнить, что наша страна имеет хорошие традиции активного участия в создании норм МГП, заложенные еще со времен известной оговорки Федора Федоровича Мартенса. Как известно, этот петербургский профессор в свое время предложил выход из переговорного тупика, сложившегося при выработке международной Конвенции о законах и обычаях сухопутной войны 1899 г. С того момента эта российская оговорка стала нечто большим — она превратилась в неотъемлемую часть МГП.

ТОМ ГРАНТ: Я бы хотел сказать несколько слов о нынешнем состоянии международного права и особенно о том, как оно рассматривает науку и технологии в сфере автономных вооружений. За последние два столетия были созданы самые разные инструменты, призванные решить вопрос новых военных разработок и технологий. Однако интересно было бы взглянуть на параллели и различия между этими инструментами. Уже к середине XIX в. стало понятно, что развитие науки может повлиять на оружейные технологии. Это ясно и сейчас, в этом плане ничего не изменилось. Но есть и определенные важные отличия. Как вы знаете, уже в Санкт-Петербургской декларации 1868 г. появились признаки того, что выработка общего подхода к проблеме возможна. Стороны договорились достигнуть взаимопонимания по поводу конкретных предложений, по крайней мере они согласились действовать коллективно. В принятом 100 лет спустя Дополнительном протоколе I 1977 г. говорится, что высокая договаривающаяся сторона — в единственном числе — будет обязана определить, не станет ли применение такого оружия нарушением договоренностей. Однако теперь уже акцент делался на обязательстве, а не на будущих законодательных инструментах. Кроме того, акцент делался на отдельном государстве, а не на группе государств. Поэтому давайте подчеркнем, что в Санкт-Петербургской декларации речь шла о группе государств. А сейчас мы говорим о международном законодательном инструменте 1977 г., который применим к высоким договаривающимся сторонам. Почему так важно это различие? Оно имеет огромное значение, потому что политика в области вооружений и отношение государств к новым оружейным технологиям — это та

область, где крайне важна самостоятельная оценка. По крайней мере, существующее ныне законодательство показывает, что именно государствам принадлежит право решать, что они могут и обязаны сделать. Несомненно, в соответствии с Протоколом 1977 г. существует обязанность предпринимать какие-то действия. Там так и говорится: на государствах лежит обязательство определить, соответствует ли развертывание какого-либо оружия требованиям МГП. Другими словами, решение должна принимать высокая договаривающаяся сторона — акцент делается на самостоятельной оценке.

В гуманитарном праве также затрагивается тема развития информированности по военным вопросам. Конвенция, в частности, гласит, что государства должны ее придерживаться и включать ее текст в свои законы — возможно, с какими-то дальнейшими разъяснениями, но это они должны делать обязательно. Однако не существует международной военной конвенции или международного договора, где прямо бы описывалось, как выполнять эти предписания, как преподавать в военных школах и развивать эту информированность среди военных. Так что преподавать их приходится так, как это определено в военных образовательных программах конкретного государства.

Я не особо разбираюсь в технологиях, но меня всегда очень интересовала тема машинного обучения и шагов, которые нужно предпринять, для того чтобы разработать способные к автономным действиям машины. В законодательных и нормативных актах мало говорится о преподавании МГП, и, насколько я понимаю, там отсутствует описание методик, которые помогли бы нам обучить машину гуманитарным принципам, если до такого когда-нибудь дойдет. В любом случае, в подобных документах ничего не говорится о том, как сконструировать обучающие алгоритмы или программы. Тем не менее, как видите, международное законодательство уже имеет опыт регулирования вопросов научно-технического прогресса.

СТАРЫЕ НОРМЫ О ГЛАВНОМ

ВАДИМ КОЗЮЛИН: Как сегодня было неоднократно отмечено, система контроля над вооружениями имеет богатую историю и широкий инструментарий. Начиная с Петербургской декларации 1868 г. было принято множество международных документов, в том числе относительно правил ведения войны и применения силы. Может быть, существующих международных договоренностей уже достаточно, и стоит сконцентрироваться на их реализации, а не стремиться заключить новые соглашения?

ТОМ ГРАНТ: Пару лет назад между Австралией и Японией возник спор. На первый взгляд, он не имел никакого отношения к автономным боевым системам. Спор шел о том, как трактовать понятие «забой китов в научных целях». В соответствующей конвенции сказано: «Если вы преследуете научные цели, вы имеете право убивать китов». И вот какое заключение дал Международный Суд: «Суд считает, что Статья VIII дает государствам — участникам Конвенции о китобойном промысле право самостоятельно принимать решение об отказе в выдаче особого разрешения либо указывать конкретные условия, на которых выдается такое разрешение». Ключевое слово здесь — «разрешение». Так что в данном вопросе, который относится к научным исследованиям, каждое конкретное государство имеет право само-

стоятельно принимать решение. На мой взгляд, тут можно провести параллель с самостоятельной оценкой, предполагаемой статьей 36, когда речь идет о разработке нового оружия.

Однако далее в судебном решении говорится: «Однако решение о том, действительно ли цель забоя, отлова или обработки кита в соответствии с запрошенным особым разрешением является *научной*, не может быть оставлено лишь на усмотрение отдельного государства». Таким образом, юристы, работающие с национальным законодательством, а также международные юристы часто оказываются в ситуации, когда для правильной трактовки закона нужно читать все законодательство, а не какой-то отдельный параграф из закона. Я привел этот спор в качестве примера, чтобы показать, что международное право склоняется к тому, чтобы не оставлять научно-технические вопросы на усмотрение отдельных государств, позволяя им проводить самостоятельную оценку. Возможно, это дает повод для оптимизма. Киты — это важный вопрос, для некоторых стран даже очень важный. Но вопросы обороны и безопасности для большинства государств еще важнее.

СИНЬПИН СУН: Международное сообщество может пойти двумя разными законодательными путями. Первый путь — это так называемое публичное законотворчество. В рамах этого подхода одно или несколько государств выдвигают законодательную инициативу, разрабатывают проект законодательного акта, а затем призывают другие страны присоединиться к предложенному договору. Примерами публичного законотворчества являются Оттавский договор о запрещении противопехотных мин и подписанная в 2008 г. ККБ. Второй путь — это официальное законотворчество, т. е. подход, в котором ведущую роль играет ООН. Его примером является Конвенция о запрещении и ограничении применения конкретных видов обычного оружия 1980 г. По сравнению с публичным законотворчеством официальное обычно завершается подписанием более эффективных договоров, хотя для заключения таких договоров бывает сложнее заручиться всеобщей поддержкой и сделать их юридически обязывающими. Официальный путь занимает больше времени, но, с другой стороны, он имеет преимущества высокого статуса и влияния ООН. Его также может быть удобнее исполнять, поскольку его участниками являются суверенные государства. Поэтому я считаю, что официальное законотворчество является оптимальным выбором, поскольку контролировать выполнение обязательств в рамках таких договоров можно под эгидой ООН.

МЭРИ УОРХЭМ: В мае 2013 г. правительства впервые рассматривали вопрос о контроле над роботизированными вооружениями в рамках многостороннего форума, после того как специальный докладчик ООН по вопросам внесудебных убийств выпустил доклад, в котором рекомендовал государствам ввести национальный мораторий на автономное оружие. В ходе диалога, последовавшего за презентацией доклада Совету по правам человека, 20 стран выразили интерес к проблеме, связанной с полностью автономным оружием. Ни одна страна не выступила против проведения дискуссии по этому вопросу, а некоторые высказали мнение, что КНО была бы подходящим местом для дальнейшего обсуждения этой темы.

В ноябре 2013 г. высокие договаривающиеся стороны КНО согласились включить вопрос о том, что они назвали САС вооружений, в программу работы КНО и провести четырехдневное совещание на эту тему в мае 2014 г. в ООН в Женеве.

Итог этого неофициального совещания экспертов был феноменальным и беспрецедентным. В нем приняли участие представители 87 стран, сотрудники ООН, МККК, активисты, а также 18 экспертов. Представители пяти стран призвали полностью запретить автономное оружие, многие другие подчеркивали важность постоянного значимого человеческого контроля при выборе боевой системой цели и принятии решения о начале атаки.

Начиная с 2014 г. КНО провела три недельные встречи по боевым автономным системам вооружений. В декабре 2016 г. правительства откликнулись на призыв гражданского общества активизировать обсуждение вызовов, которые влечет за собой развитие САС. Было принято решение учредить ГПЭ на площадке КНО, что еще на шаг приблизило мир к введению запрета на использование САС. На сегодняшний день можно говорить о большем понимании участниками дискуссий правовых вопросов, вопросов ответственности, аспектов распространения и безопасности, проблематики прав человека, а также этических соображений, связанных с развитием САС.

Кампания против роботов-убийц считает, что развитие КНО может привести к разработке нового протокола, и поддерживает продолжение переговоров, но не любой ценой. Длительного, затяжного процесса, который дает слабый или нулевой результат, следует избегать.

СИНЬПИН СУН: На сегодняшний день существует немало принципов МГП, на соблюдении которых при развитии и использовании САС действительно стоит сконцентрироваться. Во-первых, нужно отметить принцип разграничения между военными целями и мирным населением, между комбатантами и гражданскими лицами во время войны. Этот принцип берет свое начало еще в Санкт-Петербургской декларации 1868 г. В дальнейшем он был подтвержден в Дополнительном протоколе I 1977 г (статья 48). Некоторые САС не соответствуют этому принципу как из-за степени смертоносности их поражающего воздействия, так и по целому ряду других причин.

Второй важный принцип — это принцип пропорциональности. Он гласит, что масштаб разрушений должен примерно соответствовать важности решаемой военной задачи. В статье 57 Дополнительного протокола I 1977 г. говорится, что в ходе военных операций нужно предпринимать все разумные меры предосторожности в выборе средств и методов поражения. Подчеркивается, что воюющим сторонам следует также воздерживаться от операций, которые могут вызвать случайные жертвы среди мирного населения и причинить гражданским объектам ущерб, который окажется несоразмерным ожидаемой военной ценности операции. Некоторые САС могут вызывать настолько масштабные и долгосрочные разрушения, что их применение приведет к нарушению принципа пропорциональности.

Наконец, следует применять принцип анализа новых вооружений на предмет их соответствия требованиям МГП. Это положение содержится в Санкт-Петербургской декларации 1868 г. и в Дополнительном протоколе 1977 г. (статья 36). Это обязательство также будет нарушено, если государства не будут должным образом контролировать разработку САС.

АНДРЕЙ ГРЕБЕНЩИКОВ: Хотел бы остановиться на политике нашей страны в отношении вооружений с растущей степенью автономности. Не буду скрывать,

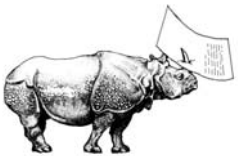
что за последние годы в России был принят целый ряд мер, направленных на развитие отечественного роботостроения для нужд российских вооруженных сил. Значительная работа была проделана и по формированию законодательной базы на этом направлении — по этому вопросу был принят указ президента.

Однако мы исходим из необходимости неукоснительно соблюдать существующие положения МГП, которые в полной мере применимы к автономному оружию. Речь идет прежде всего об уже упомянутом Доппротоколе I 1977 г. к Женевским Конвенциям 1949 г. Россия строго придерживается данных обязательств и призывает государства, до сих пор не подписавшие Доппротокол I (в том числе США, Израиль, Иран, Палестину, Индию и Турцию), присоединиться к нему. На наш взгляд, это способствовало бы решению проблем, связанных с развитием САС.

В нашей стране соблюдается и статья 36 о проведении так называемых правовых обзоров новых систем оружия. На начальных этапах создания образцов вооружения, военной и специальной техники соответствующая экспертиза осуществляется в рамках НИОКР.

Национальное законодательство РФ содержит и другие положения, ставящие барьер для возможного использования вооружений, которые противоречат обязательствам России в рамках МГП. Нормы международного права составляют основу принятой в декабре 2014 г. военной доктрины России, ссылки на МГП содержат и соответствующие документы Вооруженных Сил России.

ВАДИМ КОЗЮЛИН: Уважаемые коллеги, благодарю всех участников за интересную и содержательную дискуссию. Редакция журнала совместно с ПИР-Центром будет внимательно следить за обсуждением темы САС в мировой прессе и на международных форумах. Давайте и впредь будем обмениваться мнениями по этой проблеме, чтобы наши читатели оставались в курсе текущих процессов.



Ярмо Сарева

ВЫЗОВЫ ТЕХНОЛОГИЙ XXI в. ДЛЯ СТРАТЕГИЧЕСКОЙ СТАБИЛЬНОСТИ И ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ[1]

В 1139 г. на Втором Латеранском соборе, созванном по инициативе Папы Римского Иннокентия II, был принят Канон № 29, который запретил христианам использовать луки и арбалеты против других христиан. Это простое в применении и давно уже известное оружие позволяло обычному солдату убить рыцаря в тяжелых доспехах на расстоянии, не вступая с ним в непосредственный бой, что противоречило концепции рыцарской чести. При этом и луки, и арбалеты могли убивать без разбора и на большом расстоянии, когда сам лучник не подвергался никакой опасности. Поэтому наложенный на них запрет объяснялся не какими-то особенностями самой технологии, а новыми обстоятельствами их применения, а также их растущей убойной силой. Таким образом, практика запрещения новых технологий, которые воспринимаются как диспропорционально опасные или неэтичные, вовсе не нова.

ЧТО ТАКОЕ ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ В КОНТЕКСТЕ БЕЗОПАСНОСТИ?

Сегодня определить круг технологий, подпадающих под определение «новых» или «перспективных» (emerging technologies) не менее сложно, чем прийти к единому определению «перспективных экономик» (emerging economies), ведь слово «перспективные» весьма многогранно. Поэтому можно обозначить ряд характеристик, которые делают технологию перспективной:

1. Перспективные технологии являются относительно новыми, они еще не стали повсеместными и широко распространенными. Они пока находятся на самых ранних стадиях своего развития либо вообще существуют лишь в теории.
2. Перспективные технологии выводят на повестку дня вопросы о роли людей, которые их применяют, о человеческой ответственности и об этическом измерении их использования. Является ли развитие некоторых перспективных технологий нежелательным? Что, если они приведут к *обесчеловечиванию* стоящих за ними людей? Как определить понятие *значимый человеческий контроль* (meaningful human control)?
3. Эволюция и развитие перспективных технологий нелинейны. Перспективные технологии не идут по логичному эволюционному пути «зарождение–перспективность–повсеместное распространение». Их эволюция зависит скорее от нашей воли, чем от логики научного прогресса. Некоторые технологии раз-

виваются намного быстрее или медленнее, чем ожидалось, другие даже оказываются нежизнеспособными. Как выразился один автор, «эффект новых технологий — как позитивный, так и негативный — зачастую переоценивается в краткосрочной перспективе и недооценивается в долгосрочной»[2].

4. Перспективные технологии могут разрушать существующее равновесие, а также порождать страхи и сомнения по следующим причинам:

   - в силу самой своей природы эти технологии много обещают, однако их реальный потенциал до конца не известен. Они не только открывают новые перспективы, но и порождают сомнения и страхи относительно своих потенциальных негативных аспектов;

   - такого рода технологии имеют определенный деструктивный потенциал, разрушая сложившийся баланс, создавая новые рынки и вытесняя уже устоявшиеся технологии. Этим они отличаются от эволюционного пути инноваций, в рамках которого технологии совершенствуются постепенно и предсказуемо. В этой связи нам приходится задаваться вопросом о том, какие устоявшиеся технологии устареют с приходом той или иной новой технологии;

   - перспективные технологии могут приводить к масштабным переменам и поднимать новые вопросы. Дело не столько в том, когда и как эти технологии получат широкое распространение, а в том, насколько связанные с ними опасения сами по себе являются проблемой для современных международных отношений. Точно так же, как анархия не является врожденным свойством международных отношений, научный прогресс однозначно тоже не может повлиять на данную сферу — все зависит от того, какой подход изберут сами участники международных отношений. Наше отношение к перспективным технологиям и связанным с ними проблемами во многом определяется культурными, моральными и религиозными факторами. Антиутопическое видение будущего (так называемый *синдром Терминатора*) часто отбрасывается в сторону как плод болезненного воображения. Тем не менее такое видение отражает некие конкретные опасения и частично задает направление общественной дискуссии. И, наоборот, утопическое видение будущего, связанное с перспективными технологиями, часто задает направление усилиям ученых и исследователей.

К перспективным обычно относят следующие новые технологии: автономные оружейные системы, кибер-, био- и космические технологии, трехмерную (3D) печать и оружие направленной энергии. Все эти технологии имеют разное прошлое и будущее, но при этом они тесно переплетаются между собой и поднимают многие вышеупомянутые вопросы.

Рассмотрим подробнее ситуацию вокруг перспективных биотехнологий, к которым относятся клеточные технологии (регенеративная медицина), молекулярные биотехнологии (включая трансгенные растения и животные), геномная медицина (персонализированная медицина, генная терапия и биоинформатика) и синтетическая биология (то есть синтез биологических структур с целью создания стандартизированных биологических объектов, обычно построенных на основе ДНК). Перед нами открываются перспективы создания новых биологических организмов для применения в разных сферах, например, для синтеза биотоплива. Недавно впервые были успешно синтезированы и реплицированы искусственные бактерии и вирусы. Еще

более амбициозной целью синтетической биологии является создание новых форм жизни. В этот же список можно включить нанотехнологии и наномедицину.

Для биотехнологий весьма характерно уже упомянутое противоречивое сочетание больших надежд и серьезных опасений. Часто говорят: если XX в. был веком физики, то XXI в. станет веком биотехнологий. Общество и ученые связывают с биотехнологиями большие ожидания, поскольку они могут значительно продвинуть вперед медицину и повысить благосостояние всего человечества. Однако биотехнологии вызывают и серьезные опасения: кое-кто утверждает, что по сравнению с некоторыми из них биологическое и химическое оружие XX в. покажется глубоко устаревшим. Нельзя исключить возможность того, что синтетические организмы выйдут из-под контроля, особенно если они будут обладать способностью к самостоятельной репликации.

Что касается работы ООН в данном направлении, стоит особо отметить ежегодные заседания экспертов в рамках Конвенции о запрещении биологического оружия (КБО), проводившиеся в 2012–2015 гг. Этим экспертам было поручено проанализировать последние достижения в сфере науки и передовых технологий, в том числе:

- исследования и разработки, которые потенциально могут использоваться в целях, противоречащих положениям Конвенции;
- исследования и разработки, которые потенциально могут помочь в достижении целей и задач Конвенции;
- меры по укреплению национальных систем управления биологическими рисками;
- добровольные правила поведения и другие меры, призванные обеспечить ответственное поведение со стороны ученых, исследователей и промышленности;
- образовательные программы и проекты информирования общественности о рисках и преимуществах биологических исследований и биотехнологий;
- события и тенденции, затрагивающие работу таких многосторонних организаций, как Всемирная организация здравоохранения, Всемирная зооветеринарная организация, Продовольственная и сельскохозяйственная организация ООН, Международная конвенция по защите растений и Организация по запрещению химического оружия.

В этой связи необходимо упомянуть внесенное Россией предложение о принятии документа, имеющего юридически обязывающую силу и направленного на укрепление Конвенции, о создании мобильных биомедицинских отрядов в рамках КБО для оказания помощи в случае биологических инцидентов, а также о создании Научного консультационного комитета, который бы анализировал последние научные достижения и вносил рекомендации в тех случаях, когда такие достижения имеют отношения к предмету Конвенции. Россия также поддержала китайскую инициативу о внедрении международного механизма экспортного контроля и принятии международного кодекса поведения для ученых-биологов.

Технология оружия направленной энергии, несомненно, подпадает под определение перспективной, поскольку со временем она может сделать ненужными амуницию и боеприпасы. После подписания Протокола IV Конвенции о запрещении или ограничении применения конкретных видов обычного оружия дискуссии о перспективных технологиях в данной сфере отошли на периферию повестки дня. При этом оружие направленной энергии является технологией двойного применения

в меньшей степени, чем другие перспективные технологии, к тому же программы разработки такого оружия пока что ведутся лишь в самых передовых странах.

Распространение и дальнейшее совершенствование технологии трехмерной печати также может породить ряд серьезных проблем, особенно в сфере контроля над экспортом вооружений. Экспортный контроль может потерять всякий смысл, если каждый сможет напечатать оружие и боеприпасы к нему у себя дома на 3D-принтере. В то же время 3D-печать является многообещающей технологией в плане защиты окружающей среды и устойчивого развития, поскольку она значительно сократит потребность в перевозке товаров из одной точки планеты в другую, а также облегчит дистрибуцию продукции в самых отдаленных и труднодоступных регионах.

СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ КАК УСЛОВИЕ РЕШЕНИЯ ГЛОБАЛЬНЫХ ПРОБЛЕМ

Стратегическая стабильность — это состояние, при котором военная мощь сбалансированно распределена между государствами, и ни у одного из них нет стимулов для попыток разрушить сложившийся баланс. Эта концепция тесно связана с концепцией сдерживания, в основном опирающегося на ядерную мощь, однако превосходство в обычных вооружениях, то есть, наличие большой армии, технологически превосходящей своих потенциальных противников, также может стать средством сдерживания.

Что касается глобальной безопасности, ее иногда воспринимают в качестве понятия, лежащего на противоположном конце спектра от национальной безопасности, то есть от выживания какого-то конкретного государства. Однако в силу таких факторов, как изменение климата, эти две концепции все более тесно переплетаются между собой. Глобальная безопасность — это ситуация, при которой государства осознают, что их национальная безопасность зависит от безопасности других стран и что наилучший способ ее гарантировать — это многостороннее сотрудничество. В расширенное понятие глобальной безопасности также включают такие новые аспекты, как экономическая, продовольственная и социальная безопасность и поддержание здоровой окружающей среды. Все эти концепции самым тесным образом перекликаются с целями устойчивого развития Повестки дня до 2030 г.

Понятия стратегической стабильности и глобальной безопасности неразрывно связаны между собой. Укрепление глобальной безопасности возможно только посредством сотрудничества по глобальным вопросам и в отсутствие войны, что обеспечивает человеческую безопасность, то есть благосостояние людей. А этим критериям отвечает только стратегически стабильный миропорядок.

В ООН уверены, что глобальной безопасности и стратегической стабильности можно добиться только в рамках эффективного многостороннего подхода. Такой подход можно определить как коллективные межправительственные действия с использованием механизмов, учитывающих мнение всех заинтересованных сторон и обеспечивающих проведение надлежащего обсуждения перед принятием решения. Этот подход нацелен на то, чтобы у каждой страны, интересы которой могут быть затронуты, был голос в принятии решения. В этом смысле международное сообщество — это многосторонние коллективные действия. Такое видение было в очередной раз закреплено в принятой прошлой осенью резолюции

Первого комитета по продвижению многостороннего подхода в области разоружения и нераспространения (RES/A/70/31).

В последние годы многосторонний подход к вопросу разоружения столкнулся с определенными трудностями; соответствующие усилия в рамках ООН пока не приносят желаемых результатов. Однако нет сомнений в том, что вопрос перспективных технологий должен обсуждаться и решаться на самых широких площадках. Такие технологии потенциально могут поставить под удар мирное население, причем в намного большей степени, чем легитимные военные цели.

Поскольку эти технологии зачастую дешевле традиционных и легко ставятся на военные рельсы, они могут дать новые возможности как государственным, так и негосударственным игрокам, которые пока не обладают достаточным военным потенциалом для изменения сложившегося миропорядка. Силовые действия с применением перспективных технологий со стороны негосударственных игроков могут нарушить сложившийся силовой баланс — саму структуру миропорядка — и потенциально хрупкий стратегический баланс, а значит, подорвать глобальную безопасность. И этот вызов требует действительно коллективного реагирования.

Перспективные технологии могут изменить или подорвать существующую систему военного сдерживания, поскольку иногда очень сложно определить, кто стоит за агрессией с применением этих технологий, и дать пропорциональный ответ на такую агрессию в рамках принципов международного гуманитарного законодательства. В этом контексте встает другая важная нерешенная проблема в отношении перспективных технологий — это вопрос применимости к ним международного законодательства и существующих соглашений, принятых под эгидой ООН, эффективная работа которых наряду с балансом военных сил поддерживает стабильность международной системы. Являясь источником новых вызовов, перспективные технологии выводят на первый план недостатки существующей международно-правовой основы и могут поставить под вопрос фундаментальные принципы международного законодательства. Это относится и к международному гуманитарному законодательству, поскольку содержащиеся в нем определения понятий «применение силы», «суверенитет», «территория», «атрибуция», «вероломное нарушение обязательств», «пропорциональность» и т. д. не всегда хорошо уживаются с перспективными технологиями. Таким образом, возникает риск дестабилизации всей системы, поскольку юридические инструменты созданы для формирования общих ожиданий среди всех игроков с целью укрепления доверия между ними и сведения недоразумений к минимуму. В более широком смысле, само функционирование международного миропорядка будет меняться, если государства и негосударственные игроки изменят свою политику в силу выхода на сцену перспективных технологий.

И стратегическая стабильность, и глобальная безопасность во многом основаны на доверии. Потенциал двойного применения, который изначально присущ всем перспективным технологиям, может подорвать доверие и спровоцировать новую гонку вооружений. Следует также задаться вопросом о том, не положат ли перспективные технологии начало новому циклу наступательных действий в рамках теории нападения и обороны. Сегодня на нашей планете в основном царит мир, поскольку стоимость нападения, агрессии и односторонних действий намного превышает их потенциальную выгоду. Однако применение новых технологий потенциально может создать новую ситуацию, когда выгода от нападения растет, а риск сокращается. Даже если это впечатление на поверку окажется обманчи-

вым, оно может подтолкнуть государства и негосударственных игроков к более агрессивному поведению. В последний раз агрессивный курс наиболее выгодным представлялся ряду государств в 1914 г.

В этой связи уместно задаться вопросом о том, чем на самом деле являются перспективные технологии: новым тактическим преимуществом или роковым даром, который не приведет ни к чему хорошему? Новые типы вооружений теоретически дают разработавшему их государству преимущество над соперниками, поскольку они позволяют более эффективно нейтрализовать средства противника с помощью новых инструментов, слабые стороны которых пока не обнаружены. Однако данная теория не применима к кибер- и космическому оружию. Кибератака может дать тактическое преимущество агрессору, однако кибероружие бьет по уязвимостям, которые существуют в ИТ-системах как жертвы агрессии, так и самого агрессора, поскольку Интернет — эта единая сеть. Кибератака может вскрыть уязвимость в сетях соперника, однако впоследствии той же уязвимостью можно воспользоваться для атаки на сети самого агрессора. Поэтому обнаруженные уязвимости можно скрывать, чтобы разработать эксплуатирующие их вирусы и атаковать ИТ-инфраструктуру соперника, а можно их предать широкой огласке, чтобы укрепить кибероборону всех игроков. Это совершенно новая дилемма, которую нам придется решать.

СВЕСТИ К МИНИМУМУ ДЕСТАБИЛИЗИРУЮЩИЕ ЭФФЕКТЫ

Перспективные технологии, а некоторые из них еще не воплощены в реальную жизнь, уже поднимают сложные этические и правовые вопросы, требующие своевременного ответа от международного сообщества. И на данном этапе необходимо искать способы свести к минимуму дестабилизирующие эффекты перспективных технологий с помощью многосторонних инструментов. Среди возможных методов достижения этой цели можно выделить:

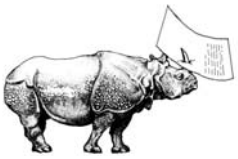
- укрепление международного законодательства с помощью групп правительственных экспертов;
- дальнейшее развитие мер прозрачности и укрепления доверия;
- сведение к минимуму реальной или кажущейся выгоды от агрессивных действий с применением новых технологий путем укрепления устойчивости систем, создания резервных систем и т. д.;
- совершенствование методов определения источников атак в киберпространстве.

Необходимо также акцентирование позитивного эффекта перспективных технологий и их вклада в достижение целей социального развития и укрепление глобальной безопасности.

Примечания

1 Текст комментария составлен на основе выступления г-на Ярмы Саревы на международной конференции «Повестка XXI в. — новые технологии и вызовы глобальной безопасности», организованной ПИР-Центром и Дипломатической академией МИД России 29 сентября 2016 г.

2 Collins Francis. Has the revolution arrived? *Nature*. 2010, 1 April. Vol. 464. P. 674.



Михаил Ковальчук, Олег Нарайкин

ПРИРОДОПОДОБНЫЕ ТЕХНОЛОГИИ — НОВЫЕ ВОЗМОЖНОСТИ И НОВЫЕ УГРОЗЫ

Движущей силой развития цивилизации являются глобальные (большие) вызовы. Эти вызовы определяют приоритеты научно-технологического развития, которые с точки зрения масштаба и глубины их влияния на социально-экономическое развитие делятся на две категории: тактические и стратегические. Тактические приоритеты определяют ближнесрочную перспективу, обеспечивая день сегодняшний. Стратегические приоритеты ориентированы на средне- и долгосрочную перспективу, обеспечивают создание принципиально новых прорывных технологий, приводят к смене технологического уклада. Важно соблюсти правильное соотношение между ними: в отсутствие тактических приоритетов будущее может не наступить, а отсутствие стратегических приоритетов лишает смысла решение тактических задач.

В качестве примера можно привести ситуацию, сложившуюся в конце Великой Отечественной войны. Советский Союз выиграл войну, реализуя тактические приоритеты, но новый *атомный вызов* задал новый стратегический приоритет. Если бы этот приоритет не реализовался, Победа была бы полностью обесценена! Результатом реализации стратегического моноприоритета стал новый технологический облик страны как мировой сверхдержавы.

Сегодняшняя ситуация совершенно аналогична. Отличие лишь в глубине и в масштабах последствий современных глобальных вызовов по сравнению с атомным.

Глобальный вызов XXI века связан с необходимостью обеспечения устойчивого развития цивилизации. Базовым условием такого развития является достаточное количество энергии и ресурсов. Причем речь идет не только о нефти и газе: истощаются запасы питьевой воды, пахотных земель, леса, полезных ископаемых. За них уже идет острая борьба, во многом ставшая доминантой мировой политики.

Важно подчеркнуть, что лидерство сегодня обеспечивается не прямой военной силой, а технологическим превосходством, подкрепляемым прямой военной силой. То есть военная колонизация сменилась технологической, и объектами такой колонизации могут быть не только государства третьего мира, но и развитые страны.

Мы построили комфортную для человека цивилизацию, техносферу, паразитируя на базе и ресурсах биосферы Земли, которая существовала миллионы лет до появления в ней человека абсолютно самодостаточно и гармонично. Индустриальная же цивилизация всего лишь за 200 лет своего существования поставила мир на порог ресурсного коллапса. Приведем лишь один пример: за антропогенную историю было израсходовано примерно 200 млрд тонн кислорода. Такое же количество кислорода было израсходовано за последние 50 лет индустриальной эры.

Причиной сложившейся кризисной ситуации является антагонизм природы и созданной человеком техносферы. Технический прогресс нарушил естественный ресурсооборот — своеобразный обмен веществ природы, создав технологии, враждебные ей. Эти технологии, будучи вырванными из естественного природного контекста, по сути являются плохими копиями отдельных элементов природных процессов и базируются на узкоспециализированной модели науки и на отраслевых технологиях.

В целом такое развитие было неизбежно и закономерно, но в итоге масштабы влияния человека на окружающий мир перешли критическую границу. При этом в условиях глобализации в технологическое развитие, а следовательно, и в истребление ресурсов, вовлекаются все новые страны и регионы, подводя мир на грань катастрофы. Есть ли в этих условиях у нашей цивилизации шансы на дальнейшее развитие, на будущее?

Все чаще звучит мысль о том, что сегодняшний глобальный кризис не может быть разрешен по прежним фундаментальным *лекалам* нашей цивилизации, в существующей парадигме ее развития. Нужен качественный скачок, переход на иные принципы прежде всего производства и потребления энергии, которые изменят облик всей техносферы.

Современные технологии требуют колоссального количества энергии, которое существующая альтернативная энергетика не способна выработать в принципе. Выйти из этого технологического тупика поможет наука, которая уже сегодня дает возможность создавать принципиально новые технологии генерации и потребления энергии по образцу живой природы — *природоподобные* технологии.

Смысл создания *природоподобной* техносферы состоит в восстановлении естественного самосогласованного ресурсооборота, нарушенного сегодняшними технологиями, вырванными из естественного природного контекста. Инструмент создания такой техносферы — конвергентные нано-, био-, информационные, когнитивные и социогуманитарные технологии (НБИКС-технологии).

Самое совершенное творение природы — человеческий мозг — потребляет не более 30 Ватт, а современная суперЭВМ — десятки мегаватт. При этом эффективность всех компьютеров мира не достигает эффективности мозга среднестатистического человека. Выход из положения — создание компьютеров, работающих на принципах человеческого мозга.

Таким образом, стратегическая цель современной цивилизации — включить технологии в естественный природный ресурсооборот на базе развития интегрированной междисциплинарной науки.

Интеграция и междисциплинарность в наше время являются определяющей тенденцией развития научной сферы, и в этом смысле природоподобные технологии — закономерный этап естественного развития науки и технологий: через междисциплинарность к конвергенции и природоподобию.

Сегодня бóльшая часть всех мировых исследований приходится на живые объекты. Нанобиотехнологии, по сути, уже стали новой технологической культурой, где на атомарном уровне стираются грани между живым и неживым, между органическим природным миром и неорганикой. Созданные на основе этих технологий новые материалы и системы уже используются в медицине, энергетике, экологии, на транспорте и т. д. Следующий этап — воспроизведение систем и процессов живой природы в виде синтетической клетки, массового создания искусственных тканей и органов.

Аддитивные технологии уже сейчас позволяют создавать биоорганические объекты, используя природный принцип формирования, выращивая их *под заказ*.

Наряду с аддитивными технологиями активно развивается биоэнергетика, в частности разрабатываются биоэнергетические устройства, которые вырабатывают и потребляют энергию, используя естественные метаболические процессы в живых системах. Следующим шагом может стать создание искусственного интеллекта для биоподобных и синтетических биологических объектов на основе достижений когнитивных и информационных технологий.

Все это постепенно сформирует базу для природоподобной техносферы, которая станет органической частью природы, включенной в ее естественный ресурсооборот. Она способна не только сохранить цивилизацию, но и дать толчок к ее развитию на принципиально ином уровне. Однако есть принципиальное условие: без изменения нашего сознания, отношения к цивилизации, природе и к самому себе эти перспективы могут остаться ничем. Это придает особое значение социогуманитарному измерению конвергенции наук и технологий.

Исследования и разработки по созданию природоподобных технологий активно ведутся в ряде зарубежных стран. В частности в США, в странах Европейского союза, в Японии и в других реализуются сотни проектов в этой области.

Первым ответом нашей страны на стратегический вызов XXI века стала президентская инициатива «Стратегия развития наноиндустрии», два этапа которой были успешно реализованы в 2007–2015 гг. В качестве задачи третьего этапа, начавшегося в 2016 г., указано «опережающее развитие принципиально новых направлений… обеспечивающих создание в стране надотраслевой научно-образовательной и производственной среды в перспективе на ближайшие 10–20 лет…

Главным содержанием этого этапа станут разработка и создание:

- продукции нанобиотехнологий;
- гибридных устройств и приборов бионического типа;
- нанобиосистем и устройств, включая принципиально новые гибридные системы очувствления бионического типа;
- биоробототехнических систем.

Реализация задачи третьего этапа приведет к созданию принципиально нового технологического базиса экономики в Российской Федерации»[1].

Таким образом, главный вектор, задающий направление научно-технологического развития, определен. В ходе реализации первых двух этапов президентской инициативы «Стратегия развития наноиндустрии» была заложена идеологическая (интеллектуальная), кадровая и инфраструктурная база для развития природоподобных, конвергентных НБИКС-технологий.

В частности создан уникальный, не имеющий прямых аналогов в мире центр конвергентных наук и технологий — Курчатовский НБИКС-центр. В этом центре на мировом уровне проводятся исследования и разработки по всему спектру конвергентных наук и технологий. Сформирована инновационная научно-образовательная система междисциплинарной подготовки кадров, включающая первый в мире факультет нано-, био-, инфо-, когнитивных технологий (ФНБИК) в Национальном исследовательском университете МФТИ. В соответствии с поручением Президента Российской Федерации разработан проект президентской инициативы «Стратегия развития конвергентных технологий», которая определяет базовые элементы и принципы формирования такой системы.

Однако природоподобные технологии, давая человечеству шанс избежать ресурсного коллапса, определяют вместе с тем принципиально новые глобальные угрозы и вызовы. Эти угрозы связаны с самим характером природоподобных технологий, построенных на возможности технологического воспроизведения систем и процессов живой природы. Эта возможность открывает перспективу целенаправленного вмешательства в жизнедеятельность природных объектов, прежде всего человека и, впервые в истории, в процесс его эволюции.

Такое вмешательство по используемой технологической базе и методам воздействия можно разделить на два важнейших типа:

- биогенетическое, базирующееся на применении методов нанобиотехнологий;
- когнитивное, основанное на конвергенции инфокогнитивных и социогуманитарных наук.

Первый уже сегодня реализуется в технологиях так называемой синтетической биологии, позволяющих продуцировать искусственные живые системы с заданными свойствами, в том числе не существующие в природе.

Базовым элементом таких систем является искусственная клетка, обладающая минимально необходимым набором генов, достаточным для жизни и размножения. На основе такой клетки могут быть созданы как сверхэффективные лекарства, так и средства поражения.

Показательным примером новых угроз, связанных с созданием искусственных живых систем, является возможность появления новых видов наркотических средств. Так, непригодный для получения морфина природный прицветниковый мак может быть превращен в его продуцент и использован для получения наркотиков.

Второй тип вмешательства связан с воздействием на психофизиологическую сферу человека с целью контроля и управления его сознанием и телом. Активно разрабатываются принципиально новые мозго-машинные и мозго-мозговые

интерфейсы, позволяющие формировать у человека заданное представление о действительности.

В повестке дня — создание интегрированных человеко-машинных систем, управляемых извне. Существующая уже сегодня сетевая технологическая база (интернет) позволяет достаточно эффективно управлять как индивидуальным, так и массовым сознанием, используя интегрированные технологии инфокогнитивных и социогуманитарных наук.

Риски, сопровождающие создание и развитие природоподобных технологий, многократно увеличиваются в силу ряда специфических особенностей, присущих последним.

Важнейшими из них являются:

- двойственный характер технологий, размытые границы между гражданскими и военными применениями и, как следствие, неэффективность существующих средств и технологий контроля;
- доступность и относительная дешевизна технологий, возможность создания средств поражения даже в кустарных условиях, отсутствие необходимости в сложнейших и чрезвычайно дорогостоящих системах доставки;
- невозможность предугадать все последствия выхода искусственных живых систем в окружающую среду.

Ярким примером непредсказуемости последствий выхода искусственных живых систем в окружающую среду является вытеснение ими своих природных аналогов, что ставит под угрозу естественное биоразнообразие. В частности в Индии, в США и в Канаде зафиксированы случаи передачи от генно-модифицированных растений к дикорастущим видам устойчивости к гербицидам, что превратило их в *суперсорняки*.

Традиционно человечество следовало модели контроля результата технологической деятельности — достаточно вспомнить режимы нераспространения ядерного, химического и бактериологического оружия. В случае с конвергентными, природоподобными технологиями контроль необходим уже на этапе развития этой новой технологической структуры, поскольку контроль результата может оказать несвоевременным — запоздать.

В этих условиях возникает угроза глобальной безопасности, связанная с возможностью одностороннего владения технологиями указанного класса и их использования, в том числе экстремистскими группировками.

Это требует консолидации усилий мирового сообщества для формирования новой международной системы, которая бы обеспечила безопасное контролируемое развитие природоподобных (конвергентных) технологий. Эта система должна базироваться на новом принципе: контроль над технологиями, а не над вооружениями!

Именно об этом говорил Президент Российской Федерации В. В. Путин в своем выступлении на 70-й сессии Генеральной Ассамблеи ООН 28 сентября 2015 г.: «…Нам нужны качественно иные подходы. Речь должна идти о внедрении принципиально новых природоподобных технологий, которые не наносят урон окружаю-

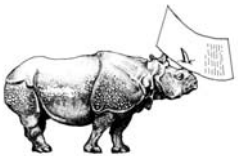
щему миру, а существуют с ним в гармонии и позволят восстановить нарушенный человеком баланс между биосферой и техносферой. Это действительно вызов планетарного масштаба...

Нам необходимо объединить усилия и прежде всего тех государств, которые располагают мощной исследовательской базой, заделами фундаментальной науки. Предлагаем созвать под эгидой ООН специальный форум, на котором комплексно посмотреть на проблемы, связанные с исчерпанием природных ресурсов, разрушением среды обитания, изменением климата...»[2].

Примечания

1 Президентская инициатива «Стратегия развития наноиндустрии». 24 апреля 2007 г. Сайт Российская национальная нанотехнологическая сеть http://www.rusnanonet.ru/download/nano/20070424_strategy_688.pdf (дата последнего посещения — 29.12.2017).

2 Выступление Президента России Владимира Путина на пленарном заседании 70-й сессии Генеральной Ассамблеи ООН 28 сентября 2015 г. Сайт президента России http://kremlin.ru/events/president/news/50385 (дата последнего посещения — 29.12.2017).



Владимир Легойда

МОЖЕТ ЛИ ТЕХНОЛОГИЯ БЫТЬ БЕЗНРАВСТВННОЙ, А РЕЛИГИЯ СТОЯТЬ НА ПУТИ РАЗВИТИЯ НАУКИ? ВЗГЛЯД ЦЕРКВИ[1]

Есть три основных способа познания мира человеком: наука, религия и искусство. Наука позволяет человеку рационально познавать окружающую среду. Через искусство человек реализует свою потребность художественным способом познать себя, «прожить» разные жизненные ситуации. Религия — тоже способ познания мира, но не посредством изучения физического мира, в котором живет человек. По большому счету в познании законов материального мира религия не очень заинтересована. Но религия — это не вымысел, не уход из реального мира в придуманный художником, а ответ на самый главный и сложный вопрос: что такое смерть?

Человек приходит в этот мир, который не создавал, помимо своей воли, и уходит из него тоже без учета его желания. Если в приходе в этот мир, существовании и уходе есть какой-то смысл, то этот смысл, говорят религии, должен быть внеположен человеку и миру. Человек не может найти ответ на вопрос о природе смерти, изучая окружающую среду посредством науки, потому что наука отвечает на вопросы «как?» и «почему?». Условно говоря, даже если ученые смогут когда-то ответить на вопрос, как на Земле появилась органическая жизнь, они никогда не ответят на вопрос, для чего она появилась? Этот вопрос выходит за пределы компетенции науки. Ученый перестает быть ученым, когда начинает отвечать на вопрос о целеполагании: «для чего?» — не этим вопросом задается ученый. Исследователи отвечают на вопрос «как?», они устанавливают причинно-следственные связи. В мировоззренческом смысле вопросы о целеполагании относятся к религиозному дискурсу, а не к научному. Соответственно, наука, религия и искусство позволяют человеку воспринимать и познавать мир на разных уровнях, а это означает, что между этими тремя сферами нет сущностного конфликта. Между тем стереотип о неизбежном конфликте между религией и наукой давно стал общим местом.

ДОКАЗАТЕЛЬСТВА ОТ КОСМОНАВТОВ. К ИСТОРИИ КОНФЛИКТА НАУКИ И РЕЛИГИИ

Наследие эпохи Просвещения и советской эпохи предлагает упрощенное понимание моделей взаимодействия религии и науки — об этом говорил патриарх

Кирилл, выступая на круглом столе в федеральном ядерном центре в Сарове[2], где присутствовали ученые из федерального научного центра и из других научных институтов страны. Патриарх выразил обеспокоенность существованием упрощений, направленных как против религии, так и как бы в пользу нее. Таким образом, проблема неверного толкования отношений между наукой и религией не сводится лишь к поиску области их прямого конфликта.

Упрощение, направленное против религии, представляет отношения науки и религии в виде конфликта сути. Такое представление основано на сложившейся в XIX в. точке зрения о том, что религия родилась из страха, который может быть развеян путем обретения знания. Считалось, чем больше человек знает, тем меньше он боится, а значит, религия отомрет за ненадобностью. С тех пор человечество узнало многое, а религия не отмерла, потому что вопрос о смерти до сих пор актуален. Это доказывает мысль о том, что наука и религия представляют разные способы познания мира, и конфликта сути между ними быть не может.

Вместе с тем конфликты между наукой и религией или искусством и религией действительно возникают, но они не отражают содержательные противоречия между искусством и наукой, а также религией и наукой. Они являются результатом того, как взаимные отношения этих трех сфер воспринимаются обществом. Наиболее часто конфликт в восприятии возникает в том случае, когда наука соприкасается с моральными измерениями, например, когда результаты научных открытий начинают внедряться в общественную жизнь. Хотя предмет науки и не соотносится с моралью, итоги научной деятельности оцениваются с ее позиций: например, насколько допустимо применять ядерное оружие? Аналогичным образом проявляется конфликт между искусством и религией — в виде реакции общества на художественные произведения.

Упрощение, направленное в пользу религии,— упрощение, свойственное нынешнему времени, — это представление о том, что наука и религия непременно должны дополнять друг друга, поскольку между ними отсутствует конфликт. Такая точка зрения относится и к упрощениям, потому что на одном уровне рассматривает явления, находящиеся в разных эпистемологических плоскостях. Следуя этой логике, в один ряд можно поставить христиан, мусульман, буддистов и физиков, — и все они непременно должны будут взаимодействовать друг с другом. Абсурдность этого примера показывает, что прямого взаимодействия двух разных систем не может быть, как не может быть между ними и конфликта. Патриарх Кирилл, выступая в Сарове, описал это упрощение так: «Если раньше пытались доказать, что Бога нет, так как Его не видели космонавты, теперь, образно говоря, с помощью тех же космонавтов пытаются доказать, что Бог есть»[3]. Такая методология не имеет отношения к содержанию религии, хотя открытия, определенные развитием науки в XX в., значительно повлияли на развитие богословской и гуманитарной мысли. К таким открытиям можно отнести принцип дополнительности, сформулированный Бором, принцип относительности, теорему Геделя о неполноте. Все эти принципы, открытые физиками и математиками, заставили ученых-гуманитариев, в том числе богословов, переосмыслить ряд общепринятых положений.

Рассмотрев эти два упрощения, можно сказать, что наука и религия, разные инструменты познания мира и человека, дополняют друг друга в представлении человека о мире и делают его картину мира более яркой и объемной. Однако это взаимодополнение происходит не на пересечении пространств науки и религии, потому что наука и религия стремятся ответить на разные вопросы.

НЬЮТОН ПРОТИВ АНТИЧНОГО ГРЕКА — РОЛЬ ХРИСТИАНСТВА В СТАНОВЛЕНИИ НАУКИ

Помимо упомянутых упрощений, восприятию взаимоотношений науки и религии присущ еще один стереотип — идея о том, что наука ответственна за секуляризацию общества, что именно она вытесняет религию на периферию. Этот стереотип относится к наследию эпохи Просвещения. Тогда считалось, что наука — это настоящее понимание мира, а религия — ненастоящее, иллюзорное, и именно поэтому чем больше науки будет в обществе, тем меньше там останется религии.

Вместе с тем христианство внесло значительный вклад в становление науки. Христианство не ставило своей целью создание научной картины мира, но именно благодаря тем мировоззренческим установкам, которые возникли в христианстве, появилась европейская наука в современном понимании. По канонам современности, деятельность ученых в эпохи, предшествующие Новому времени, наукой не является. Почему же считается, что наука возникла не в античной Греции, хотя у греков уже существовала математика?

Серьезным научным поворотом Нового времени стало появление естествознания и объединение физики с математикой. Ньютон создал современную науку, потому что он первым в истории европейской культуры вывел механическую модель мира, то есть физическую модель мира на языке математики. Декарт сравнивал организм с механизмом, говоря, что они работают по схожим признакам — отличие лишь в том, что механизм нужно заводить, а организм самозаведен. Этот серьезный мировоззренческий вывод был недоступен античному греку, поскольку в античной мировоззренческой системе физика и математика — две непересекающиеся плоскости. Античное мировоззрение исходило из языческих установок, в которых не существовало идеи творения, а значит, и идеи замысла — там было четко разведено то, что существует в живой природе, и то, что сотворено человеческими руками, то есть математика и физика мыслились отдельно. Наука смогла прийти к механической модели мира только в XVI–XVII вв., потому что когда-то христианство вывело формулу: «У мира есть творец, а мир есть результат замысла и творения». Через несколько веков эта христианская революция в мировоззрении привела к научному результату.

В обсуждениях взаимоотношений между наукой и религией часто всплывает тема соотношения религии с идеей научного прогресса. С одной стороны, есть представление о неизбежности положительного движения науки. С другой — есть образ ретроградной церкви, которая все время пытается помешать движению научного прогресса. Какова позиция церкви по этому вопросу?

Сама идея прогресса появилась в культуре уже после того, как возникла идея линейности истории — то, что называется *стрелой времени*. Идея *стрелы вре-*

мени сначала утвердилась в древнееврейской традиции, а потом в христианской и исламской культурах. Все эти традиции говорят о том, что у мира есть начало, есть направление движения и, скорее всего, считается в этих религиях, будет конец. Окончание любого процесса указывает на наличие смысла в нем — и в христианстве, и в исламе, в иудаизме есть концепции, которые об этом смысле говорят.

В античный период греки представляли время иначе — скорее, в виде диска, вращающегося вокруг своей оси. Примечательный пример: греки не фиксировали результаты спортсменов на Олимпийских играх — они не видели в этом смысла, потому что в их мировоззрении любое событие повторялось по кругу. Понимание необходимости фиксировать текущий результат для сравнения его с будущим показателем появилось только с приходом к идее о линейности времени. А идея о линейной временной направленности как мировоззренческая категория возникла только с распространением христианства. Иначе говоря, если бы не произошла христианская мировоззренческая революция, в культуре не появилась бы идея прогресса в широком смысле, а значит, и понятие научного прогресса.

МНЕ ВСЕ РАВНО ИЛИ НЕТ? ПОЛЬЗОВАНИЕ–АНОНИМНОСТЬ–ЗЛОУПОТРЕБЛЕНИЕ

Если обращаться непосредственно к вопросу отношения церкви к технологиям, некие опасения в самой церковной среде и вне ее действительно существуют, но они не имеют отношения к самим технологиям. Богословское отношение к тому, что происходит в технологическом мире таково: технологии необходимы для выживания человека. Для христианства водоразделом в истории человечества являются факт грехопадения Адама и Евы и их изгнание из рая. Что это значит, если попытаться перевести эту историю с символического языка священной книги? Высшее творение Господа — человек — первоначально находился с Богом в определенных отношениях, в которых затем произошел катастрофический разрыв. Адам съел запретный плод и спрятался, то есть в отношениях Адама с Богом появился страх, которого не было раньше. Изменились также отношения человека с человеком: после грехопадения Адам и Ева начинают стыдиться друг друга, закрываются друг от друга одеждой, хотя раньше, как сказано в Библии, «и были оба наги, Адам и жена его, и не стыдились» (Быт. 2:25). В условиях Рая, для которых человек был задуман другим, после грехопадения Адам и Ева выжить уже не могли, поэтому Бог спасает их, изгоняя из Эдемского сада. Дальнейшее выживание человека, согласно логике библейского повествования, неизбежно связано, говоря современным языком, с развитием технологий. Поэтому глобальное отношение христианства к любой технологии, вне зависимости от того, колесо это, самолет или социальная сеть, одинаково и не меняется с течением времени.

Это отношение определяется классическим противопоставлением — богословие делит применение технологических инструментов на пользование и злоупотребление. Классический святоотеческий пример говорит, что ножом можно нарезать хлеб, а можно убить человека. Является ли нож сам по себе добром или злом? Не является: моральный результат его применения определяется оппо-

зицией — использованием или злоупотреблением инструмента, который сам по себе нейтрален. Этот богословский принцип универсален — он относится к любому технологическому инструменту.

Справедливости ради стоит упомянуть, что в рамках современного православного богословия существуют и другие точки зрения. В частности греческий митрополит Иоанн Зизиулас говорит о том, что некоторые современные информационно-технологические открытия уже по своей природе ни к чему хорошему приспособлены быть не могут. Можно встретить православных общественников, которые будут говорить про компьютер-зверь, который находится в Брюсселе и может уничтожить все человечество. Однако с классической богословской точки зрения любая технология нейтральна и обретает окраску уже в момент применения.

В рамках дискуссионной площадки межсоборного присутствия Русской Православной Церкви существует задача оформить отношение церкви к информационно-коммуникативным технологиям в форме документа. На повестке дня стоит тема антропологических рисков и опасностей, которые у человека возникают в связи с развитием информационных технологий. По результатам проводимых дискуссий причины антропологических рисков видятся участникам споров не в религиозных вещах, а, например, в возможности поражения человека в правах.

Большинство технологических вопросов, по которым Русская Православная Церковь старается выработать свою позицию, она рассматривает в рамках оппозиции «пользование–злоупотребление». Например, в отношении электронной системы учета и контроля для церкви неважно, по каким причинам гражданин желает остаться с бумажным паспортом, но значимо, чтобы государство гарантировало отсутствие ущемления прав для тех граждан, которые не хотят принимать электронную систему учета.

Вопрос же о нравственной составляющей распространения технологий встает главным образом в связи с виртуализацией. Сама по себе проблема виртуального — виртуальное действие не происходит в полной мере — усугубляется тем, что оно может твориться анонимно. Достоевский в произведении «Сон смешного человека» задавался вопросом: «Мне вдруг представилось одно странное соображение, что если б я жил прежде на Луне или на Марсе и сделал бы там какой-нибудь самый срамный и бесчестный поступок, какой только можно себе представить, и был там за него поруган и обесчещен так, как только можно ощутить и представить лишь разве иногда во сне, в кошмаре, и если б, очутившись потом на земле, я продолжал бы сохранять сознание о том, что сделал на другой планете, и, кроме того, знал бы, что уже туда ни за что и никогда не возвращусь, то, смотря с Земли на Луну, — было бы мне все равно или нет? Ощущал ли бы я за тот поступок стыд или нет?»[4]. Современный богослов Сергей Карузин предположил, что возможность анонимности в современном интернет-диалоге может быть своего рода предсказанием Достоевского — разница только в том, что сегодня необязательно быть на Луне, чтобы совершить вещественный поступок, авторство которого будет ото всех сокрыто. Анонимность в виртуальном взаимодей-

ствии и является проблемной зоной, которую можно выделить как нравственную проблему в вопросе с информационными технологиями.

Природоподобные технологии и воспроизводство природоподобных вещей с точки зрения Церкви не представляют нравственную проблему. В технологиях, направленных на совершенствование человека, для церкви нет ничего предосудительного до тех пор, пока разговор идет о помощи человеку, когда он, например, потерял руку или органы. Однако современные теории трансгуманизма, говорящие о возможности создания другого человека, претендуют на роль человека как творца. И это не может не беспокоить церковь. 

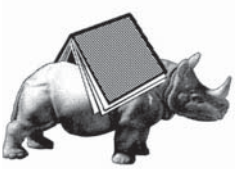
Примечания

1 Комментарий составлен на основе выступления В. Р. Легойды на Международной Школе по проблемам глобальной безопасности 1 октября 2016 г.

2 Слово Святейшего Патриарха Кирилла на встрече с учеными в Сарове, 1 августа 2016 г., http://www.patriarchia.ru/db/text/4579909.html (последнее посещение — 20 декабря 2016 г.).

3 Там же.

4 Достоевский Ф. М. Сон смешного человека, цит. по.: http://az.lib.ru/d/dostoewskij_f_m/text_0330.shtml (последнее посещение — 18 декабря 2016 г.).



ОБ ИКТ, НЕ РАСТЕКАЯСЬ МЫСЛЬЮ ПО ДРЕВУ, — ПРОБЛЕМЫ, ЦЕЛИ И, ГЛАВНОЕ, РЕКОМЕНДАЦИИ

Олег Демидов. Глобальное управление Интернетом и безопасность в сфере использования ИКТ. Ключевые вызовы для мирового сообщества. М.: ПИР-Пресс, Альпина Паблишер. 2016. 198 с.

Рецензия — Елена Волчинская

Олег Демидов, работая в ПИР-Центре, более пяти лет занимается вопросами глобальной безопасности в сфере использования информационно-коммуникационных технологий (ИКТ). Он известен как информированный эксперт и думающий человек. Поэтому выход этой книги представляет безусловный интерес для всех, кто понимает, какие глобальные преимущества и, одновременно, какие глобальные вызовы национальной и международной безопасности несет применение ИКТ.

Книга отличается сжатым содержательным текстом, информативность обеспечивается привлечением большого количества разнообразных источников, а анализ тенденций и проблем в сфере использования ИКТ сопровождается выводами и предложениями. Книга написана очень хорошим, богатым русским языком, который нынче, к сожалению, в дефиците не только в публицистике, но и в научной литературе.

Структура монографии позволяет автору обратить внимание читателя на важные аспекты повестки дня — рассмотрение ИКТ в качестве критического фактора глобального развития. К ним относятся прежде всего вопросы безопасности в развитии и применении ИКТ, угрозы бесперебойному функционированию объектов критической информационной инфраструктуры и стратегии реагирования на эти угрозы, правовые и политические проблемы глобального управления интернетом, а также защита права на частную жизнь в Сети.

Каждый из восьми разделов книги построен по единой схеме: на основе анализа ситуации постулируются основные проблемы и формулируются цели и рекомендации. Эта жесткая конструкция не позволяет автору *растекаться мыслью по древу*, дисциплинирует повествование и является, по моему мнению, одним из достоинств монографии. Другое достоинство — редкая для такого издания актуальность привлекаемого материала. Наконец в качестве главного достоинства я бы определила авторские рекомендации (предложения). Они представляют интерес даже в том случае, если читатель с ними не соглашается. Остановлюсь на некоторых из них.

В разделе I «ИКТ — критический фактор глобального развития» автор справедливо, на мой взгляд, указывает на необходимость формирования на государственном уровне режима максимального благоприятствования для ИКТ-сектора.

В последнем обращении к Федеральному Собранию Президент России Владимир Путин впервые поставил задачу «запустить масштабную системную программу развития экономики нового технологического поколения, так называемой *цифровой экономики*[1]». При реализации этой программы приоритет будет отдаваться российским компаниям, а также научным, исследовательским и инжиниринговым центрам страны. Подобная постановка вопроса вселяет надежды. Однако многое будет зависеть от способа реализации амбициозных задач. К сожалению, необходимо признать, что институциональные механизмы формирования и реализации государственной политики в области развития и применения ИКТ недостаточно эффективны. В связи с этим содержащиеся в книге предложения о необходимости создания межведомственной координационной площадки для диалога между многочисленными регуляторами сферы ИКТ представляются целесообразными.

Анализируя проблемы выработки единых подходов к обеспечению безопасности при использовании ИКТ, автор обращает внимание на принципиальные разногласия в терминологии, имея в виду различия в содержании понятий *кибербезопасность* (используется в документах США, стран Европы, ряда стран Азии, НАТО, ОБСЕ, ОЭСР и др.) и *информационная безопасность* (используют Россия, СНГ, ШОС, ОДКБ). Автор понимает, что проблема разных подходов только внешне выглядит терминологической, на деле же она глубже, системнее. Автор книги предлагает, в частности, в целях ухода от терминологического конфликта применять нейтральный термин *обеспечение безопасности при использовании ИКТ*, который используется группой правительственных экспертов ООН в резолюциях Генеральной Ассамблеи ООН. Вместе с тем автор высоко оценивает опыт работы экспертного сообщества под эгидой Совета Федерации над проектом стратегии кибербезопасности Российской Федерации. Этот документ так и остался в статусе проекта, он не был поддержан органами государственной власти и частью экспертов. Но терминологические разногласия не были единственной и, тем более, определяющей проблемой. Например, я в своем отзыве на проект стратегии обращала внимание на недостаточную конкретизацию круга проблем, на решение которых направлен проект, на внутренние противоречия при формулировании направлений обеспечения кибербезопасности, а также на недостаточно продуманные принципы стратегии и механизмы координации деятельности по ее реализации. Наконец, в проекте не была обоснована целесообразность разработки стратегии кибербезопасности — нового доктринального документа, который был задуман как самостоятельный документ наряду с уже имеющимися. Полаю, что опыт создания стратегии подобного уровня был интересен и полезен для участников процесса, однако, к сожалению, для большинства из них этот опыт был первым, а он редко бывает удачным.

Представляется, что в процессе формирования и реализации государственной политики в сфере ИКТ необходимо обеспечить баланс интересов как минимум трех групп субъектов: государства, производителей ИКТ и связанных услуг, а также пользователей технологий. Так, принцип баланса интересов был провозглашен еще на Тунисском этапе Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО). Принцип замечательный, но его реализация оказалась сложной задачей. Рассуждая о том, как этот принцип может быть реализован, Олег Демидов задается вопросом: «Нужен ли сообществу российских интернет-пользователей собственный представитель, наделенный полномочиями

и имеющий доступ к публичным каналам выражения мнений?» (с. 29). Создание поста советника Президента России по вопросам развития интернета и назначение на этот пост Германа Клименко рассматривается как необходимый, но недостаточный шаг. С этой позицией я соглашусь, поскольку в существующих реалиях советник не имеет полномочий — по крайней мере он сильно проигрывает в статусе аналогичной фигуре в администрации президента США. Однако далее Олег Демидов, отвечая на свой вопрос, предлагает в качестве «условного прототипа» коллективного представителя российское общественно-политическое объединение «Пиратская партия». По моему мнению, эта организация не ставит перед собой задачу достижения баланса интересов или поиска компромисса. На мой взгляд, вопрос обеспечения баланса интересов даже не заключается в выборе конкретного ответственного субъекта, который бы представлял интересы интернет-сообщества. Убеждена, что внимание стоит сконцентрировать на выстраивании процесса принятия решений, в рамках которого: а) появится возможность представлять различные интересы; б) будут существовать механизмы их отстаивания; в) представители разных субъектов смогут участвовать в выработке проектов решений. Последний пункт представляется актуальным, поскольку в настоящее время большинство таких решений принимается кулуарно в органах власти, а экспертные советы Минкомсвязи России практически не работают. Кроме того, информация о готовящихся решениях иногда появляется слишком поздно, тексты проектов на портале regulation.gov.ru[2] размещаются в неактуальной редакции, а стадия разработки законопроектов зачастую указывается неверно. В таких условиях о балансе интересов говорить не приходится.

Подробно освещаемые в книге вопросы кибербезопасности объектов критической информационной инфраструктуры (КИИ) получили в настоящее время особую актуальность в связи с внесением в Государственную Думу 6 декабря 2016 г. пакета законопроектов, разработанных и направленных на обеспечение безопасности КИИ России. В базовом законопроекте под КИИ Российской Федерации понимается совокупность объектов КИИ, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой. Таким образом, российская терминология относит телекоммуникационные системы, сети и системы связи к КИИ, так же как и в других странах. В связи с этим к значимым объектам КИИ предъявляются повышенные требования по обеспечению их безопасности.

Автор делает акцент на вопросах международного взаимодействия в сфере обеспечения безопасности КИИ, справедливо полагая, что выработка базовых механизмов обмена информацией об угрозах безопасности объектов КИИ, а также формирование общей системы классификации таких объектов будут способствовать повышению эффективности их систем безопасности. Достижение результатов в этой сфере отвечает интересам всего мирового сообщества, потому что эффект техногенных катастроф, вызванных атаками на системы управления объектами КИИ, выходит за рамки границ одного государства.

Конечно, автор не мог обойти вниманием вопросы использования ИКТ в военно-политических целях. Обсуждение подобных угроз ведется достаточно давно, а в настоящее время можно наблюдать, как они стали воплощаться в реальность. Тем не менее говорить о существовании компьютерных войн преждевременно, поскольку, как верно указывает Олег Демидов, «использование ИКТ в военно-обо-

ронительных целях не охвачено какой-либо системой международных договоров, конвенций или иных соглашений» (с. 100). Это означает, что любая квалификация компьютерных инцидентов как военных конфликтов уязвима с точки зрения международного права. Конечно, отсутствие признанных классификаций зачастую не останавливает акторов от использования подобных определений. Недавний пример: администрация США обвинила российских хакеров в проигрыше Демократической партии на выборах президента Соединенных Штатов.

Несмотря на альтернативные подходы к развитию норм международного права, в конечном итоге все акторы заинтересованы в том, чтобы был принят юридически обязательный международный документ, направленный на запрет и предотвращение использования ИКТ в военно-политических целях. Однако автор книги считает, что принятие такого международного акта вряд ли возможно, пока не решены вопросы атрибуции, т. е. пока не выработаны критерии для квалификации использования ИКТ в качестве средства вооруженного нападения в определении статьи 52 Устава ООН. Олег Демидов предлагает *тактику малых шагов*, позволяющую максимально адаптировать существующие основополагающие нормы международного права, включая Устав ООН, нормы международного гуманитарного права и права вооруженных конфликтов для использования этих положений в разрешении вопросов военного использования ИКТ. Не отрицая целесообразность такой деятельности, я все же не соглашусь с тем, что подобных усилий будет достаточно. Занимаясь вопросами правового регулирования сферы ИКТ, я нередко убеждалась в том, что привычные нормы права дают сбой и не работают в виртуальной реальности. Это касается как национального законодательства, так и международного права. По этой причине создание новых норм международного *компьютерного права* наряду с возможным развитием и адаптацией норм международного гуманитарного права не только полезно, но и необходимо.

Два раздела книги посвящены проблемам глобального управления Интернетом. Автор подробно анализирует функции основных технических организаций глобального интернет-сообщества, так или иначе участвующих в управлении Интернетом, а также трансформацию подходов к его управлению за последние 10–15 лет. При этом в качестве одной из тенденций рассматривается нарастающее присутствие государства в Сети. В России эта тенденция очевидна — доказательством тому служит обнародованный в 2014 г. проект Минкомсвязи России, который предусматривает, по словам российского интернет-омбудсмена Дмитрия Мариничева, возможность отключения Рунета от глобальной сети при определенных условиях. «Речь идет не о каких-либо блокировках и ограничении доступа к интернет-ресурсам, а о выработке плана действий в экстренных случаях»[3], — сообщил представитель Минкомсвязи России, комментируя появившуюся в СМИ информацию. Несмотря на отсутствие признанных определений международных компьютерных преступлений, как указывает Олег Демидов, мы действительно являемся свидетелями использования ИКТ в военно-политических целях, в целях экономического шпионажа и иных противоправных целях, и это неизбежно стимулирует страны к разработке защитных мер на государственном уровне.

Тема защиты персональных данных в Сети и, шире, защиты права на тайну частной жизни в течение 10 лет после принятия Федерального закона «О персональных данных» не покидает повестку дня в России. Автор анализирует, как изменилось понимание этой проблемы после разоблачений Эдварда Сноудена 2013 г. и утвержда-

ет, что международно-политический итог этих разоблачений «не сводим к удару по авторитету США, он фундаментальнее, поскольку позволил констатировать, что «ИКТ и Интернет являются инструментом систематического одностороннего контроля государства над обществом и внешними контрагентами» (с. 167). Действительно, потенциальные возможности для подобного контроля со стороны государства при помощи использования ИКТ существуют, но, по моему мнению, не все государства озабочены таким контролем, и он не является всеобъемлющим, поскольку для государства его реализация трудноосуществима и затратна. Тем не менее задача создания механизмов защиты права на тайну частной жизни, безусловно, востребована, и автор предлагает несколько направлений действий для мирового сообщества, в частности распространение на программно-аппаратное обеспечение подобной слежки механизмов Вассенаарских договоренностей по экспортному контролю за обычными вооружениями и товарами и технологиями двойного применения.

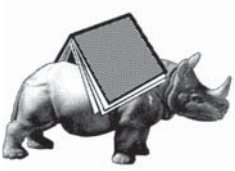
Как уже было указано выше, монография изобилует предложениями, и многие из них могут быть учтены как при формировании российской стратегии в отношении применения ИКТ или при модернизации Стратегии развития информационного общества в России, так и в рамках развития международно-правовых институтов. Однако можно с уверенностью сказать, что свое отношение к указанным рекомендациям читателю следует формировать только после прочтения этой интересной книги.

Примечания

1 Послание Президента Федеральному Собранию, 1 декабря 2016 г. http://kremlin.ru/events/president/news/53379 (последнее посещение — 22 января 2017 г.).

2 Официальный сайт для размещения информации о подготовке федеральными органами исполнительной власти проектов нормативных правовых актов и результатах их общественного обсуждения.

3 Минкомсвязь: рунет не планируется отключать от глобальной сети. Ведомости. 2014, 19 сентября. http://www.vedomosti.ru/technology/news/2014/09/19/minkomsvyaz-runet-ne-planiruetsya-otklyuchat-ot-globalnoj (последнее посещение — 23 января 2017 г.).



КРАСНАЯ ПАУТИНА: ИСТОРИЯ С НЕИЗВЕСТНЫМИ ПОДРОБНОСТЯМИ

Андрей Солдатов, Ирина Бороган.
Битва за Рунет: Как власть манипулирует информацией и следит за каждым из нас.
М.: Альпина Паблишер, 2017. — 342 с.

Рецензия — Елена Черненко

Книга основателей портала Agentura.ru Андрея Солдатова и Ирины Бороган *Битва за Рунет: Как власть манипулирует информацией и следит за каждым из нас* вышла на английском языке (название в оригинале — *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*) в 2015 г. Я собиралась ее приобрести на Амазоне, так как была почти уверена, что в российском переводе книга вряд ли увидит свет. Но в итоге книга Солдатова и Бороган все же была переведена на русский язык и недавно появилась в книжных магазинах. До последнего момента я сомневалась, что это произойдет. Незадолго до назначенной даты публикации Андрей сообщил на своей страничке в Facebook, что у издательства Альпина Паблишер возникли какие-то проблемы, и многие, включая меня, подумали, что в дело все же вмешалась цензура. В России такие книги сейчас — большая редкость. Благодаря разоблачениям экс-агента ЦРУ и АНБ Эдварда Сноудена мир узнал о массовой слежке американских спецслужб за пользователями интернета. О том же, какие возможности есть у российских властей в этой сфере, широкой публике было известно намного меньше. В *Битве за Рунет* рассказано, как российские власти манипулируют информацией и следят за каждым из нас. Не зря сам Эдвард Сноуден назвал Андрея Солдатова «самым заметным критиком российского аппарата электронной слежки»[1].

В книге подробно описана история слежки за российскими гражданами — от телефонной прослушки 1930-х гг. до современных технологий СОРМ и скандального *пакета Яровой*. В ней, в частности, рассказывается о неизвестных ранее подробностях системы слежки, которую российские спецслужбы использовали на зимней Олимпиаде 2014 г. в Сочи. Авторы изучили множество открытых источников, включая техническую документацию на сайте госзакупок. Были проанализированы презентации и публичные заявления, сделанные российскими чиновниками и топ-менеджерами компаний — поставщиков Олимпиады, а также документы надзорных служб, например, Роскомнадзора. Как удалось выяснить авторам в результате проделанной работы, ФСБ осуществила серьезный апгрейд технологий системы оперативно-розыскных мероприятий (СОРМ), значительно расширив возможности слежки. По мнению Солдатова и Бороган, российские власти в ходе подготовки к Олимпиаде 2014 г. использовали самые современные технологии слежки не только для обеспечения безопасности их проведения на фоне активизации

деятельности террористов (осуществивших два теракта в Волгограде), но и для предотвращения протестных акций активистов.

Эдварду Сноудену и его деятельности в книге посвящена отдельная глава. В ней, в частности, подробно рассказывается о состоявшейся 12 июля 2013 г. закрытой встрече бывшего агента американских спецслужб с российскими правозащитниками и главами прокремлевских «правозащитных» структур. Мероприятие, которое проходило в аэропорту Шереметьево (в транзитной зоне именно этого московского аэропорта находился в тот момент Сноуден) освещали, наверное, все журналисты Москвы — по крайней мере, ни до, ни после этой встречи я не видела такого количества представителей СМИ, собравшихся в одном месте. Тем интереснее было узнать из книги Солдатова и Бороган неизвестные подробности этой встречи в пересказе ее непосредственных участников — программного директора Международной правозащитной организации Human Rights Watch по России Татьяны Локшиной и директора московского бюро Amnesty International Сергея Никитина.

Вместе с тем не могу не отметить небольшую неточность в главе о Сноудене. В ней сказано, что официальная версия его прилета в Москву со временем становилась все менее убедительной. 4 сентября 2013 г. президент Владимир Путин заявил в интервью, что еще в Гонконге Сноуден приходил в российское консульство, о чем сразу доложили в Кремль. Авторы отмечают, что публика впервые узнала эту часть истории именно из интервью президента России. Между тем в газете *Коммерсантъ* еще 26 августа 2013 г., т. е. еще до упомянутого интервью Владимира Путина, вышла заметка, в которой впервые говорилось о том, что Сноуден вошел в контакт с представителями РФ еще до того, как сел в самолет рейса компании «Аэрофлот» Гонконг–Москва. Эта информация была затем широко растиражирована российскими и иностранными СМИ.

Образ российских властей мне представляется несколько демонизированным в главе «Кремль атакует», где в частности рассказывается о попытках Москвы убедить международное сообщество в необходимости выработки правил поведения государств. Действительно, еще несколько лет назад Россию обвиняли в попытке подчинить интернет жесткому государственному контролю, однако в последнее время о необходимости принятия неких норм поведения в сети говорят и лидеры многих западных стран, включая президента США. Что же касается описанных в книге неудачных попыток Кремля изменить глобальные правила функционирования интернета и лишить США возможности доминировать в этой сфере, в прошлом году американские власти под напором международного сообщества все же отказались от большей части своих особых полномочий.

В целом я бы рекомендовала книгу Солдатова и Бороган всем, кто интересуется информационно-коммуникационными технологиями, работой спецслужб и историей постсоветской России. Возможно, после ее прочтения читателю будет казаться, что ФСБ следит за ним даже через стеклянную дверцу его микроволновки, но таков уж мир, в котором мы живем.

Примечания

1 Harney John. Snowden Defends Query to Putin on Surveillance. *The New York Times*. 2014, 18 April. https://www.nytimes.com/2014/04/19/world/europe/snowden-defends-query-to-putin-on-surveillance.html?_r=0 (последнее посещение 29 декабря 2016 г.)

Findlay, Trevor. What Price Nuclear Governance? Funding the International Atomic Energy Agency. Cambridge, Mass.: Report for Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2016. 104 p.

Деятельность МАГАТЭ уже не одно десятилетие способствует поддержанию международного мира и безопасности — агентство поддерживает использование атомной энергии в мирных целях и снижает риск распространения ядерного оружия. Казалось бы, успешная деятельность организации окупает все финансовые затраты на ее осуществление. Тем не менее новый доклад доктора Тревора Финдлея *What Price Nuclear Governance? Funding the International Atomic Energy Agency* ставит ряд вопросов в отношении механизмов финансирования организации — достаточно неизвестного широкой публике аспекта функционирования МАГАТЭ. В докладе автор задается вопросом: является ли текущий уровень финансирования МАГАТЭ достаточным для нормального и эффективного функционирования агентства? Насколько устойчивой является растущая зависимость агентства от добровольного финансирования? Можно ли считать существующую систему финансирования справедливой? И насколько этично использование альтернативных источников финансирования?

Известное высказывание Уинстона Черчилля «За безопасность необходимо платить, а за ее отсутствие расплачиваться» как нельзя точно описывает суть доклада Тревора Финдлея — этот афоризм вспоминается при прочтении буквально каждого параграфа. В исследовании представлены различные варианты решения хронических проблем финансирования организации. Финдлей ярко иллюстрирует политику государств в отношении наполнения бюджета агентства и демонстрирует позиции членов агентства при определении первоочередных нужд МАГАТЭ, демонстрируя, кто готов платить за международную и, следовательно, собственную безопасность и в каком размере.

Регулярный бюджет МАГАТЭ, формирующийся за счет начисляемых (то есть обязательных) взносов, ежегодно утверждается документом *Программа и бюджет агентства* и охватывает шесть основных программ: ядерную энергетику, топливный цикл и науку; ядерные технологии для развития и защиты окружающей среды; техническую и физическую ядерную безопасность; верификационные механизмы; политическую, управленческую и административную службы; техническое сотрудничество в целях развития. При этом, несмотря на разнообразие программ

бюджета, основная часть средств выделяется на осуществление гарантий МАГАТЭ (safeguards) и на функционирование структур политического и общего управления — на эти цели выделяется около двух третей от всего бюджета агентства.

Следует отметить, что за последние 15 лет произошло изменение доли различных программ в распределении бюджета. После событий 11 сентября 2001 г. и аварии на АЭС *Фукусима-1* доля финансирования поддержания ядерной безопасности увеличилась до 10%. Приоритет также отводится атомной энергетике, ядерному топливному циклу и науке (11%) в связи с ростом интереса к выработке электроэнергии на АЭС. Но львиная доля финансирования по-прежнему направляется на поддержание верификационных механизмов, поглощающих 39% бюджета. Такой крен в финансировании вызван увеличением числа новых членов — развивающихся стран, таких, как Джибути, Гайана и Вануату, которые меньше участвуют в наполнении бюджета организации, но нуждаются в помощи в области осуществления гарантий. Принятие Дополнительного протокола в 1997 г. также увеличило расходы агентства на проведение инспекций.

Проблемы вокруг ядерных программ Ирана, Северной Кореи и Сирии также представляются вызовами для бюджета агентства. Последней грандиозной тратой МАГАТЭ стал иранский *проект*, в котором агентство принимает участие с 2003 г. и который в настоящее время является наиболее дорогостоящим *мероприятием*, которое осуществляет МАГАТЭ в рамках государственного сотрудничества. Совместный всеобъемлющий план действий по иранской ядерной программе, согласованный в июле 2015 г., требует еще больших финансовых, кадровых и других ресурсов, которые оцениваются в 9,2 млн евро в год. Подобные неучтенные в бюджете траты, связанные, в том числе, с ликвидацией последствий ядерных аварий и инцидентов, возникают неожиданно, требуя срочных и значительных финансовых вложений, которых у агентства зачастую нет. На этот случай автор рекомендует создать специальный фонд для решения проблем подобного рода — средства для него будут выделяться из общего бюджета и вноситься странами-донорами.

Регулярный бюджет МАГАТЭ составляет около 70% от общего бюджета, остальные 30% формируются за счет других источников финансирования: добровольных взносов и негосударственного финансирования. Кроме того, агентство имеет право привлекать *бесплатных* экспертов — их работу оплачивают непосредственно государства-члены, а также получать помощь в натуральной форме. Зачастую внебюджетные средства выделяются конкретными донорами на решение конкретной проблемы, что приводит к искажению бюджетных приоритетов агентства. Ссылаясь на доклад *Alternative Funding Sources for the International Atomic Energy*, подготовленный Кристофером Туми и его коллегами, автор указывает на то, что такая практика де-факто превращает МАГАТЭ в благотворительную организацию и ставит выполнение основной миссии агентства в зависимость от внебюджетных взносов.

Другой проблемой распределения бюджета организации выступает финансирование программы технического сотрудничества. Согласно Уставу МАГАТЭ, реализация основных направлений деятельности агентства обеспечивается за счет средств регулярного бюджета. Среди таких ключевых направлений Устав выделяет осуществление гарантий и административную деятельность, необходимую для функционирования агентства. Программа технического сотрудничества также упоминается в числе программ, финансируемых из регулярного бюджета, однако на практике конкретные проекты из этой программы финансируются за счет

добровольных взносов в фонд технического сотрудничества. После принятия *индикативного подхода к планированию*, согласно которому страны — члены МАГАТЭ приняли решение наполнять бюджет путем взносов, определенных ООН, на трехлетние целевые программы развития, родилась парадоксальная идея о планировании добровольных взносов. Данная ситуация в корне не устраивает основные страны-доноры — по их мнению, международная помощь должна быть добровольной, а не предписанной де-факто. Кроме того, большинство развивающихся стран, являющихся реципиентами программы технического сотрудничества, регулярно не платит даже обязательные взносы.

Подводя итоги своего исследования, доктор Финдлей предлагает способы балансировки бюджета МАГАТЭ. В первую очередь автор предлагает включить фонд технического сотрудничества и фонд физической ядерной безопасности в регулярный бюджет. Во-вторых, выдвигается идея установить фиксированное соотношение трат на программу гарантий и технического сотрудничества, которое поможет избежать необоснованного увеличения финансирования последнего. В-третьих, предлагается упразднить систему скидок на взносы для финансирования системы гарантий, созданную в 1971 г. — по мнению автора, она уже не адекватна. Осуществление гарантий в крупных развивающихся странах, в первую очередь в Китае, непропорционально размеру их ВВП и осуществляемым взносам в бюджет агентства. Размер платежей в регулярный бюджет со стороны государств — членов МАГАТЭ, по мнению Финдлея, должен определяться на основе постоянной оценки экономического положения стран, которая бы проводилась ООН.

Стоит ли специалистам в сфере международной безопасности ознакомиться с докладом, в названии которого используются слова «стоимость» и «финансирование»? Стоит. Будет ли интересна, а главное полезна, аудитории, далекой от мира финансов, представленная в работе информация? Безусловно, будет. Автор сумел оживить сухие цифры и доступно объяснить формирование бюджета агентства. Доклад Тревора Финдлея поможет читателям сформировать общую картину финансирования организации, заполнить пробелы в понимании замысловатых денежных механизмов и (отчасти) ответить на вопрос «Почему МАГАТЭ действует именно так, а не иначе?».

Наталья Косолапова

Харрис Ш. Кибервойн@. Пятый театр военных действий. М.: Альпина нонфикшн, 2016. 390 с.

Среди ряда корешков на книжной полке магазина название этой книги бросается в глаза — современный читатель, осознающий зависимость своей повседневной жизни от Всемирной сети и знакомый с разоблачениями Джулиана Ассанжа и Эдварда Сноудена, не может не отреагировать на такую смелую формулировку. Интернет превратился в поле битвы — такое нельзя пропустить, нужно быть в курсе. А автору с таким опытом рассказ интересной истории доверить можно — несколькими годами ранее Харрис получил престижную журналистскую премию за свой писательский дебют, посвященный государственной слежке в США.

Кибервойн@, состоящая из двух разделов, развивает эту тему. Первый раздел описывает процесс появления и развития в США национальной киберармии. С появ-

лением новых угроз в интернет-пространстве у Вашингтона возникла потребность в особых группах технических специалистов, которые бы действовали в составе разных государственных структур, впоследствии роль главного координатора их деятельности стало играть АНБ. Впрочем, американская администрация понимала, что ее возможности в реализации столь амбициозной задачи далеко не безграничны. Осознав это, американские власти были вынуждены обратиться к частным компаниям: начиная от американских фирм, куда в поисках лучших условий работы перешли некоторые из бывших *правительственных хакеров*, до зарубежных корпораций, торгующих сведениями об уязвимостях в программах.

Вторая часть посвящена роли крупного бизнеса в разграничении интернет-пространства: защите компаний от хакерских атак, попыткам гигантов финансовой, банковской и IT-сфер самостоятельно выстроить систему собственной кибероборонs, опыту взаимодействия подобных компаний с государством. Даже тон повествования дает понять, что американские власти не могут похвастаться абсолютным влиянием над IT-компаниями: представители разведслужб стараются усилить свое влияние на Nasdaq, Apple или Google и склонить их к обмену информацией, а на практике далеко не всегда в состоянии сообщить им что-то, чего те не знали бы сами. Приведенные в книге факты это лишь подтверждают. Оказывается, американская государственная кибербразведка в каком-то смысле предстает *бумажным тигром*, а ее устрашающая репутация и доминирование в области государственной слежки — до определенной степени заслуга нескольких амбициозных военных, уверенно продвигающих собственные проекты.

Свое журналистское расследование Харрис завершает собственными предположениями о том, каким станет киберпространство в будущем. Он рисует поле битвы государств, корпораций и хакерских группировок, где стремление к анонимности априори будет означать наличие преступных намерений, а безопасность сможет позволить себе далеко не каждый.

Автор книги на протяжении долгого времени освещает деятельность спецслужб США и организуемую ими массовую слежку. Действительно, книга богата подробностями, именами, цифрами, которые могут быть известны лишь эксперту, давно специализирующемуся на теме спецслужб. Харрис не позволяет себе голословных утверждений и догадок — везде, где это необходимо, указан источник информации. Еще одним несомненным плюсом является то, что даже непосвященному в сложные технические детали читателю простота и доступность языка дает возможность разобраться в теме.

Хотя на родине Шейн Харрис известен как публицист с активной гражданской позицией, книга написана в нейтральном ключе. Как заявляет сам автор, он не хотел превращать ее в политическое высказывание. В книге не найти резких, категоричных пассажей в адрес американской администрации или противников США в киберпространстве. Впрочем, возможно, именно отсутствие элементов публицистического жара может быть воспринято некоторыми читателями как недостаток данной работы. Яркая конструктивная критика могла бы оживить качественный, но немного флегматичный нарратив.

Так или иначе, *Кибервойну* можно посоветовать широкому кругу читателей. Прежде всего она будет полезна тем, кто хотел бы иметь более обширное представление о возможностях, которые получила разведка с развитием интернет-тех-

нологий, процессе создания киберармий, а также степени государственного вмешательства в функционирование Всемирной паутины. В то же время детальная информация о методах работы АНБ сможет заинтересовать любого, кого волнуют вопросы анонимности и безопасности личных данных. Иными словами, книга дает отличную возможность поразмыслить над вопросом, на который сам автор ответа не дает: как рядовому пользователю в эпоху глобального киберпротивостояния *всех против всех* не попасть под перекрестный огонь и защитить самого себя.

Анна Поленова

Paradox of Progress, A publication of the National Intelligence Council, January 2017, NIC 2017-001 / Национальный совет по разведке США. Парадокс прогресса. Январь 2017 г. 226 с.

Достижения индустриальной и информационной эпох формируют облик будущего — оно таит опасности, но одновременно открывает больше возможностей, чем когда-либо ранее.

Движение прогресса в последние десятилетия позволило избавить от бедности 1 млрд жителей планеты, а также расширило горизонты достижимого для индивидов, сообществ и целых государств. Но тот же прогресс породил и потрясения, подобные *арабской весне*, мировому финансовому кризису 2008 г., и привел к подъему популизма. Эти события, ставшие предвестниками мрачного будущего, показали, насколько хрупки достижения современности. Анализу рисков и перспектив развития человечества до 2035 г. и посвящен объединенный доклад разведсообщества США.

Авторы рассматривают сценарии развития событий и влияние технологий (космических, энергетических, биологических) на ближайшее будущее.

К сожалению, мир будущего не рисуется как *прекрасное далеко* — человечество станет свидетелем возрастания напряженности как внутри государств, так и между странами. По мнению авторов, глобальный экономический рост замедлится, что вызовет еще более комплексные мировые проблемы. Эра американского господства, которая утвердилась с окончанием холодной войны, завершится, основы существующего миропорядка будут пересмотрены. Право вето ООН все чаще будет становиться тормозом международного сотрудничества, а различное видение событий углубит различия в понимании международной обстановки, роли правительств в области экономики, окружающей среды, религии, безопасности и прав человека. Споры о моральных границах, ценностях и интересах государств обострятся до такой степени, что будут угрожать международной безопасности.

Попытки навести порядок в этом хаосе в долгосрочной перспективе будут обречены на неудачу. Замедление экономического роста и увеличение долговых обязательств сначала приведут к ослаблению демократии, а затем к установлению авторитарных режимов и воцарению нестабильности внутри отдельных государств. Информация станет инструментом конкуренции и сотрудничества, в ее распространении наиболее влиятельные глобальные игроки будут опираться на сетевые структуры.

Сосредоточенность Соединенных Штатов и стран Запада на собственных проблемах в совокупности с эрозией норм международного права будет способствовать

попыткам Китая и России ослабить влияние США в мире. Неявная агрессия не перейдет в состояние открытой войны, но усилит риски случайных просчетов. Подобная *многополярная* модель мира развяжет руки агрессивным региональным акторам.

Не лучше выглядит и внутреннее положение государств: глобализация и развитие технологий обогатят богатых и выведут из нищеты миллионы бедных, но выиграют от этого преимущественно страны Азии. Пострадает средний класс западных стран. Огромный поток мигрантов истощит национальные бюджеты и увеличит конкуренцию за рабочие места, что усилит протестные импульсы, вызовет рост националистических настроений и напряженность внутри стран.

На примере трех сценариев авторы доклада излагают свое видение будущего мироустройства, которое будет зависеть от того, как будет складываться взаимодействие отдельных граждан, сообществ и правительств в условиях быстроменяющейся экономики. По их мнению, будущее мира зависит и от того, какие формы примут международные конкуренция и сотрудничество, а также от того, насколько эффективно человечество будет справляться с возникающими глобальными проблемами.

Три сценария рассматривают глобальную перспективу на национальном (*Острова*), региональном (*Орбиты*) и глобальном уровнях (*Сообщества*).

Сценарий *Островов* ставит под сомнение теорию глобализации и предполагает перестройку мировой экономики с длительными периодами медленного (или даже нулевого) роста. В этом сценарии национальные правительства воспользуются протекционистскими методами и будут поддерживать экстенсивное экономическое развитие для обеспечения экономической и физической безопасности граждан в условиях политической нестабильности.

Сценарий *Орбиты* описывает сложное сосуществование крупных держав, конкурирующих за сферы влияния и одновременно борющихся с внутренней нестабильностью. Рост национализма, появление новых деструктивных технологий и снижение стремления к международному сотрудничеству увеличивают риски межгосударственных конфликтов. При этом лидеры ведущих стран могут проводить политику, которая либо укрепит стабильность, либо еще более обострит напряженность.

Наконец сценарий *Сообщества* ищет альтернативы традиционным инструментам управления. В нем подробно рассматриваются информационные технологии в качестве ключевого средства борьбы сетевых структур и правительств за власть.

Соблюдая традиции американского *хеппи-энда*, авторы приходят к заключению, что тенденции, которые приводят к рискам в краткосрочной перспективе, в долгосрочной могут создавать возможности для достижения наилучших результатов. И если миру хватит благоразумия использовать эти возможности во благо, наше будущее будет более светлым, чем предполагают эти три сценария.

Золотым ключиком для правительств и сообществ индивидов будет использование индивидуальных, коллективных и национальных ресурсов таким образом, чтобы это привело к устойчивому развитию, безопасности и процветанию.

Данная работа, несомненно, будет интересна экспертам по вопросам аналитического и стратегического планирования, а также всем любителям заглянуть за ширму времени.

Александра Тихонова

SUMMARY

FROM THE EDITOR

The editor of the latest Security Index issue highlights the main global security challenges posed by new technologies. He speculates on the feasibility and practicalities of nuclear arms control in the changing national and international governance environment, and says that various research communities should pool their efforts to identify solutions for the multitude of global problems.

Key words: *global security, new technologies, international law, ethical problems of new technologies.*

INTERVIEW

Russian Deputy Foreign Minister Sergey Ryabkov on the lessons, principles, and outlines of future Russian-U.S. global security efforts.

Key words: *Russian-U.S. relations, nonproliferation, sanctions, arms control, JCPOA, Iran, Korea.*

Sergey Savelyev, Deputy Director General of the Roscosmos State Corporation, interviewed on space services; on what could become weapons in space; on overblown fears and real threats facing peaceful space exploration; and on Russia's international space cooperation.

Key words: *weaponization of space, satellites, space junk, space debris, mission to Mars, Roscosmos.*

ANALYSIS

The IAEA safeguards system, a key element of the nuclear nonproliferation regime, is facing various technological and political challenges. The main challenge results from the inherent conflict between the global nature of

and other issues are discussed in a special report released by PIR Center in cooperation with *Centre russe d'etudes politiques* in Geneva. Andrey Doukhvalov and Natalya Kaspersky also look at the cyberthreats to automated industrial control systems and at the formation of the cybersecurity market.

Key words: *critical infrastructure, cybersecurity of critical infrastructure, civilian nuclear facilities, industrial control systems (ICS).*

ROUND TABLE

Warfare of the future may involve lethal autonomous systems, or robots that possess a degree of artificial intelligence and could potentially make their own decisions. Deployment of such weapons is a new challenge on the international agenda. It lies at the crossroads of political, legal, technological, ethical, and moral considerations. Definitions of lethal autonomous systems, the key problems arising from their use, and mechanisms of keeping them under control — these and other issues were discussed by leading international experts in the field at a round table held by PIR Center and the Russian Foreign Ministry's Diplomatic Academy in September 2016.

Key words: *military robots, lethal autonomous systems, artificial intelligence, ethics in robotics, international humanitarian law.*

COMMENTARY

This is not the first time the humankind is facing the need for regulating new technologies and their military applications. What makes the emerging technologies of the 21st century different? What are the opportunities and threats to global security posed by autonomous weapons systems, cyber-, bio-, and space technologies, 3D printing and directed-energy weapons? How can their destabilizing effects be minimized? And how is the very idea of strategic stability evolving? These and other questions are addressed by Jarmo Sareva, Director of the UN Institute for Disarmament Research (UNIDIR).

Key words: *emerging technologies, strategic stability, global security, directed-energy weapons, disarmament, UNIDIR.*

Technologies that can prevent a resource collapse and give the humankind models of effective consumption can also interfere with the process of human evolution as a species and make useless all the existing mechanisms of global security. Kurchatov Institute President Mikhail Kovalchuk and Vice President Oleg Naraykin warn of the dual nature of environmental technologies and the need for a transition towards a new system of international security based on the principle of controlling technologies rather than armaments.

Key words: *environmental technologies, convergent technologies, technology control, arms control, Kurchatov Institute.*

ОБ АВТОРАХ

Баклицкий Андрей Александрович — директор программы ПИР-Центра «Россия и Ядерное нераспространение». Научный сотрудник Центра глобальных проблем и международных организаций Института актуальных международных проблем 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». Выступает с лекциями в МГИМО и Дипломатической академии МИД России. Сфера научных интересов: международная безопасность, большой Ближний Восток, ядерная энергетика и ядерное нераспространение. Адрес электронной почты: *baklitsky@pircenter.org*

Бычков Валерий Михайлович — канд. физ-мат. наук. независимый эксперт. Окончил Московский инженерно-физический институт по специальности «Экспериментальная ядерная физика». В 1970–1981 и в 1985–1987 гг. работал в Физико-энергетическом институте (г. Обнинск) в Центре ядерных данных. В 1981–1985 и в 1987–2007 гг.— в департаменте гарантий МАГАТЭ инспектором, руководителем операционных подразделений и руководителем секции «оценки эффективности гарантий». Сфера научных интересов: учёт и контроль ядерного материала, системы международного контроля, режим нераспространения ядерного оружия. Адрес электронной почты: *valeri.bytchkov@gmail.com*

Волчинская Елена Константиновна — канд. эконом. наук, главный специалист юридического отдела Федеральной нотариальной палаты. С 1995 по 2012 гг. работала в аппарате Комитета Государственной Думы по безопасности. В рамках служебных полномочий вела, в том числе, вопросы законодательного обеспечения информационной безопасности. Принимала участие в разработке законопроектов «О коммерческой тайне», «О персональных данных», «О слу-

жебной тайне», «Об электронной цифровой подписи», «Об электронной торговле», «О применении полиграфа», «О праве на информацию», «Об информации, информационных технологиях и о защите информации» и других, а также ряда модельных законов Межпарламентской ассамблеи СНГ, в том числе «О персональных данных», «Об электронной цифровой подписи». Автор более 120 монографий, научных статей и докладов, из них около 100 по проблемам информационной безопасности, в том числе монографий. Один из инициаторов и организаторов проведения (с 2001) под эгидой Комитета Государственной Думы по безопасности Национального форума Информационная безопасность России в условиях глобального информационного общества (Инфофорум). Член Рабочей группы при Экспертном Совете ПИР-Центра по международной информационной безопасности и глобальному управлению Интернетом с 2012 г. Член Экспертного Совета ПИР-Центра с 2015 г. Адрес электронной почты: *ks-vek@list.ru*

Грант Том — научный сотрудник центра международного права им. Лаутэрпахта при Кембриджском университете. Получил степень бакалавра в Гарварде (1991). Окончил юридическую школу в Йеле (1994) и получил степень доктора философии в Кембридже (2000). Служил юридическим советником при правительстве, международных организациях, а также двух президентских избирательных кампаниях в США. Бывший член Комиссии по международному праву. Занимался исследовательской деятельностью в Институте Макса Планка, Гейдельберге, Колледже Святой Анны, Оксфорде и Институте мира США, Вашингтон, округ Колумбия. Работал клерком в Верховном суде (2002) и Апелляционном суде США. Научные и профессиональные интересы включают сухопутные и морские границы, государственный иммунитет, правопреемство государств, международную защиту инвестиций, международные организации, применение силы, сравнительное конституционное право, избирательное право США, историю дипломатии, международное урегулирование споров. Адрес электронной почты: *tdg20@cam.ac.uk*

Гребенщиков Андрей Вадимович — первый секретарь Департамента по вопросам нераспространения и контроля над вооружениями МИД России. Выпускник отделения международных отношений Нижегородского государственного университета им. Н. И. Лобачевского (2001), а также российско-французского отделения магистратуры по международным отношениям (направление «Мировая политика») МГИМО (У) МИД (2004). В системе МИД с 2004 г. Работал в посольствах России в Республике Мали (2004–2007) и в Канаде (2011–2014). В настоящее время работает в ДНКВ, где занимается военно-космической проблематикой, а также вопросами Конвенции о «негуманном» оружии. Адрес электронной почты: *dnkv@mid.ru*

Гуднов Василий Михайлович — начальник отдела по взаимодействию с международными организациями Департамента международного сотрудничества Государственной корпорации «Роскосмос». Советник Российской Федерации 1 класса. Окончил Московский авиационный институт (1990) по специальности «инженер-испытатель летательных аппаратов». Выпускник Института международного бизнеса Академии внешней торговли при Министерстве экономического развития Российской Федерации (1991) — оперативно-коммерческий работник торговых представительств за рубежом. В госкорпорации «Роскосмос» решает задачи организации, координации и осуществления сотрудничества с международными организациями по вопросам исследования

и использования космического пространства в мирных целях, использования результатов космической деятельности и ее международно-правового регулирования, проведения анализа состояния и тенденций развития международного политико-правового и нормативного регулирования в области космической деятельности, разработки предложений, соответствующих интересам Российской Федерации, целям и задачам ее государственной политики в установленной сфере деятельности Корпорации и др. Адрес электронной почты: *Gudnov.VM@roscosmos.ru*

Джиака Жиль — советник по правовым вопросам, Международный Комитет Красного Креста (МККК). Имеет докторскую степень в области международного права и юриспруденции (Женевский институт международных отношений, 2012), магистр международного публичного права (Эссекский университет, 2006). Занимает должность советника по правовым вопросам Правового департамента МККК (с сентября 2014), является научным сотрудником Оксфордского института по вопросам этики, права и вооружённых конфликтов (с января 2013). Лауреат премии International Geneva Award Швейцарской сети международных исследований (2011) и награды имени Фрэнсиса Либера, врученной ему Американским обществом международного права (2015). Научные интересы: международный договор о торговле оружием (АТТ), доступность вооружения/стрелковое оружие, применение новых технологий в ходе военных действий (включая дистанционно управляемые и автономные виды вооружений, а также кибероружие и вопросы кибербезопасности), оружие ближнего боя, применение Конвенции о конкретных видах обычного оружия в отношении автономных боевых систем, рассмотрение вопросов вооружений и Дополнительный протокол I к Женевской конвенции. Адрес электронной почты: *ggiacca@icrc.org*

Духвалов Андрей Петрович — руководитель управления перспективных технологий «Лаборатория Касперского». Окончил факультет специального машиностроения МГТУ им. Н. Э. Баумана (1981). В софтверном бизнесе около 30 лет. Большую часть профессиональной деятельности занимался разработкой разнообразного ПО в качестве программиста, ведущего инженера, архитектора, лидера проекта. Участвовал в различных проектах по созданию программных продуктов системного и прикладного уровня. Последние 18 лет, работая в «Лаборатории Касперского», разрабатывает ПО в области информационной безопасности. В настоящее время возглавляет подразделение, занимающееся исследованиями перспективных методов обеспечения информационной безопасности и разработкой новейших технологий на основании этих исследований, в частности ведет проект Kaspersky Industrial CyberSecurity — решение по защите автоматизированных систем управления технологическими процессами от кибератак. Адрес электронной почты: *Andrey.Doukhalov@kaspersky.com*

Зульхарнеев Альберт Фархатович — директор ПИР-Центра, научный сотрудник Центра глобальных проблем и международных организаций Института актуальных международных проблем Дипломатической академии МИД России. Окончил аспирантуру факультета мировой политики и мировой экономики Национального исследовательского университета — Высшая школа экономики. Выпускник магистратуры факультета международных отношений Уральского государственного университета (2008) и магистратуры исторического факультета Центрально-Европейского университета (2007, Будапешт, Венгрия). С 2007 г. стажер, сотрудник ПИР-Центра. В августе — декабре 2011 г. стипен-

диат программы по преподаванию и исследованию Академии ОБСЕ в Бишкеке. В 2013–2015 гг. — исполнительный директор ПИР-Центра, с апреля 2015 директор ПИР-Центра. Адрес электронной почты: *zulkharneev@pircenter.org*

Ефимов Альберт Рувимович — руководитель робототехнического центра Фонда «Сколково». В 1993 году с окончил факультет кибернетики Московского института радиотехники электроники и математики. В 2002 стал лауреатом стипендиальной программы Chevening и получил степень Master in Communication Management в Strathclyde Graduate Business School (UK). В 2012 прошел обучение в летней школе робототехники в Imperial College of London. С 2013 года является аспирантом Института мировой экономики и международных отношений РАН. С 1994 по 2011 год работал в средних и крупных российских телекоммуникационных компаниях — «Аэроком», «Equant» и Группа Мобильные телесистемы (МТС). В 2011 перешел на работу в Кластер информационных технологий Фонда «Сколково» на должность директора по ИТ-проектам. В 2011–2014 годах развивал ряд направлений поддержки малых наукоемких предприятий, участников Сколково в области информатизации здравоохранения, связи и компьютерного зрения. В 2013–2014 годах работал общественным секретарем экспертного совета Министерства связи и массовых коммуникаций России по развитию отрасли информационных технологий. В 2013 году провел первую в России робототехническую конференцию Skolkovo Robotics. С августа 2014 возглавляет робототехнический центр Фонда «Сколково», основной целью является акселерация предпринимательской активности по направлению робототехники и киберфизических систем. Адрес электронной почты: *Aefimov@sk.ru*

Касперская Наталья Ивановна — президент группы компаний InfoWatch. Окончила Московский институт электронного машиностроения (МИЭМ) по специальности «Прикладная математика». С 1997 г. генеральный директор «Лаборатории Касперского». В 2007 году возглавила компанию InfoWatch, разрабатывающую инновационные решения в области защиты корпораций от наиболее актуальных внутренних и внешних угроз. Активно инвестирует в развитие высокотехнологичных компаний, является членом Грантового комитета фонда «Сколково», членом правления Ассоциации Разработчиков Программных продуктов (АРПП) «Отечественный Софт», членом Экспертного совета по российскому программному обеспечению при Министерстве связи и массовых коммуникаций. Возглавляет подгруппу «Интернет+общество» при Администрации Президента, созданную во исполнение перечня поручений Президента РФ от 29.01.2016. Адрес электронной почты: *Natalya.Kaspersky@infowatch.*

Козюлин Вадим Борисович — канд. полит. наук, старший научный сотрудник ПИР-Центра, профессор Академии военных наук. Окончил МГИМО МИД СССР (1990). Работал в МИД СССР/РФ, затем в отделе эксклюзивной информации газеты Московские Новости, был представителем РГП «Казспецэкспорт» в России. Обучался во Всероссийской академии внешней торговли по программе «Менеджмент в сфере военно-технического сотрудничества» (2000–2002). Тесно сотрудничает с компаниями-спецэкспортерами стран СНГ и дальнего зарубежья. Защитил диссертацию по теме: «Совершенствование политических механизмов влияния военно-технического сотрудничества на региональную стабильность в Центрально-Азиатском регионе». Сфера научных интересов — ВТС России с зарубежными государствами, региональная стабильность в Центральной Азии и Афганистане. Научный сотрудник ПИР-Центра (с 1994). Адрес электронной почты: *kozyulin@pircenter.org*

Ковальчук Михаил Валентинович — д-р физ-мат. наук, член-корреспондент РАН президент Национального исследовательского центра «Курчатовский институт». Выпускник физического факультета Ленинградского государственного университета (1970). Занимал должность директора Института кристаллографии имени А. В. Шубникова РАН (1998–2013). В 2005–2015 гг. — директор Национального исследовательского центра «Курчатовский институт». Руководитель межведомственной рабочей группы по направлению «Приоритетные и междисциплинарные научные исследования» при Совете при Президенте РФ по науке и образованию. Является научным руководителем факультета нано-, био-, информационных и когнитивных технологий МФТИ; деканом физического факультета СПБГУ, заведующим кафедрой оптики, спектроскопии и физики наносистем физического факультета МГУ имени М. В. Ломоносова и кафедрой нейтронной и синхротронной физики СПбГУ; главным редактором журнала «Кристаллография» РАН. Лауреат премии Правительства РФ в области науки и техники за 2006 год, действительный член Американской ассоциации развития науки (AAAS) по секции «Физика»; удостоен премии Правительства Российской Федерации в области образования (2012). Основные направления научной деятельности: рентгеновская физика, кристаллография, нанодиагностка, онвергенции нано-, био-, инфо-, когнитивных и социогуманитарных наук и технологий. Адрес электронной почты: *nrcki@nrcki.ru*

Кувалдин Станислав Аркадьевич — канд. истор. наук., независимый журналист. Выпускник исторического факультета МГУ. Эксперт Российского совета по международным делам. Работал в журнале «Эксперт» и различных изданиях издательского дома «Коммерсантъ». Колумнист издания Republic. Автор курса лекций на портале Arzamas. Преподаватель Университета Дмитрия Пожарского. Журналист, освещающий экологическую и социальную тематику. Специализируется на вопросах климатической политики различных стран мира. Сотрудничает с изданиями «Экология и право», проектом «+1», Кислород.Life, «Новой газетой» и другими изданиями. Адрес электронной почты: *kuvaldin35@gmail.com*

Легойда Владимир Романович — канд. полит. наук., председатель Синодального отдела по взаимоотношениям Церкви с обществом и СМИ Московского Патриархата. Церковный и общественный деятель, журналист, педагог, специалист в области культурологии, политологии и религиоведения, профессор кафедры международной журналистики, профессор кафедры мировой литературы и культуры МГИМО (У) МИД России, один из основателей и главный редактор журнала «Фома» (с 1996 г.). Окончил факультет международной информации МГИМО МИД РФ (1996). С 2009 г. — член Совета при Президенте РФ по развитию институтов гражданского общества и правам человека. С 2010 г. — член Патриаршего совета по культуре. С 2011 г. является членом Патриаршей комиссии по вопросам семьи и защиты материнства, а также секретарем Высшего Церковного Совета Русской Православной Церкви. С 2016 г. занимает должность председателя Комиссии по вопросам гармонизации межнациональных и межрелигиозных отношений Совета по взаимодействию с религиозными объединениями при Президенте РФ. Адрес электронной почты: *contact@sinfo-mp.ru*

Нарайкин Олег Степанович — д-р техн. наук, член-корреспондент РАН, вице-президент Национального исследовательского центра «Курчатовский институт». В 1970 году окончил МВТУ имени Н. Э. Баумана по специальности «Динамика и прочность машин». Член рабочей группы «Инфраструктура научных

исследований» при Совете при Президенте Российской Федерации по науке и образованию, член Межведомственной комиссии по технологическому развитию и Межведомственной комиссии по технологическому прогнозированию при Совете по модернизации экономики и инновационному развитию при Президенте Российской Федерации, член Рабочей группы по развитию биотехнологий. Председатель научно-методического совета по механике Минобрнауки России, член экспертного совета Российского научного фонда, входит в состав рабочей группы по разработке новой редакции федерального закона «О науке и государственной научно-технической политике в Российской Федерации» комитета Государственной Думы по науке и наукоёмким технологиям. Заведующий кафедрой «Прикладная механика» МГТУ имени Н. Э. Баумана. Автор более 90 работ в ведущих отечественных и международных научных журналах. Соавтор 9 изобретений. Основные направления научной деятельности: теория колебаний, мехатроника, нано- и микросистемная техника, биомеханика и биомедицинские технологии. Адрес электронной почты: *naraykin_os@nrcki.ru*

Рябков Сергей Алексеевич — Чрезвычайный и Полномочный Посол, заместитель министра иностранных дел Российской Федерации. В 1982 г. окончил МГИМО МИД СССР. С этого же года на дипломатической службе. В 1995–1999 гг. — начальник отдела ОБСЕ Департамента общеевропейского сотрудничества Министерства иностранных дел Российской Федерации. В 1999–2001 гг. — старший советник Посольства России в США, в 2002 –2005 гг. — советник-посланник Посольства России в США. В 2005–2008 гг. — директор Департамента общеевропейского сотрудничества МИД РФ. С августа 2008 г. — заместитель министра иностранных дел. Член редакционной коллегии журнала *Индекс Безопасности*.

Савельев Сергей Валентинович — заместитель генерального директора по международному сотрудничеству Государственной корпорации по космической деятельности «Роскосмос». Окончил Московский авиационный институт им. С. Орджоникидзе по специальности «радиоинженер» (1989). Служил в Управлении развития международного научно-технического сотрудничества Министерства науки и технической политики РФ (1993–1995). Занимал должность третьего секретаря Постоянного представительства РФ при ЮНЕСКО (1995–2001). В 2004–2007 гг. выполнял функции второго секретаря Посольства РФ в Великобритании. Старший менеджер проектов департамента управления стратегическими проектами Дирекции стратегического планирования ЗАО «Гражданские Самолеты Сухого» (2007–2008). Занимал должность заместителя руководителя Федерального космического агентства в 2008–2015 гг.

Сарева Ярмо — директор Института Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР). Получил степень магистра в Школе международных исследований Университета Джона Хопкинса в Вашингтоне и магистра политических наук в Университете Турку, Финляндия. Заместитель посла Финляндии в Москве (1996–1998). Занимал должность директора по вопросам разоружения, контроля над вооружениями и нераспространения Министерства иностранных дел Финляндии, пост первого секретаря в посольстве Финляндии в Вашингтоне и советника миссии при ОБСЕ в Вене, советника-посланника Постоянного представительства Финляндии при ООН (1998–2000). Занимал должность начальника канцелярии председателя 55-й сессии Генеральной Ассамблеи ООН (Ассамблеи тысячелетия 2000–2001). Занимал должность начальника Сектора по вопросам разоружения и мира при Департаменте по делам Генеральной Ассамблеи и конференционному управ-

лению (ДГАКУ) (2006–2009). Заместитель Постоянного представителя Финляндии при ООН в Нью-Йорке, Председателя Первого комитета ГА ООН, заместителем Генерального секретаря Конференции по разоружению и директором секретариата Конференции по разоружению (2009–2014). Адрес электронной почты: *jsareva@unog.ch*

Сун Синьпин — профессор Сианьской политической академии (КНР). Адрес электронной почты: *songxp165@sohu.com*

Уорхэм Мэри — координатор Кампании против роботов-убийц (Campaign to Stop Killer Robots). Получила степень бакалавра и степень магистра в области политологии Университета Виктории в Веллингтоне. Проводила исследования для парламента Новой Зеландии (1995–1996). Работала в Американском фонде ветеранов Вьетнамской войны помогая Джоди Уильямс в координации международной кампании по запрещению противопехотных мин (МКЗНМ) (1996–1997). Занимала должность старшего защитника Отдела вооружений Human Rights Watch (1998–2006), директора по правозащитной деятельности в Оксфам Новая Зеландия (2006–2008). Адрес электронной почты: *wareham@hrw.org*

Хитченс Тереза — старший научный сотрудник Центра международных исследований и исследований в области безопасности при университете Мэриленда. Работала директором Центра оборонной информации, возглавляла Центр проекта космической безопасности (2001–2008). Занимала пост директора по исследования Британо-американского совета по информационной безопасности, филиал в Вашингтоне. Директор Института ООН по исследованию проблем разоружения (ЮНИДИР) в 2009–2014 гг. Международный редактор Defense News по вопросам безопасности, торговли оружием, ядерного, химического и биологического оружия. Адрес электронной почты: *thitchen@umd.edu*

Черненко Елена Владимировна — канд. историческ. наук., заведующая отделом внешней политики издательского дома «Коммерсантъ». Выпускница исторического факультета Московского государственного университета имени М. В. Ломоносова (2005). В 2003–2006 гг. корреспондент немецкой редакции и ведущей радиопередач РГРК Голос России. В разное время была корреспондентом газеты Moskauer Deutsche Zeitung, информационного агентства EurActiv, журнала Русский Newsweek. Сфера научных интересов: информационная безопасность, нераспространение ОМУ, контроль над вооружениями и разоружение, развитие атомной энергетики. Член Совета ПИР-Центра и Рабочей группы при Экспертном совете ПИР-Центра по международной информационной безопасности и глобальному управлению Интернетом с 2012 г. Адрес электронной почты: *chernenko@kommersant.ru*

ПИР-ЦЕНТР

(по состоянию на 30 декабря 2016 г.)

Анна А. **Акимова**, бухгалтер
Андрей А. **Баклицкий**, директор программы *Россия и ядерное нераспространение*
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
Мая Х. **Иванова**, стажер
Галия Р. **Ибрагимова**, к.п.н., консультант
Наталья И. **Калинина**, д.м.н., член Совета
Вадим Б. **Козюлин**, к.п.н., старший научный сотрудник, член Совета
Наталья В. **Косолапова**, стажер
Александра В. **Куликова**, консультант
Василий Ф. **Лата**, д.в.н., генерал-лейтенант, консультант
Евгений П. **Маслин**, генерал-полковник, член Совета
Владимир А. **Мау**, д.э.н., член Совета
Адлан Р. **Маргоев**, консультант
Максим С. **Мирошников**, координатор проектов, секретарь международного клуба *Триалог*
Владимир А. **Орлов**, к.п.н., советник, член Совета
Анна Л. **Поленова**, стажер
Дмитрий В. **Поликанов**, к.п.н., член Совета
Галина Д. **Рассказова**, бухгалтер
Юлия В. **Свешникова**, консультант
Юлия С. **Сеславинская**, помощник главного редактора журнала *Индекс Безопасности*
Екатерина А. **Степанова**, д.п.н., член Совета
Вячеслав И. **Трубников**, генерал армии, Чрезвычайный и Полномочный Посол, член Совета
Юрий Е. **Федоров**, к.и.н., член Совета
Юлия В. **Фетисова**, редактор бюллетеня эксклюзивной аналитики *Russia Confidential*
Муроджон А. **Халиков**, стажер
Александра В. **Чепелева**, координатор базы данных
Елена В. **Черненко**, к.и.н., член Совета
Олег И. **Шакиров**, консультант

ЭКСПЕРТНЫЙ СОВЕТ ПИР-ЦЕНТРА

(по состоянию на 30 декабря 2016 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, член Дирекции, ИМЭМО 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, Юридический отдел, 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 генерального секретаря НАТО, 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, президент, Пагуошское движение ученых, 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, Ракетные войска 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, преподаватель, 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, 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, ПАО *Компания „Сухой“*, Москва, Россия (с 2002 г.)

Лебедев Владимир Владимирович, директор, Центр гуманитарного и делового сотрудничества с соотечественниками за рубежом — Московский Дом соотечественника, Москва, Россия (с 2000 г.)

Лукацкий Алексей Викторович, бизнес-консультант по безопасности, 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, член Экспертного совета, ПИР-Центр, Москва, Россия (с 2004 г.)

Льюис Патриция, д-р, директор по исследованиям, Chatham House, Лондон, Великобритания (с 1994 г.)

Маргелов Михаил Витальевич, вице-президент, АО «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, Постоянное представительство Российской Федерации при международных организациях в Вене, Вена, Австрия (с 2015 г.)

Мурогов Виктор Михайлович, д.т.н., проф., председатель Международный Союз Ветеранов Атомной Энергетики и Промышленности, Обнинск, Россия (с 2009 г.)

Мурсанков Сергей Геннадьевич, ведущий специалист, Информационно-аналитическое управление, Фонд «Сколково», Москва, Россия (с 2010 г.)

Мюллер Харальд, д-р, проф., член Исполнительного совета, Франкфуртский Институт проблем мира, Франкфурт, Германия (с 1997 г.)

Мясников Евгений Владимирович, к. ф.-м. н. преподаватель, кафедра общей физики, Московский физико-технический институт (государственный университет), Москва, Россия (с 2011 г.)

Национальный исследовательский ядерный университет «МИФИ», Москва, Россия (с 1994 г.)

Наумкин Виталий Вячеславович, д.и.н., проф., академик 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 по научной работе, 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, Миддлберийский институт международных исследований в Монтерее, 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.)

НИЦ *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., главный научный сотрудник, 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., член Экспертного совета, ПИР-Центр, 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», 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., вице-президент, Российская ассоциация международного права, Москва, Россия (с 2001 г.)

Убеев Алексей Вадимович, к.т.н., член Экспертного совета, ПИР-Центр, Москва (с 2009 г.)

Федоров Александр Валентинович, к.ф.-м.н., член Экспертного совета, ПИР-Центр, 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 по взаимодействию с заинтересованными сторонами в Восточной Европе и Центральной Азии, Корпорация Интернета по присвоению имен и номеров (ICANN), Москва, Россия (с 2014 г.)

Якушкин Дмитрий Дмитриевич, член Экспертного совета, ПИР-Центр, 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 30 декабря 2016 г.)

Волчинская Елена Константиновна, главный специалист, юридический отдел, Федеральная нотариальная палата, Москва, Россия (с 2012 г.)

Демидов Олег Викторович, консультант, ПИР-Центр, Москва, Россия (с 2012 г.)

Зинина Ульяна Викторовна, директор по корпоративным вопросам, *Microsoft Russia*, Москва, Россия (с 2012 г.)

Зиновьева Елена Сергеевна, доцент, 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, заведующая кафедрой, кафедра международного частного права, Дипломатическая академия МИД России, Москва, Россия (с 2013 г.)

Куликова Александра Владимировна, менеджер по взаимодействию с заинтересованными сторонами в Восточной Европе и Центральной Азии, Корпорация Интернета по распределению имен и адресов, Москва, Россия (с 2014 г.)

Левова Ирина Юрьевна, директор по стратегическим проектам, Институт исследований интернета, Москва, Россия (с 2012 г.)

Лукацкий Алексей Викторович, бизнес-консультант по 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, член Экспертного совета, ПИР-Центр, Москва, Россия (с 2012 г.)

Черненко Елена Владимировна, руководитель, отдел внешней политики, Издательский дом *Коммерсантъ,* Москва, Россия (с 2012 г.)

Якушев Михаил Владимирович, вице-президент по взаимодействию с заинтересованными сторонами в Восточной Европе и Центральной Азии, Корпорация Интернета по присвоению имен и номеров (ICANN), Москва, Россия (с 2012 г.)

МЕЖДУНАРОДНАЯ ЭКСПЕРТНАЯ ГРУППА

(по состоянию на 30 декабря 2016 г.)

Абишева Мариан Асаровна, руководитель Службы международных и национальных проектов Библиотеки Первого Президента Республики Казахстан — 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, профессор, Европейский центр исследований безопасности имени Джорджа Маршалла, Гармиш-Партенкирхен, Германия (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.)

СОДЕРЖАНИЕ ЖУРНАЛА *ИНДЕКС БЕЗОПАСНОСТИ* ЗА 2016 г.

РЕЦЕНЗЕНТЫ СТАТЕЙ, ОПУБЛИКОВАННЫХ В ЖУРНАЛЕ *ИНДЕКС БЕЗОПАСНОСТИ* В 2016 г.

Редакция журнала «Индекс Безопасности» *благодарит членов редакционной коллегии, консультантов и читателей за сотрудничество в 2016 г. Работать над журналом в качестве рецензентов нам помогали:*

Марина Павловна **Беляева**, директор Департамента международного сотрудничества Государственной корпорации по атомной энергии *Росатом*;

Альберт Рувимович **Ефимов,** руководитель Робототехнического центра Фонда Сколково;

Ирина Доновна **Звягельская**, д-р. истор. наук., профессор, главный научный сотрудник Центра арабских и исламских исследований Института востоковедения РАН;

Дмитрий Алексеевич **Ковчегин**, независимый консультант;

Алексей Олегович **Кокорин**, канд. физ.-мат. наук, руководитель программы «Климат и энергетика» Всемирного фонда дикой природы (WWF России);

Владимир Петрович **Кучинов**, советник генерального директора Государственной корпорации по атомной энергии *Росатом*;

Алексей Викторович **Лукацкий**, бизнес-консультант по информационной безопасности компании Cisco Systems;

Александр Георгиевич **Савельев**, д-р. полит. наук., главный научный сотрудник Центра международной безопасности Национального исследовательского института мировой экономики и международных отношений имени Е. М. Примакова РАН (ИМЭМО РАН);

Елена Владимировна **Супонина**, канд. философск. наук, советник директора Российского института стратегических исследований;

Александр Валентинович **Федоров**, канд. физ.-мат. наук;

Никита Александрович **Филин**, канд. истор. наук, научный сотрудник Центра изучения стран Ближнего и Среднего Востока Института востоковедения РАН.