ВЕСНА-ЛЕТО 2016 ИНДЕКС БЕЗОПАСНОСТИ № 1 (116), Том 22

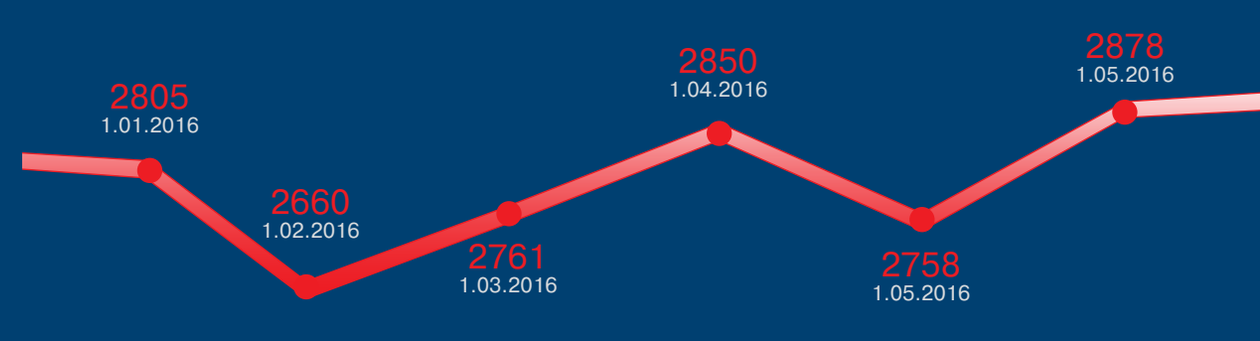
Российский
журнал
о международной
безопасности

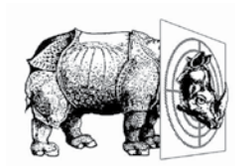
SECURITY INDEX

ИНДЕКС БЕЗОПАСНОСТИ

№ 1 (116) 2016

ПИР-Пресс представляет



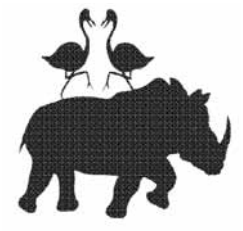


О ДИСКУРСЕ И КОНСЕНСУСЕ

ЦИТАТЫ. КОНЕЦ

Сперва, пока они плелись по тропинке на краю Дремучего Леса, оба молчали; но когда они дошли до речки и стали помогать друг другу перебираться по камушкам, а потом бок о бок пошли по узкой тропке между кустов, у них завязался Очень Умный Разговор. Пятачок говорил: “Понимаешь, Пух, что я хочу сказать?” А Пух говорил: “Я и сам так, Пятачок, думаю”. Пятачок говорил: “Но с другой стороны, Пух, мы не должны забывать”. А Пух отвечал: “Совершенно верно, Пятачок. Не понимаю, как я мог упустить это из виду”.

АЛАН АЛЕКСАНДР МИЛН. ВИННИ-ПУХ И ВСЕ-ВСЕ-ВСЕ.



О БЫЛОМ И БУДУЩЕМ

Взрывной рост высоких технологий в очередной раз за последние сто лет на наших глазах радикально меняет всю систему общественного устройства. У обычных людей появляется возможность действовать самостоятельно там, где еще недавно требовалось участие квалифицированных посредников.

Благодаря соцсетям каждый давно получил уорхолловские 15 минут славы, точнее, возможность бесконечно высказываться и быть услышанным. Мебель, обувь, музыкальные инструменты, бытовую технику и даже оружие уже сегодня можно напечатать на 3D-принтере. Финтех-сообщество все успешнее конкурирует с традиционными финансовыми учреждениями. Децентрализованные валюты на базе технологии блокчейна используются в расчетах и постепенно теснят традиционные системы денежных переводов. Архитектура блокчейна, не позволяющая вносить изменения в записанную информацию, делает его универсальной заменой нотариата. Образовательные платформы меняют систему образования. Лучшие университеты соревнуются, выкладывая в открытый доступ полные курсы лекций.

Новые возможности активно исследуют военные. *Война моторов* уходит в прошлое — приоритетной мишенью становятся не регулярные войска противника, а его командование и инфраструктура. Работы по созданию боевых систем, основанных на принципах автономности, ведутся уже много лет. О машинах, которые могли бы самостоятельно принимать решение открывать огонь на поражение, говорить рано, однако в правозащитном сообществе на эту тему уже началась оживленная дискуссия и даже стартовала кампания, призывающая запретить *роботов-убийц*. В то же время ряд экспертов говорит о том, что использование роботов может сделать военные действия более гуманными, сократив потери среди личного состава и мирного населения. Старший научный сотрудник ПИР-Центра Вадим Козюлин и руководитель Робототехнического центра Фонда *Сколково* Альберт Ефимов в своей статье *Новый Бонд — машина с лицензией на убийство* анализируют основные направления развития смертоносных автономных систем в России и США, законодательную базу, применимую к их регулированию, а также деятельность крупнейших организаций, занимающихся разработкамив этой области.

Киберпространство, в которое помимо интернета входят локальные сети, автоматизированные системы управления, интернет вещей, продолжает стремительно расширяться и лишь в малой степени контролируется государством. В ближайшем будущем глобальная сеть *хот-спотов* позволит обеспечить непрерывный доступ в интернет, а технологии VPN и анонимайзеры несмотря на все усилия властей пока позволяют пользователям сохранять анонимность. Это создает крайне привле-

кательную среду для криминала. Помимо традиционных преступлений, которые переместились в интернет, вроде шантажа и шпионажа, появились новые виды правонарушений, противостоять которым правоохранительные органы и суды не готовы и к которым очень снисходительно относится общество. Проблемы новой преступности обсуждались на круглом столе, проведенном Комитетом гражданских инициатив совместно с ПИР-Центром. Тексты основных выступлений публикуются в этом номере.

Нападения в киберпространстве могут иметь настолько серьезные последствия, что возникает вопрос о том, где проходит граница между обычными преступлениями и военными действиями. Это особенно актуально, когда мишенью становятся объекты критической инфраструктуры. Уже на этапе атрибуции источника нападения требуется высокий уровень доверия и сотрудничества между спецслужбами, не говоря о наказании виновных, совершающих атаку через территорию сразу нескольких стран. Масштаб проблемы сложно оценить, так как и коммерческие компании, и госструктуры крайне неохотно раскрывают информацию об успешных кибернападениях. Исследование таксономии киберугроз для критической инфраструктуры, начатое в предыдущих номерах *Индекса Безопасности*, продолжает статья специалиста по физической ядерной безопасности Ольги Михайловой, а руководитель отдела продуктового маркетинга департамента защиты критических инфраструктур *Лаборатории Касперского* Матвей Войтов объясняет, какие объекты попадают под это определение.

Мир меняется, но не становится проще. Традиционные вызовы и угрозы международной безопасности сохраняются. КНДР – единственная страна в XXI веке – в начале года провела очередное ядерное испытание. Нет прогресса в создании зоны, свободной от оружия массового уничтожения, на Ближнем Востоке. Исполнительный секретарь Подготовительной комиссии Организации по Договору о всеобъемлющем запрещении ядерных испытаний Лассина Зербо в интервью *Индексу Безопасности* еще в начале года говорил о том, что важным шагом к созданию ЗСОМУ стала бы ратификация ДВЗЯИ Израилем и Ираном. Однако вопрос упирается в то, что договор до сих пор не ратифицировали Соединенные Штаты. По слухам, именно поэтому при согласовании Совместного всеобъемлющего плана действий переговорщики *шестерки* не настаивали на том, чтобы Иран ратифицировал ДВЗЯИ или хотя бы подключил к Международной сети мониторинга сейсмическую станцию, располагающуюся на его территории.

Сохраняются сложности с выполнением и универсализацией ДНЯО. Несмотря на противодействие со стороны членов *ядерного клуба*, обрастает сторонниками Гуманитарная инициатива. Более ста стран, недовольных темпами ядерного разоружения, ссылаясь на катастрофические последствия применения ядерного оружия требуют объявить его вне закона. Научный сотрудник ПИР-Центра Алена Махуковав своей статье *Гуманитарная инициатива: критическая масса антиядерных активистов* исследовала существующие в обзорном процессе ДНЯО тенденции и течения и проанализировала, как меняется отношение к ядерному оружию в мире под воздействием гуманитарной риторики.

Архитектура международной безопасности безнадежно устарела и нуждается в радикальном пересмотре, система контроля над вооружениями переживает глубокий кризис, механизмы многосторонней дипломатии буксуют. ПИР-Центр проанализировал существующие угрозы стратегической стабильности и подготовил набор предложений по упрочению международного режима ядерного нераспространения и дальнейшему разоружению. Приглашаем коллег к диалогу. Комментарии Высокого представителя Генерального секретаря ООН по вопросам разоружения (2007–2012) Сержио Дуарте публикуются уже в этом номере.

Данная нам в ощущениях реальность переменчива, и чем серьезнее происходящие изменения, тем сложнее бывает непосредственным участникам событий их отследить. В этом смысле очень показательны попытки представить себе будущее, бывшие популярными на рубеже XIX–XX веков. Мир будущего глазами людей из прошлого грешит как раз неспособностью увидеть принципиальные изменения, происходящие вокруг, и понять, как привычные общественные и экономические отношения могут быть вписаны в новую реальность. Впрочем, в этом нет беды. Все равно не угадаешь, так хоть посмешишь потомков.

Ольга МОСТИНСКАЯ
Главный редактор журнала *Индекс Безопасности*

РЕКОМЕНДАЦИИ ПИР-ЦЕНТРА ПО УКРЕПЛЕНИЮ МЕЖДУНАРОДНОГО РЕЖИМА ЯДЕРНОГО НЕРАСПРОСТРАНЕНИЯ В 2016–2020 гг.[1]

Обзорная конференция ДНЯО 2015 г., завершившаяся без принятия Заключительного документа, ярко продемонстрировала основные вызовы, стоящие перед режимом ядерного нераспространения. В целом, их можно подразделить на четыре основные категории:

Во-первых, сохраняющиеся сложности с выполнением и универсализацией договора. Существование *неофициальных* ядерных государств стало нормой международной политики, а призывы к универсализации договора все больше воспринимаются как ритуал. Это ведет к де-факто признанию ядерного статуса государств вне ДНЯО и может стимулировать неядерные государства к созданию ядерного оружия.

Во-вторых, нарушение стратегической стабильности, вызванное действиями ряда государств, направленными на установление или сохранение своего преимущества в стратегических сферах. Данные вызовы не только представляют угрозу национальной безопасности ядерных государств, но и тем самым делают невозможным переговоры о дальнейшем ядерном разоружении, что ведет к усилению противоречий внутри ДНЯО.

В-третьих, снижение эффективности механизмов многосторонней дипломатии и принятия решений с учетом интересов всех сторон, вызванное неготовностью отдельных стран договариваться в рамках процедур, основанных на консенсусе. Отказ от поисков компромисса привел к многолетнему блокированию работы Конференции по разоружению, а в недавнем прошлом и к отсутствию Заключительного документа ОК ДНЯО 2015 г. В результате важные многосторонние инициативы остаются нереализованными.

В-четвертых, отсутствие прогресса по созданию ЗСОМУ на Ближнем Востоке, обусловленное сохраняющимися региональными противоречиями. В связи с увязкой вопроса зоны и бессрочного продления ДНЯО в 1995 г. ближневосточный вопрос приобрел значение, выходящее за границы региона, и оказывает значительное влияние на ход обзорного процесса ДНЯО.

В рамках обзорного цикла ДНЯО 2016–2020 гг. международному сообществу предстоит выработать ответы на обозначенные вызовы.

СОБЛЮДЕНИЕ И УНИВЕРСАЛИЗАЦИЯ ДНЯО

Согласно статье X, **каждый участник ДНЯО имеет право покинуть договор**, в случае если «связанные с содержанием настоящего Договора исключительные обстоятельства поставили под угрозу высшие интересы его страны». При этом

пример КНДР демонстрирует, что страна, получившая мирные ядерные технологии как член ДНЯО, может затем использовать их в военных целях.

Юридическое ограничение права стран на выход из договора едва ли возможно, поскольку потребовало бы пересмотра ДНЯО и вряд ли стало бы непреодолимым препятствием в случае угрозы национальным интересам страны. Вместе с тем, существует необходимость обеспечения возврата ядерных материалов и оборудования, полученных страной до выхода из договора, государству-поставщику или, как минимум, их постановки под пожизненные гарантии МАГАТЭ.

Призывы к Индии и Пакистану присоединиться к ДНЯО в качестве неядерных государств не дают результата на протяжении десятилетий, превращаясь в ритуальные фразы.

В качестве первого шага по включению этих государств в международный режим ядерного нераспространения следует сконцентрироваться на подписании этими двумя государствами ДВЗЯИ. Пакистан является наблюдателем в рамках ПК ОДВЗЯИ, мировое сообщество может использовать этот пример, чтобы привлечь к участию в работе Подготовительной комиссии Индию. В дальнейшем международное сообщество должно продолжить диалог с Индией и Пакистаном по подписанию и ратификации ДВЗЯИ.

Шестисторонние переговоры по ядерной программе КНДР не ведутся с 2009 г. Отсутствие переговорного процесса с КНДР *замораживает* конфликт, с прекращением диалога исчезает один из факторов, сдерживающих Пхеньян от развития ядерной программы. Ядерное испытание КНДР 2016 г., на наш взгляд, стимулирует необходимость возобновления многостороннего диалога с участием КНДР.

В ходе такого многостороннего диалога о всеобъемлющем решении ситуации вокруг ядерной программы КНДР, как нам представляется, в среднесрочной перспективе возможно достижение промежуточного соглашения, согласно которому Пхеньян воздержался бы от дальнейших ядерных испытаний, испытаний ракет, наработки ядерных материалов и распространения чувствительных материалов и технологий в обмен на смягчение санкций, предоставление помощи и гарантии безопасности.

Совместный всеобъемлющий план действий (СВПД), согласованный Ираном и шестеркой международных посредников, продемонстрировал возможность успешной многосторонней дипломатии в сфере нераспространения. При этом длительность и сложность плана действий, большое количество участвующих сторон создают предпосылки для разногласий в ходе его реализации.

Стороны должны выполнять план действий в духе доброй воли, пользуясь всеми механизмами соглашения для разрешения возникающих противоречий в рамках СВПД. Выполнение плана действий не должно ставиться в зависимость от взаимоотношений сторон в других сферах.

УГРОЗЫ ДЛЯ СТРАТЕГИЧЕСКОЙ СТАБИЛЬНОСТИ

Европейский сегмент системы противоракетной обороны США, направленный, по заявлениям Вашингтона, против Ирана, может в перспективе получить возможность перехватывать российские баллистические ракеты. В качестве ответной меры Россия рассматривает технические возможности для преодоления ПРО

США, что может вызвать новую гонку вооружений. Несмотря на важность данного вопроса для европейской и международной безопасности, переговоры между Россией и США в области ПРО были прекращены в 2014 г. на фоне украинского кризиса. Заключение совместного всеобъемлющего плана действий (СВПД) по иранской ядерной программе не изменило планы США и НАТО по развертыванию системы ПРО. Подобное поведение также поднимает вопросы относительно того, является ли американская система ПРО, разворачиваемая против КНДР, частью плана по сдерживанию ядерного арсенала Китая.

Соединенные Штаты и НАТО должны вернуться к переговорам с Россией относительно ПРО в Европе. Первым шагом могло бы стать введение западными государствами мер транспарентности относительно разворачиваемой ими инфраструктуры ПРО.

Ядерное оружие США продолжает размещаться **за пределами национальной территории** (в Бельгии, Германии, Италии, Нидерландах и Турции), в том числе в непосредственной близости к границам России. Министерство обороны США проводит программу модернизации размещенных в Европе атомных бомб B-61.

Учитывая, что подобная практика входит в противоречие с положениями ДНЯО, а размещение ядерного оружия в европейских странах не только не повышает их безопасность, но может в определенной ситуации ее снижать, мировое сообщество заинтересовано в его скорейшем выводе на национальную территорию США.

В этом контексте стоит обратить внимание на предложения Республики Беларусь о создании зоны, свободной от ядерного оружия, в Центральной и Восточной Европе и австрийско-швейцарскую инициативу по созданию зоны, свободной от ядерного оружия, в Европе. Подобная зона может распространяться только на территорию неядерных государств и формироваться постепенно.

Разработка стратегического неядерного оружия с использованием гиперзвуковых технологий (наиболее развитой программой подобного рода, *Быстрый глобальный удар,* располагают США) может в перспективе представлять угрозу для стратегических ядерных сил и нарушить стратегическую стабильность.

Учитывая высокую стоимость, низкую успешность технологии и не до конца ясную область применения, существует возможность ограничения развития военных гиперзвуковых программ. Первым шагом по предотвращению гонки гиперзвуковых вооружений могло бы стать проведение международной конференции с участием всех ключевых игроков в данной сфере для обсуждения вопроса.

В перспективе государства, развивающие вооружения, основанные на гиперзвуковых технологиях, должны договориться о завершении этих программ и запрещении связанных разработок. Возможна разработка международного соглашения, запрещающего использование гиперзвуковых технологий в военных целях.

Ряд государств продолжает наращивать свои ядерные арсеналы. Несмотря на общее сокращение количества ядерного оружия в мире, этот процесс идет неравномерно и разнонаправленно. Даже в рамках ДНЯО не все государства, обладающие ядерным оружием, публикуют свои количественные показатели, что не позволяет отследить динамику изменений. Ядерные государства вне Договора продолжают наращивать свои арсеналы.

В рамках Конференции по разоружению все государства, обладающие ядерным оружием, (как официальные обладатели ядерного оружия согласно ДНЯО, так и прочие) должны в одностороннем порядке одновременно опубликовать официальные документы с указанием роли ядерного оружия в обеспечении национальной безопасности, числа и типов ядерных вооружений. За основу может быть взят формат публикаций о ядерных арсеналах России и США в рамках нового Договора СНВ.

Договор о всеобъемлющем запрещении ядерных испытаний (ДВЗЯИ) по-прежнему не вступил в силу, поскольку 8 стран из Приложения 2 к договору до сих пор его не ратифицировали (Египет, Индия, Иран, Израиль, Китай, КНДР, Пакистан и США). 20-летие открытия Договора к подписанию в 2016 г. должно дать новый импульс к завершению процесса ратификации ДВЗЯИ теми государствами, кто еще не сделал этого.

Содействие дальнейшей ратификации ДВЗЯИ и вступление договора в силу должно занимать важное место в политике мирового сообщества. До вступления договора в силу также важно продолжать оказывать максимальную поддержку ПК ОДВЗЯИ и развивать сеть мониторинга. Логичным шагом в этом направлении может стать подключение станций, размещенных на территории Ирана.

Отсутствие прогресса по обозначенным выше вопросам **делает дальнейшее сокращение ядерных арсеналов в ближайшей перспективе (2016–2020 гг.) мало реалистичным**. На данный момент Россия и США выполняют положения нового Договора СНВ. Очень важно, чтобы договор продолжал выполняться сторонами до завершения своего действия в 2021 г. В дальнейшем Москва и Вашингтон могли бы продолжать диалог с целью создания условий для нового договора, который бы удовлетворял обе стороны.

Новый договор может также включать в себя ограничения на развернутые стратегические системы (боеголовки и средства доставки), развернутые и неразвернутые пусковые установки и неразвернутые ядерные боеголовки с включением в переговорный процесс других вопросов контроля над вооружениями (например, КРМБ и КРВБ в неядерном оснащении и ПРО).

МНОГОСТОРОННИЕ ФОРМАТЫ СОТРУДНИЧЕСТВА В ОБЛАСТИ НЕРАСПРОСТРАНЕНИЯ И РАЗОРУЖЕНИЯ

В рамках ДНЯО **нарастают противоречия между государствами, обладающими ядерным оружием, и большинством неядерных стран относительно реализации статьи VI Договора**. Государства, не обладающие ядерным оружием, настаивают на ускорении темпов разоружения и введении временных рамок, что наталкивается на противодействие со стороны государств ядерной пятерки. Усилившаяся поляризация в рамках обзорного процесса ДНЯО и на других международных площадках все больше мешает открытой и конструктивной дискуссии между ядерными и неядерными государствами по вопросам дальнейших сокращений ядерных вооружений.

В этих условиях государствам, обладающим ядерным оружием, следует сохранять свою приверженность выполнению статьи VI ДНЯО, артикулируя свое стремление к дальнейшим шагам на пути к ядерному разоружению — причем шагам практическим и продуманным, способствующим разоружению на деле, а не в угоду какой-либо политической кампании.

Эта площадка остается главным многосторонним переговорным форумом для выработки соглашений по разоружению. При этом тот факт, что **переговорная работа КР фактически заблокирована с 1998 г.**, а Программа работы Конференции не принималась с 2009 г., негативно влияет на возможность международного сообщества проводить многосторонние переговоры и ставит под вопрос доверие к существующим международным механизмам, что может привести к созданию параллельных структур.

Ключевым вопросом, мешающим принять Программу работы Конференции, является несогласие относительно Договора о запрещении производства расщепляющихся материалов (ДЗПРМ). Недавнее российское предложение о внесении в программу работы КР нового пункта — о разработке Конвенции по борьбе с актами химического терроризма — и ограничение дискуссионными мандатами по остальным четырем пунктам (включая ДЗПРМ) является креативным решением для перезапуска работы Конференции.

В случае если российское предложение все же не станет основой для консенсуса, придется рассмотреть возможность введения временного моратория на переговоры по ДЗПРМ, что позволило бы начать работу по другим направлениям. При этом важно, чтобы мораторий был ограничен четкими временными рамками, вопрос не снимался с КР и оставался в общей корзине обсуждения.

На сегодняшний день не существует юридического ограничения на **размещение обычных вооружений в космическом пространстве**. При этом размещение оружия в космосе создало бы новый вид стратегических вооружений, оказало бы дестабилизирующее влияние на стратегическую стабильность и вызвало необходимость соответствующей модернизации и развития национальных ядерных сил. Для устранения угрозы новой гонки вооружений необходимо начать в рамках Конференции по разоружению многосторонний переговорный процесс по запрету размещения оружия в космическом пространстве. Российско-китайский проект Договора о предотвращении размещения оружия в космическом пространстве, применения силы или угрозы силой в отношении космических объектов (ДПРОК) был вынесен на рассмотрение Конференции по разоружению в 2008 г., обновленный вариант был представлен в 2014 г.

При этом, учитывая, что Конференция по разоружению остается заблокированной на неопределенный срок, важно продолжать работу над текстом Договора и его продвижение. Россия и Китай могли бы инициировать созыв международной конференции для широкого обсуждения проекта ДПРОК (включая спорные вопросы о верификации договора и противоспутниковом вооружении). Документ, доработанный в рамках конференции, может быть затем вынесен на Конференцию по разоружению.

Российско-американский Договор о ликвидации ракет средней и меньшей дальности (РСМД) сыграл важную роль в ограничении гонки ядерных вооружений и остается важным элементом стратегической стабильности. В то же время на сегодняшний день Договор ограничивает военные возможности России и США, не накладывая никаких обязательств на другие страны, обладающие развитыми ракетными программами. Ликвидация РСМД всеми государствами (де-юре или де-факто), обладающими ядерным оружием, помогла бы снизить межгосударственную напряженность, особенно в конфликтных регионах и положила бы начало многостороннему процессу ядерного разоружения. Переговоры

по приданию договору РСМД многостороннего характера также оказали бы стабилизирующее воздействие на российско-американское соглашение.

На 62-й сессии Генеральной Ассамблеи ООН в 2007 г. было оглашено совместное российско-американское заявление по Договору о ликвидации ракет средней и меньшей дальности, в котором было предложено придать договору РСМД глобальный характер. Заявление не получило поддержки потенциальных участников и не получило развития, тем не менее идея по-прежнему поддерживается Россией и США. Экспертная проработка придания договору РСМД многостороннего характера с участием представителей стран, обладающих ядерным оружием, также оказала бы стабилизирующее воздействие на действующий российско-американский договор.

Развитие образования в сфере нераспространения и разоружения является одним из непротиворечивых пунктов повестки дня в рамках обзорного процесса ДНЯО. Действие 22 плана действий Заключительного документа Обзорной конференции ДНЯО 2015 г. рекомендует «всем государствам ... осуществить рекомендации, содержащиеся в докладе Генерального секретаря Организации Объединенных Наций (A/57/124), касающемся исследования Организации Объединенных Наций по вопросу о просвещении в области разоружения и нераспространения». При этом подавляющее большинство членов ДНЯО не предоставляют ООН отчеты об осуществлении данных рекомендаций. Предоставление в ООН отчетов о деятельности по просвещению в области разоружения и нераспространения позволило бы продемонстрировать выполнение государствами своих обязательств.

Важную роль в развитии образования в сфере нераспространения и разоружения призван сыграть **Консультативный совет по вопросам разоружения при Генеральном секретаре ООН**. На своей 67-й и 68-й сессиях Консультативный совет мог бы провести обзор выполнения рекомендаций исследования Организации Объединенных Наций по вопросу о просвещении в области разоружения и нераспространения и, в случае необходимости, организовать пересмотр исследования с учетом накопленного опыта и новых технических возможностей для развития образовательных программ.

Новые инициативы в сфере образования в области ядерного нераспространения, в частности инициатива российских и американских университетов по запуску международной совместно аккредитованной магистерской программы по нераспространению оружия массового уничтожения, должны быть поддержаны. Особое внимание должно быть уделено участию в подобных программах студентов из государств-новичков в области мирного использования атомной энергии, где риски распространения более велики.

ЗОНА, СВОБОДНАЯ ОТ ОРУЖИЯ МАССОВОГО УНИЧТОЖЕНИЯ, НА БЛИЖНЕМ ВОСТОКЕ

Отправной точкой развития ситуации вокруг ЗСОМУ на Ближнем Востоке на 2016–2020 гг. стало завершение мандата 2010 г. на созыв конференции по зоне в 2012 г. После сложения полномочий специальным координатором конференции финским послом Яакко Лааява участники переговоров по зоне лишились механизма организации процесса. **Наиболее реалистичным форматом для продолжения переговоров станет их передача под эгиду аппарата Генерального секретаря ООН**. Ко-спонсоры резолюции 1995 г. и страны региона могут обра-

титься к генсеку с просьбой организовать переговорный процесс. При формулировании мандата на ведение переговоров за основу могут быть взяты положения Заключительного документа ОК ДНЯО 2015 г. При этом с целью привлечения Израиля к переговорному процессу часть формулировок допустимо смягчить.

В то же время ряд параллельных процессов может поспособствовать прогрессу в области создания зоны, свободной от оружия массового уничтожения, на Ближнем Востоке:

- Все государства региона могут сделать совместное заявление, в котором они примут обязательство воздерживаться от атак (включая кибератаки) на все задекларированные ядерные объекты друг друга, находящиеся под гарантиями МАГАТЭ, равно как и от угрозы таких атак.
- Ратификация всеми странами Ближнего Востока Договора о всеобъемлющем запрещении ядерных испытаний должна стать одной из предпосылок для заключения договора о создании в регионе зоны, свободной от оружия массового уничтожения.
- В рамках предварительных переговоров все участники должны *разработать* дорожную карту по постепенной постановке всех объектов ядерной инфраструктуры региона под гарантии МАГАТЭ.
- Все страны региона должны прийти к пониманию необходимости незамедлительной ратификации Дополнительного протокола к Соглашению о гарантиях МАГАТЭ. До момента ратификации странам рекомендуется добровольно применять положения Дополнительного протокола.
- В дальнейшем по итогам предварительных переговоров на конференции стороны должны создать постоянно действующий региональный механизм по мерам доверия в ядерной области, а также в химической и биологической областях.
- Институционализация сотрудничества в атомной области на Ближнем Востоке должна подкрепляться созданием единой региональной структуры, которая будет включать все государства региона. Арабское агентство по атомной энергии по-прежнему недостаточно эффективно и не готово к развитию регионального сотрудничества в атомной сфере. Международный центр по использованию синхротронного излучения в научных экспериментах и прикладных исследованиях на Ближнем Востоке, напротив, может послужить примером успешного научно-технического сотрудничества в регионе.
- Странам Ближнего и Среднего Востока, которые находятся на пороге быстрого развития ядерной инфраструктуры, следует рекомендовать сформировать эффективные механизмы раннего оповещения и реагирования в случае ядерных инцидентов. Рекомендуется максимально ускорить введение в действие Конвенции о помощи в случае ядерной аварии или радиационной аварийной ситуации, Венской конвенции о гражданской ответственности за ядерный ущерб и Конвенции об оперативном оповещении о ядерной аварии для тех стран, которые этого не сделали.

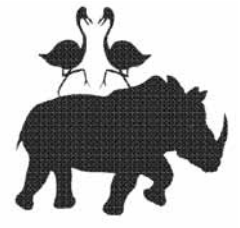
***

ПИР-Центр выступает за комплексный и беспристрастный подход к вопросам ядерного нераспространения[2]. Мы понимаем, что часть вопросов, поставленных нами в данном докладе, носит фундаментальный характер и потому ориентирована на долгосрочное осмысление, в то время как другая часть предполагает незамедлительные действия со стороны международного сообщества. Мы также понимаем, что ряд выдвинутых нами рекомендаций повторяет предложения, ранее уже высказанные государствами и экспертами; при этом некоторые предложения являются совершенно новыми и потому требуют дополнительной дискуссии.

Примечания

1 Данные рекомендации были выработаны в рамках программы ПИР-Центра *Россия и ядерное нераспространение* в период с мая 2015 г. по март 2016 г. и обсуждались на семинарах ПИР-Центра в Нью-Йорке (май 2015 г.), Женеве (июнь 2015 г.) и Москве (сентябрь и декабрь 2015 г.). Директор программы *Россия и ядерное нераспространение* Андрей Баклицкий хотел бы поблагодарить Евгения Бужинского, Альберта Зульхарнеева, Евгения Мясникова, Ольгу Мостинскую, Владимира Орлова, Владимира Рыбаченкова, Эмилию Сидорову, Алексея Убеева и Александра Федорова за их ценный вклад в работу над докладом, а также Центр глобальных проблем и международных организаций Дипломатической академии МИД России за содействие в организации дискуссии. Рекомендации представляют собой взгляды ПИР-Центра и не обязательно отражают мнение отдельных экспертов, участвовавших в обсуждении.

2 Вопросы, обозначенные в докладе, ранее освещались ПИР-Центром в серии Белых книг: *ДНЯО-2010: Как упрочить режим* в 2010 г. (npt2010.pircenter.org), *Десять шагов к созданию зоны, свободной от оружия массового уничтожения, на Ближнем Востоке* в 2013 г. (10steps.pircenter.org), *На пути к ядерному разоружению: статья VI ДНЯО и выполнение решений обзорной конференции ДНЯО 2010 года* в 2014 г. (articleVI.pircenter.org). В 2015 г. ПИР-Центр подвел итоги реализации рекомендаций в докладе *Рекомендации ПИР-Центра по укреплению режима нераспространения ядерного оружия 2010–2015* (followup2015.pircenter.org).



В этом году исполняется 20 лет с момента принятия Договора о всеобъемлющем запрещении ядерных испытаний. Несмотря на то, что он до сих пор не вступил в силу, ДВЗЯИ остается одним из краеугольных камней режима нераспространения оружия массового уничтожения. Однако положение дел в этой сфере далеко не безоблачно, поскольку над режимом продолжает тяготеть груз неизжитых и новых проблем. Продолжающееся развитие военной ядерной программы Северной Кореи (которая провела очередные испытания ядерного взрывного устройства в январе этого года), отказ крупнейших мировых игроков, включая США и Китай, от ратификации договора и пренебрежительное отношение к этому документу со стороны ряда государств ставят этот важнейший международно-правовой инструмент под угрозу.

Эти и другие темы исполнительный секретарь Подготовительной комиссии Организации по Договору о всеобъемлющем запрещении ядерных испытаний Лассина Зербо затронул в своем интервью главному редактору *Индекса Безопасности* Ольге Мостинской.

Лассина Зербо:

«ЕСЛИ ВОЗОБНОВЯТСЯ ЯДЕРНЫЕ ИСПЫТАНИЯ, МЫ ПОТЕРЯЕМ МЕЧТУ»

— Какое именно устройство испытала КНДР? Можно ли утверждать, что это была водородная бомба, и что это означает с точки зрения развития ее ядерной программы?

— В рамках Договора о всеобъемлющем запрещении ядерных испытаний (ДВЗЯИ) и Международной системы мониторинга главное для нас — не определить тип устройства, а установить, имело ли место испытание ядерного

оружия, поскольку через Договор мы стремимся запретить любые испытания, направленные на разработку или совершенствование ядерного оружия.

КНДР заявила о проведении испытаний, но еще до того, как было сделано заявление, мы заметили подозрительную активность в той части полуострова, которая обычно используется в качестве испытательного полигона. Впоследствии КНДР подтвердила ведение в том районе деятельности, обнаруженной нашей системой. Предварительный анализ показал, что данное событие аналогично имевшему место в 2013 г. не только с точки зрения места — район проведения испытаний был тот же, что и в трех предыдущих случаях, — но и с точки зрения магнитуды. Поскольку магнитуда была аналогичной или даже меньшей, чем в прошлый раз, некоторые эксперты считают маловероятным, что речь может идти о водородной бомбе. Любому ученому известно, что между атомной и термоядерной бомбой есть огромная разница в плане мощности, которой можно достигнуть, и в плане магнитуды вызванного взрывом землетрясения.

Однако первый наш вывод на основании имеющихся данных заключается в том, что имело место не природное явление, а взрыв. Сейчас мы ждем обнаружения радиоактивных изотопов, которые могли бы подтвердить, что речь идет именно о ядерном испытании. В проанализированных нами первых пробах уровень радиоизотопов находится в пределах нормы, но анализ проб продолжается. Вот что мы имеем на сегодняшний день.

— Придется подождать, пока ветер подует в направлении одной из станций, чтобы взять пробы воздуха?

— Воздушные потоки с полуострова уже дважды достигали первой станции на территории Японии — через 24 часа и 36 часов после объявленного испытания. В 2013 г. первые данные о выбросе радионуклидов были получены через 55 дней после того, как была зафиксирована сейсмическая активность. А в 2006 г. радиоактивные изотопы уже через 12 дней достигли не только Японии, но и Канады. По имеющимся данным, по прошествии 36 часов аномальных показаний зафиксировано не было. Однако это совсем не означает, что их не будет зафиксировано вообще. Радиоактивные изотопы должны попасть в атмосферу через трещины в земле, прежде чем их подхватит ветер. В данный момент ветер дует в направлении Японии, поэтому мы наблюдаем за этой конкретной станцией.

На ваш вопрос о том, была ли это водородная бомба и означает ли это, что КНДР усовершенствовала имеющуюся у нее технологию, отвечу, что если мы позволим кому-то провести ядерные испытания один, два, три, четыре раза, то можно быть уверенным, что каждое из них будет способствовать развитию ядерной программы этой страны. Именно поэтому необходимо исключить саму возможность проведения испытаний, будь то атомной, водородной или любой другой бомбы.

— Примерно месяц назад, когда была зафиксирована подозрительная активность на испытательном полигоне, многие не верили, что очередное испытание состоится. Выбор даты испытаний был обусловлен политическими или техническими причинами?

— Я был в числе тех, кто не верил в проведение испытаний. Если помните, в начале декабря я заявил, что это, вероятно, блеф. В тот момент две Кореи вели переговоры и обсуждали возможность позволить жителям Севера увидеть своих собратьев с Юга, поэтому несмотря на то, что в нашем распоряжении были спутниковые снимки, сделанные другими организациями, указывающие на перемещения на испытательном полигоне, я надеялся, что испытаний не будет.

Что касается даты, то с самого первого испытания и вообще при проведении любых других знаковых мероприятий корейские лидеры всегда использовали привязку к какому-нибудь историческому моменту, чтобы таким образом сказать международному сообществу: «Мы здесь. Не забывайте о нас». Насколько я знаю, последнее испытание было проведено за два дня до дня рождения лидера страны.

— ***В качестве подарка ко дню рождения?***

— Может быть, а может, просто решили напомнить о себе международному сообществу. Очередное знаковое событие состоится в мае — первый за 35 лет съезд партии. Есть предположения, что если в этот раз испытания провалились, в мае они могут попытаться их повторить. Об этом сейчас пишут СМИ. Считаю, что этого нельзя допустить.

Международное сообщество ведет себя слишком пассивно по отношению к Северной Корее. По той или иной причине в приоритете другие вопросы — Сирия, Ирак, Иран. Против КНДР введены санкции, но насколько они эффективны? Куба находилась под санкциями более шестидесяти лет. Если по прошествии шести десятилетий не удалось заставить народ с чем-то согласиться, наверное, надо менять подход, начинать переговоры. Мы убедились в этом на примере Кубы и Ирана — невзирая на санкции, они смогли сесть за стол переговоров. Необходимо возобновить шестисторонние переговоры с корейцами, насколько бы сложным это ни казалось.

— ***Для вступления в силу ДВЗЯИ должен быть ратифицирован еще восемью странами, в том числе США. Какие аргументы вы бы могли привести американским лидерам и законодателям, чтобы убедить их ратифицировать договор? Многие считают, что ратификация договора США стала бы мощным стимулом к его ратификации остальными странами из приложения 2.***

— Действительно, для вступления в силу договор должны ратифицировать еще восемь стран. Кто бы что ни говорил, я считаю, что в данном случае они все равны, ведь даже если наименее влиятельная страна из списка не ратифицирует договор, он не вступит в силу. Многие проводят различие между этими восемью странами. Единственное различие, которое вижу я, заключается в том, что две из этих восьми — постоянные члены СБ ООН — Китай и США, которые также являются государствами, обладающими ядерным оружием согласно Договору о нераспространении ядерного оружия. Ратификация ДВЗЯИ этими странами стала бы важнейшим шагом, подкрепляющим усилия международного сообщества по нераспространению ядерного оружия и разоружению. США и Россия заключили Договор о мерах по даль-

нейшему сокращению и ограничению стратегических наступательных вооружений в 2010 г., мы приветствуем этот шаг, который в долгосрочной перспективе будет способствовать укреплению доверия. Но на этом нельзя останавливаться. США и Китай должны ратифицировать ДВЗЯИ. При этом они не обязательно должны быть первыми из списка. Ратификация договора любой другой страной *восьмерки* показала бы хороший пример американским и китайским политикам.

Мне бы хотелось, чтобы четвертое ядерное испытание КНДР — если информация о его проведении подтвердится — стало последним напоминанием международному сообществу о важности вступления ДВЗЯИ в силу. Международное сообщество должно начать вплотную заниматься решением северокорейского вопроса и вопроса вступления в силу ДВЗЯИ, так как это единственный способ предотвратить проведение новых ядерных испытаний — и не только Северной Кореей. Ведь после того, как договор вступит в силу, проведение испытаний повлечет за собой последствия.

— ***Еще до проведения Северной Кореей четвертого ядерного испытания вы говорили, что следующим государством, которое ратифицирует ДВЗЯИ, может стать Израиль. Вы все еще так думаете? Если да, произойдет ли это в контексте создания на Ближнем Востоке зоны, свободной от оружия массового уничтожения?***

— Я всегда утверждал, что создание зоны, свободной от ОМУ на Ближнем Востоке, тесно связано с созданием в регионе зоны, свободной от ядерных испытаний. Все ближневосточные страны, перечисленные в приложении 2, подписали ДВЗЯИ. Необходимо добиться ратификации ДВЗЯИ всеми странами в регионе, это будет способствовать укреплению доверия, нераспространению ядерного оружия. Если мы не можем создать на Ближнем Востоке зону, свободную от ядерных испытаний, как можно говорить о создании зоны, свободной от ОМУ?

— ***Каковы шансы, что Израиль пойдет на это? И почему ратификация ДВЗЯИ не является частью Совместного всеобъемлющего плана действий по Ирану? Тем более что мониторинговая станция ДВЗЯИ на территории Ирана есть, она просто отключена.***

— Когда я виделся с министром иностранных дел России С. Лавровым — а и он, и президент В. Путин являются активными сторонниками ДВЗЯИ — я спросил его: «почему вы в свое время не убедили Сирию, учитывая влияние, которое Россия на нее имела, ратифицировать и подписать ДВЗЯИ?». Хотя Сирия и не фигурирует в списке стран из приложения 2, ратификация ею ДВЗЯИ способствовала бы укреплению доверия, столь необходимого на Ближнем Востоке, и ратификации договора другими государствами. Эта возможность, увы, упущена.

Что касается Ирана, я по-прежнему считаю, что заключение соглашения было прекрасной возможностью, но трудность в том, что не все участники иранской сделки сами ратифицировали ДВЗЯИ. Поэтому им было нелегко вынести этот вопрос на обсуждение, ведь если вы скажете мне, что крыль-

цо моего дома грязное, а при этом у вас самих дома беспорядок, я отвечу: «На себя посмотрите».

Однако сейчас, как мне кажется, настало подходящее время поднять этот вопрос. Ратификация ДВЗЯИ позволила бы Ирану еще раз продемонстрировать, что у него нет намерения нарушать договоренности.

Что касается Израиля, если Иран пойдет на ратификацию, это будет важным шагом по укреплению доверия. В этом случае Израиль мог бы последовать примеру Ирана. Если Израиль и Иран договор ратифицируют, то тем самым будут созданы условия для того, чтобы к ДВЗЯИ присоединились Египет, Сирия и остальные ближневосточные страны.

— Обсуждается ли этот вопрос с иранцами на экспертном или политическом уровне?

— Мы начали обсуждение на экспертном уровне. Иранские эксперты принимают участие в работе технического секретариата ОДВЗЯИ. Они участвуют в решении всех вопросов, касающихся обслуживания и эксплуатации нашей сети. Вы упоминали иранскую мониторинговую станцию. Когда-то Иран предоставлял нам данные. Сейчас, в связи с подписанием СВПД, вопрос подключения станции к общей сети, как и вопрос ратификации ДВЗЯИ, приобрел новую актуальность. Как только утихнет шумиха, я планирую найти возможность посетить Иран, чтобы проинформировать руководство страны о ходе реализации ДВЗЯИ и привлечь их к диалогу на более высоком уровне. Я озвучивал это предложение это в беседе с министром иностранных дел Мохаммадом Зарифом год назад, еще до того, как было достигнуто соглашение по сделке. С тех пор мы не встречались, но надеюсь увидеть его в ближайшее время и обсудить этот вопрос.

— КНДР пока остается единственной страной, проводившей ядерные испытания в XXI веке. Многие считают, что страны Запада слишком цивилизованы, чтобы возобновить ядерные испытания. Однако следует учитывать, что развитие военных ядерных технологий продолжается, просто на смену физическим испытаниям пришло компьютерное моделирование. Как вы думаете, нет ли риска, что по мере развития ядерных технологий западные страны могут захотеть провести еще один раунд ядерных испытаний, чтобы собрать данные для обновления своих компьютерных моделей?

— Знаете, мне нравится ваш подход. Для совершенствования технологий действительно необходимы испытания. В случае вступления ДВЗЯИ в силу присоединившиеся к договору страны не смогут развивать технологии, поскольку, как вы абсолютно верно заметили, компьютерное моделирование требует все больше и больше данных. Таким образом, чем дольше вы отказываетесь от проведения испытаний, тем меньше вероятность того, что используемая вами модель эффективна. Поэтому мы и говорим: давайте введем ДВЗЯИ в действие, чтобы не позволить странам, которые его ратифицировали, совершенствовать военные технологии, чтобы мы могли сконцентрироваться на разоружении. Тогда актуальность наличия и уровня средств сдерживания будет постепенно уменьшаться, ибо ратифицировав-

шие договор страны осознают, что не могут усовершенствовать технологии и находятся примерно на схожем уровне.

— А если разрешить странам из приложения 2 провести еще один раунд испытаний в обмен на последующую всеобщую ратификацию?

— Вы говорите, как дипломат. Возможно, дипломат бы поступил бы именно так, но я, как, прежде всего, ученый, не пошел бы этим путем. Я бы предпочел запретить испытания раз и навсегда. Разговоры о том, что надо позволить всем еще раз провести испытания и тем самым получить достаточно данных для дальнейшего совершенствования технологий, по сути, тормозят процесс, поскольку тогда через пятьдесят лет ядерные страны могут снова сказать: «Нам необходимо провести новые испытания, давайте отступим от ДВЗЯИ и проведем их». Суть в том, чтобы не проводить испытаний вообще. Если кто-то хочет проводить испытания, это значит, что они переживают из-за того, что после вступления договора в силу у них не будет возможности совершенствовать технологии и компьютерные модели. Поэтому давайте остановимся сейчас.

— В 2016 г. мы отпразднуем 20-ю годовщину ДВЗЯИ. Чего добилась организация и в каком направлении вы планируете двигаться?

— Лучше сказать, отметим. Праздновать я буду, когда смогу добиться ратификации со стороны США, Китая, Израиля, Египта или Ирана или присоединения к мораторию на проведение испытаний ядерного оружия Северной Кореи, Индии или Пакистана. И не к добровольному мораторию, а к имеющему обязательную силу мораторию в рамках данного договора. Именно поэтому мы над этим работаем: любой шаг со стороны Индии, Пакистана, Израиля, Египта, Ирана, США, Китая или Северной Кореи в сторону присоединения к договору станет для меня поводом для праздника.

При этом стоит отметить, что мы хотим, чтобы двадцатая годовщина стала поводом подумать над тем, где мы сейчас находимся. Серьезны ли наши намерения насчет этого договора? Если да, то что мы можем сделать? Никто не ожидал, что двадцатилетняя годовщина начнется с ядерных испытаний КНДР. По сути, Северная Корея заявляет: «Помните, что мы есть». Имея возможность проводить испытания, они создают угрозу вокруг себя: для Южной Кореи, для Японии, Китая, США и любой другой страны, для международного мира и стабильности. Я как-то беседовал с японскими и корейскими студентами, и они спрашивали: «Г-н Зербо, почему вы запрещаете нам проводить испытания, если это может делать КНДР. Зачем мы тогда ратифицировали договор?». Ведь они думают, что мы разрешаем Северной Корее проводить испытания. То, что студенты, завтрашние лидеры, считают, что если одна страна проводит испытания, остальные должны делать то же самое, — это серьезная угроза стабильности в регионе и во всем мире. Именно поэтому вопрос о вступлении ДВЗЯИ в силу является насущным.

— Какая из перечисленных в приложении 2 стран реально могла бы следующей ратифицировать договор?

— Я по-прежнему полагаю, что следующими могли бы стать Израиль и Иран. А, может быть, США или Китай — почему нет? Возможно, они могли бы сде-

лать это вместе. Эти страны могут ратифицировать договор без какого-либо ущерба для себя. Если взять Иран, то выполнение СВПД делает ратификацию договора актуальной.

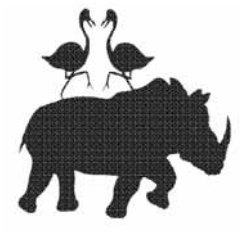
Что касается Израиля, то что ему терять? А выиграть он может очень много за счет укрепления доверия в регионе. Учтите еще тот факт, что сейчас он получил гарантии того, что Иран не занимается ничем, кроме развития мирного атома.

Что касается США и Китая, президент Б. Обама сделал этот вопрос приоритетным, и его администрация усердно над ним работает. Мы помогаем, чем можем, сотрудники секретариата выполняют очень важную работу, которая позволяет в режиме реального времени обнаруживать подозрительную активность. Это означает, что деньги американских налогоплательщиков тратятся не зря. Я считаю это достаточно веской причиной, чтобы рассмотреть возможность ратификации.

Но, что более важно, сегодня я хотел бы обратить внимание международного сообщества на неустойчивость созданной нами отличной системы. Она неустойчива, поскольку, если договор не вступит в силу, есть риск, что страны начнут выходить из договора и снова проводить ядерные испытания. В этом случае мы потеряем двадцать лет тяжелой работы, пятьдесят–шестьдесят лет переговоров по выработке договора и мечту.

— ***Будем надеяться, что этот год принесет не только ядерные испытания, но и положительные изменения.***

— Именно для этого нам и нужны такие люди, как вы, — чтобы как можно больше людей узнало о важности договора и о том, в каком направлении нам следует двигаться.



ИНТЕРВЬЮ

С 28 июня по 1 июля 2016 г. в Нью-Йорке прошла 66-я сессия Консультативного совета при Генеральном секретаре ООН по вопросам разоружения. На повестке дня стояли вопросы ядерного нераспространения, создания зоны, свободной от ОМУ на Ближнем Востоке, а также связь между оружием массового уничтожения, кибербезопасностью и терроризмом. В интервью *Индексу Безопасности* член Совета, советник ПИР-Центра Владимир Орлов рассказал о ходе обсуждений, достигнутых результатах и планах на будущее.

Владимир Орлов:

«ГЛАВНАЯ УГРОЗА ДЛЯ НЕРАСПРОСТРАНЕНИЯ В ТОМ, ЧТО КАЖДЫЙ ТЯНЕТ ОДЕЯЛО НА СЕБЯ»

— Первым пунктом на повестке 66-й сессии Консультативного совета по вопросам разоружения стояли вызовы, с которыми сталкивается ДНЯО. В чем сейчас состоит главная угроза для договора и режима ядерного нераспространения?

— В том, что каждый тянет одеяло на себя. В результате размывается консенсусный подход — а ведь именно он позволял в *успешные* для ДНЯО пятилетки цементировать режим, минимизировать риск его эрозии.

Провал Обзорной конференции ДНЯО 2015 г., непосредственным свидетелем чего я был, вообще-то настраивает на мрачные размышления. Соединенные Штаты, Великобритания и примкнувшая к ним Канада пошли на поводу у своего союзника, даже не являющегося членом ДНЯО, — и это вопреки воле большинства к принятию итогового документа, к движению вперед, а не к сползанию назад. *Досадно и тревожно* — так отреагировал Генеральный секретарь ООН Пан Ги Мун на провал обзорной конференции 2015 г., когда встречался с членами нашего Совета. Я разделяю эту оценку.

Чтобы нащупать возможные развязки, чтобы избежать *проседания* Договора, наш Совет уделил на своей летней сессии вопросам обзорного процесса ДНЯО и его перспективам на 2016–2020 гг. первостепенное внимание. Мы оказались солидарны в том, что беспокойство вызывает как провал попытки принять заключительный документ в 2015 г., так и отсутствие обсуждений по существу многих ключевых проблем ядерного нераспространения в ходе конференции. Государства сделали свои официальные заявления, обозначили позиции, а дальше началась лихорадочная кулуарная работа: кого — над сборкой *пазла* под названием *заключительный документ*, кого — над проталкиванием своих эгоистических интересов, кого — над *перепиливанием рельса*. Но слишком мало было попыток выстроить диалог по сложным вопросам-раздражителям, сократить дистанцию по ним, поставить диагноз — и начать лечение.

В связи с этим у меня особую тревогу вызывает тот факт, что за повторением мантры о *трех основополагающих столпах ДНЯО* — ядерном нераспространении, ядерном разоружении и мирном использовании ядерной энергии — ряд участников обзорного процесса не готовы видеть большее: взаимосвязанность этих столпов. Кроме того, есть вопросы, лежащие как бы на границе между ядерной и прочей стратегической проблематикой: в частности, стратегическое неядерное оружие с использованием гиперзвуковых технологий. Или возьмите взаимосвязь стратегических ядерных вооружений и оборонительных, противоракетной обороны. Вроде бы все эту связь признают, но, когда доходит до практических обсуждений, отмахиваются: мол, не будем обсуждать ПРО, оно же не имеет прямого отношения к ДНЯО. Есть и другие подобные примеры.

Необходим холистический подход к международному режиму ядерного нераспространения. Поэтому мне представляется принципиально важной констатация, сделанная нашим Советом, что ДНЯО — не просто нераспространенческий и разоруженческий договор, это краеугольный камень международной безопасности. Мы рекомендуем обратить внимание на усиливающийся разрыв между анализом ДНЯО и анализом всего состояния международной безопасности. Сокращая этот разрыв, мы снизим риски.

— Считает ли Совет, что одна из причин пробуксовки обзорного процесса — отсутствие секретариата или иного административного механизма для ДНЯО?

— Тут есть различные точки зрения. Что вообще-то хорошо: можно поспорить, подискутировать. Да, кому-то кажется нелогичным, что, например, у Конвенции о запрещении химического оружия (КЗХО) или же даже у не вступившего в силу ДВЗЯИ есть свои организационные механизмы, а у ДНЯО — нет. Лично я здесь проблемы не вижу, как и не вижу необходимости создания *секретариата* обзорного процесса ДНЯО. Дело не в наращивании бюрократии (хотя, может быть, кому-то из дипломатов, кто готовится к пенсии и хотел бы *нагреть* себе место в новом секретариате, мое замечание не покажется столь уж очевидным).

Может быть, стоит даже *наоборот* посмотреть: в 1995 г. было решено увеличить продолжительность сессий Подготовительного комитета к обзорным конференциям. Мотивация была правильная: помимо оргвопросов Препкомы должны вести обсуждение ключевых проблем по существу, чтобы подготовить к этим дебатам — в конструктивном ключе — участников обзорных конференций. Но этого не полу-

чилось. Когда мы приходим на обзорные конференции, почва не *разрыхлена*, не *удобрена*. Либо надо повышать качество и результативность таких обсуждений по существу вопросов на Препкомах, либо вернуться к их большей компактности, а не отвлекать большие делегации аж на две недели. У них в своих столицах дел по горло. Но, повторяю, это мое личное мнение.

Что касается Совета, то мы согласились в том, что одним из рецептов может быть назначение председателя обзорных конференций на гораздо более раннем этапе, чем это делается сейчас, чтобы позволить председателю заблаговременно подготовить и себя самого, и, главное, государства-участники, к качественным и конструктивным дебатам в ходе обзорных конференций с целью наиболее продуктивного рассмотрения действия Договора.

— ***По итогам ОК ДНЯО 2015 г. переговорный формат по ЗСОМУ был фактически ликвидирован. Что могло бы его заменить?***

— Мы все согласились в том, вопрос о ЗСОМУ на Ближнем Востоке занял центральное место в ходе обсуждений на Обзорной конференции ДНЯО 2015 г. и стал основным катализатором ее провала. Именно поэтому мы решили обратиться к данному сюжету безотлагательно. К тому же именно к этому нас призвал Генеральный секретарь ООН. Встречаясь с нами, он обратил наше внимание на срочность вопроса, подчеркнув, что создание такой зоны «будет нести очевидные выгоды для безопасности в регионе и во всем мире».

Мы рассмотрели вопрос о ЗСОМУ как в контексте ДНЯО, так и вне этого контекста, обсудили позиции ключевых игроков, а также усилия, которые могли бы быть приложены для активизации процесса.

Мы констатировали, что провал принятия заключительного документа Обзорной конференции ДНЯО 2015 г. привел к образованию вакуума в обзорном процессе, равно как и в процессе выполнения ближневосточной резолюции 1995 г. Этот вакуум также распространился на разработанный в 2010 г. механизм по созыву конференции с участием всех государств Ближнего Востока с целью начать процесс создания зоны.

Совет высказал мнение, что Генеральный секретарь ООН является лучшей кандидатурой для того, чтобы возглавить усилия по заполнению образовавшейся пустоты новыми инициативами и идеями для привлечения всех сторон к столу переговоров. При этом мы помнили, что сказал нам Пан Ги Мун при прошлогодней встрече: «Я сделаю все от меня зависящее для достижения этой цели».

— ***Что конкретно мог бы предпринять Пан Ги Мун?***

— Во-первых, пригласить три государства — депозитария ДНЯО (они же — соавторы резолюции 1995 г.) для обсуждения с ними плана по активизации процесса создания ЗСОМУ на Ближнем Востоке. Во-вторых, провести консультации с государствами региона. В-третьих, от своего имени и от лица трех государств-депозитариев ДНЯО, выступающих в качестве соучредителей, пригласить все государства Ближнего Востока возобновить консультации по подготовке к конференции по созданию ЗСОМУ на Ближнем Востоке в соответствии с решением Обзорной конференции 2010 г.

— ***Когда, на ваш взгляд, можно было бы начать?***

— Проведение консультаций должно быть запланировано на ближайшие возможные даты.

— Но для этого нужны и площадка, и секретариат. Миссия спецкоординатора Лааявы, как я понимаю, завершена и реанимации не подлежит. Придется начинать, по сути, с нуля.

— В этом вы правы, хотя, конечно, наработан солидный опыт, и его нельзя просто так взять и *обнулить*. Даже негативный опыт — это опыт. А помимо миссии Лааявы были ведь еще и усилия предыдущих десятилетий — я говорю прежде всего об обсуждениях данной проблематики еще в начале 1990-х гг. А что касается сегодняшнего дня, то в качестве площадки и секретариата консультаций мог бы выступить Институт ООН по исследованиям проблем разоружения (ЮНИДИР), учитывая автономность и независимость этой организации, являющейся при этом частью системы ООН.

В любом случае, государства региона должны прийти к консенсусу без постороннего вмешательства, в благоприятной для них обстановке и в рамках того формата для диалога, который помогут создать соучредители.

— А должность специального координатора?

— Тут прежде всего потребуются консультации с соавторами резолюции 1995 г. и с государствами региона. Имея в виду предложенную роль Генерального секретаря ООН, на эту должность возможно было бы предложить Высокого представителя по вопросам разоружения.

— Вероятно, полномочия соавторов резолюции 1995 г. и спецкоординатора должны быть четко определены.

— Конечно. Среди прочего, им придется следить за соблюдением первоначального мандата, выданного Обзорными конференциями 1995 и 2010 гг. с тем, чтобы не допустить отхода от него стран региона; предлагать идеи и решения по преодолению возникающих в ходе переговоров сложностей; оценивать прогресс по итогам встреч и докладывать о нем Обзорной конференции и сессиям ее Подготовительного комитета.

— Но ведь консультации могут опять затянуться, и идея конференции по началу практического разговора о подготовке зоны окажется подвешенной.

— Ни в коем случае! Приемлемый график, даты и место для проведения конференции должны быть согласованы не позже первой сессии Подготовительного комитета, то есть — крайний срок! — к апрелю 2017 г. Но верно и то, что на сегодняшний момент воплощение этих идей сталкивается с трудностями.

— Непреодолимыми?

— Не знаю. Надеюсь, что нет. Но в разговоре с нами 1 июля с. г. Пан Ги Мун признался, что на данный момент он *разочарован* отсутствием какого бы то ни было прогресса и негибкостью одной из сторон. Это реалии сегодняшнего дня. Поэтому сегодня для оптимизма, для ожидания прогресса нет причин. Может быть, Лига арабских государств (ЛАГ) возьмет тут *региональную* часть домашней работы на себя? Скажем, обсудим эти вопросы в Каире в течение лета в конструктивном ключе.

— Есть ли у Консультативного совета предложения касательно того, какие рекомендации могут быть предложены для реализации в ходе самой конференции?

— Мы определили несколько направлений, где прогресс был бы возможен. Во-первых, это выработка проекта заявления, которое могли бы принять все участники конференции и в котором государства примут на себя обязательство воздерживаться от атак либо угроз атак против всех задекларированных ядерных объектов друг друга, находящихся под гарантиями МАГАТЭ. В это обязательство должны быть включены и кибератаки. Во-вторых, это разработка *дорожной карты*, которая указывала бы путь к постепенной постановке всех объектов ядерной инфраструктуры региона под гарантии МАГАТЭ. В-третьих, это подготовка договоренностей о необходимости безотлагательного принятия всеми странами региона всеобъемлющих гарантий МАГАТЭ и Дополнительного протокола. До вступления в силу государствам следует применять Дополнительный протокол на добровольной основе. В-четвертых, это формирование постоянно действующего регионального механизма по мерам доверия в ядерной, химической и биологической областях. Наконец, в-пятых, это принятие заявления, призывающего все страны региона, не сделавшие этого, ратифицировать Договор о всеобъемлющем запрещении ядерных испытаний.

Конечно, я перечислил лишь некоторые из возможных шагов. При этом не должно быть иллюзий — особенно когда дело касается Ближнего Востока. Проработка даже этих скромных инициатив потребует времени и согласия всех участников процесса. Остается вопрос и по их последовательности. К некоторым из таких шагов, как мне кажется, государства региона могут быть готовы уже в начале консультаций. Другие, не исключаю, потребуется отложить *до лучших времен*. Но ведь это не *пакет*, а опции, направления действий, которые позволили бы зацементировать прогресс в вопросе о ЗСОМУ, — именно этого прогресса нам так не хватает с момента принятия резолюции по Ближнему Востоку на конференции ДНЯО 1995 г. Поэтому даже скромный, но устойчивый прогресс мне представляется той *синицей в руках*, которая сейчас может быть важнее *журавлей в небе*.

— Думаю, Совет не смог не коснуться вопроса о КНДР?

— Мы, конечно, обратили внимание на безответственное поведение КНДР в ракетной и ядерной областях и считаем целесообразным отдельно рассмотреть вопрос об одностороннем решении КНДР о выходе из ДНЯО и об уроках, которые следует извлечь, чтобы избежать повторения подобных ситуаций впредь.

Мое мнение заключается в том, что действия КНДР последних месяцев являются контрпродуктивными, дестабилизирующими региональную безопасность. Однако, согласитесь, что есть определенная трудность, когда Северную Корею призывают отказаться от ядерных испытаний в том числе и те государства, которые сами блокируют вступление в силу ДВЗЯИ своей неготовностью к его ратификации.

Вообще, на мой взгляд, ядерное испытание КНДР 2016 г. только стимулирует необходимость возобновления многостороннего диалога с участием КНДР. В ходе такого многостороннего диалога о всеобъемлющем решении ситуации вокруг ядерной программы КНДР и о придании безъядерного статуса всему Корейскому полуострову возможно достижение промежуточного соглашения, согласно которо-

му Пхеньян воздержался бы от дальнейших ядерных испытаний, испытаний ракет, наработки ядерных материалов и распространения чувствительных материалов и технологий в обмен на смягчение санкций, предоставление помощи и гарантии безопасности.

Понятно, что это деликатный и многотрудный процесс. Но альтернативы ему я не вижу. Некоторые члены Совета, в свою очередь, убеждены, что ни о каком диалоге с КНДР не может быть и речи, пока она не проявит искреннее стремление к выполнение всех действующих резолюций СБ ООН.

— ***Нельзя не обратить внимание на пункт в повестке дня Совета* о взаимосвязи между оружием массового уничтожения, кибербезопасностью и терроризмом*. Тема модная, но ведь ей уже занимаются различные международные организации?***

— И да, и нет. Члены рабочей группы отметили, что уже существует целый ряд механизмов, направленных на противодействие химической, биологической, радиологической и ядерной угрозе, включая договоры и политически обязывающие соглашения. Сюда относятся, в частности, резолюция СБ ООН 1540 и деятельность МАГАТЭ в области обеспечения ядерной безопасности. Кроме того, было отмечено, что связь между терроризмом и кибербезопасностью в целом и ее различными аспектами, такими как противодействие использованию интернета для организации террористических актов, также рассматривается в других форматах и не нуждается во внимании со стороны Совета.

В то же время Совет отметил, что сопряжение трех элементов — терроризма, кибератак и угрозы, исходящей от оружия массового уничтожения (ОМУ), — является действительно новым вызовом, относящимся к его мандату.

Таким образом, члены Совета решили сконцентрироваться на возможном использовании террористами ОМУ в сочетании с кибератаками, что представляет собой угрозу миру и безопасности. Подобное сочетание, в зависимости от конкретной ситуации, может привести к значительным жертвам (или тяжелым социальным и экономическим последствиям) с эффектом, равным или превосходящим эффект от применения ОМУ.

Должен заметить, что члены Совета в ходе сессии изучили доклад, подготовленный ПИР-Центром в рамках исследования, проводимого под эгидой Всемирного экономического форума и в сотрудничестве со швейцарским центром Centre Russe, о взаимосвязи между кибербезопасностью и безопасностью объектов гражданской ядерной энергетики в мире.

— ***Какие первоочередные угрозы и вызовы были выявлены?***

— Самым большим риском является угроза критической инфраструктуре, использующей или хранящей значительное количество химических, биологических, радиологических или ядерных материалов. Подобная инфраструктура бывает как гражданской, так и военной, а нередко — двойного применения. Примерами могут служить химические заводы, ядерные реакторы, комплексы по обогащению урана и переработке ядерного топлива, исследовательские биологические лаборатории и медицинские учреждения.

Риск террористических кибератак, направленных против вооружений, средств доставки и инфраструктуры обеспечения, особенно инфраструктуры, отвечающей за доставку боезарядов, был оценен нами как невысокий из-за предположительно большей защищенности военной инфраструктуры. Однако он все же не нулевой, и это уже само по себе тревожно.

Концептуальный документ, подготовленный членом Совета Тревором Финдли (Австралия), показал, что, согласно предварительной оценке, риск кибервоздействия на химическое, биологическое и радиологическое оружие оказался ниже, чем риск воздействия на ядерное оружие, поскольку химические, биологические и радиоактивные материалы не развернуты для быстрого применения. Совет отметил, что данный вопрос заслуживает дальнейшего исследования.

Помимо этого, мы приступили к детальному рассмотрению вопроса об укреплении физической ядерной безопасности (ФЯБ) для противодействия кибертерроризму.

Мне приходилось заниматься вопросами ОМУ-терроризма по протяжении последних двадцати лет. 15 лет назад я пришел к выводу — и озвучил его в своих презентациях и исследовательских докладах — что крупнейшие и наиболее финансово дееспособные международные террористические организации стремятся к проведению *комбинированного* террористического акта в крупном мегаполисе с использованием радиологического, химического или биологического оружия против населения при одновременной кибератаке на транспортные, банковские и иные элементы критической инфраструктуры мегаполиса. Тогда же по заказу правительства Москвы ПИР-Центр подготовил отдельный доклад по данному вопросу, где эта моя гипотеза получила свое подтверждение и развитие. С тех пор зависимость мегаполисов и объектов критической инфраструктуры в них от компьютерных сетей стала неизмеримо выше. Возросли и финансовые возможности террористов. И если возможность несанкционированного доступа к ядерному оружию и оружейным делящимся материалам, и 15 лет назад бывшая низкой, сегодня еще более снизилась, то этого же, к сожалению, нельзя сказать о возможностях доступа к химическим или радиологическим материалам (о *биологии* мне судить сложнее).

— ***Какие вопросы в связи с этим требуют более тщательного рассмотрения?***

— Во-первых, нормы, регулирующие мирное использование кибертехнологий, а также право на мирное использование химических, биологических и ядерных технологий.

Во-вторых, международно-правовые механизмы, связанные с химическими, биологическими, радиологическими и ядерными материалами, такие как международные договоры относительно ОМУ, резолюция СБ ООН 1540 и более специализированные договоры, такие как Международная конвенция по борьбе с актами ядерного терроризма.

В-третьих, существующее международное сотрудничество и дальнейшее укрепление потенциала в области химических, биологических, радиологических и ядерных материалов, кибертехнологий и противодействия терроризму.

Конечно, есть и целый ряд точечных вопросов, мимо которых мы не сможем пройти. Перечислю только некоторые из них:

- природа угрозы кибертерроризма против химической, биологической, радиологической и ядерной инфраструктуры, как в случае с инфраструктурой, подключенной к интернету, так и для систем, которые теоретически должны быть от интернета отключены;
- значимость внешних и внутренних угроз в контексте подобных атак;
- необходимость уточнения и разграничения обязательств государства и отрасли в противодействии этим угрозам и усиления взаимодействия между ними;
- необходимость международной поддержки и укрепления потенциала для противодействия обозначенным угрозам, особенно в отношении развивающихся стран или государств, только начинающих развивать критическую инфраструктуру в особо чувствительных областях, например строить ядерные реакторы;
- оценка правовой и регуляторной системы государств на предмет готовности к противодействию подобным угрозам;
- оценка подхода международных организаций к данному виду угроз, учета угроз в планировании деятельности организаций и уровня сотрудничества между ними.

Как видите, уже солидный список получился, и он потребует тщательной проработки. При этом мы не можем игнорировать и такой фактор, как необходимость нахождения оптимального баланса между транспарентностью, с одной стороны, и конфиденциальностью, с другой, при реализации международного сотрудничества в данной конкретной — и очень чувствительной — области.

Должен сказать, что Генеральный секретарь ООН проявил особый интерес к данной проблематике, особенно к таким вопросам, как *связка* ядерного терроризма и кибербезопасности, а также *связка* кибербезопасности с физической ядерной безопасностью (ФЯБ). Дискуссии стартовали. Приоритеты зафиксированы. Поэтому мне очевидно, что данные вопросы получат дальнейшее развитие на площадке ООН в 2017 г., безотносительно того, кто займет кресло Генерального секретаря тогда.

— Вы обсуждали этот вопрос в Нью-Йорке — и, судя по всему, в конструктивном, динамичном ключе — в то же самое время, когда в Женеве еще глубже завязла в пробуксовке Конференция по разоружению. Между тем, на вашей повестке дня — вопрос остро актуальный с точки зрения глобальной безопасности.

— Да, есть нестыковка в том, что на разоруженческой повестке дня есть остро актуальные вопросы, где на кону может быть судьба безопасности целых регионов мира, между тем как КР погрязла в процедурных вопросах. Мне кажется, оптимальное решение предложил министр иностранных дел России С. В. Лавров, выступая на КР: «подумать о начале переговоров по новой теме, которая могла бы сыграть объединяющую роль, но до сих пор не фигурировала при обсуждении проекта программы работы Конференции. Таковой, на наш взгляд, могла бы стать проблематика, находящаяся на стыке разоружения, нераспространения и антитеррористических усилий».

Как вы знаете, Россия предложила приступить к разработке отдельной конвенции по борьбе с актами химического терроризма. Как вариант, сюда можно добавить и беспокоящий всех нас биотерроризм, который уже *проклевывается* в ряде регио-

нов планеты, в частности в Африке. Конечно, есть целый ряд международных площадок, на которых этим можно было бы заняться, и в Москве это прекрасно понимают. Но предлагают сделать это именно в Женеве, именно на Конференции по разоружению, которая ранее внесла весомый вклад в снижение химической угрозы путем успешного согласования КЗХО. Как сказал С. В. Лавров, тем самым была бы решена двуединая задача — противодействия химтерроризму, с одной стороны, и разблокирования работы женевского разоруженческого форума, с другой.

Мне такой подход представляется творческим, нестандартным, заслуживающим внимания. В потенциале он — прорывной, живительный для уже *мхом поросшей* Конференции по разоружению. Генеральный секретарь ООН поделился с нами своей озабоченностью от этой уже слишком затянувшейся пробуксовки КР. Уже в октябре, на Первом комитете, могут начаться необратимые процессы, которые убьют КР.

— Консультативный совет по вопросам разоружения является, согласно своему мандату, также и Попечительским советом ЮНИДИР — института, о котором вы уже упомянули выше в контексте ЗСОМУ на Ближнем Востоке. Насколько интенсивно идет работа Наблюдательного совета, каковы ее результаты?

— Очень интенсивно. Иногда мы посвящаем до четверти нашего времени вопросам развития ЮНИДИР. А я, будучи членом подкомитета нашего Совета по ЮНИДИР, иногда даже и больше. Это не случайно. ЮНИДИР — уникальная, ценная структура. При этом в системе ООН это очень небольшая по размеру *деталь*, причем автономная. Все это открывает перед институтом редкие возможности, но одновременно и влечет те сложности, с которыми другие институты, занимающиеся разоруженческой проблематикой, не сталкиваются. Как сделать так, чтобы институт максимально использовал свои преимущества, — задача его руководства, но наш Совет предлагает здесь свое видение и свои рекомендации.

Прошлый год был для ЮНИДИР трудным. Я рад, что в 2016 г. он вошел с куда большим оптимизмом. На 20% увеличились добровольные взносы на реализацию программ, да и само число доноров выросло с двадцати до тридцати. Не менее важно, что резолюция Генассамблеи ООН 70/69, принятая 7 декабря 2015 г. по случаю 35-летия ЮНИДИР, создает основу для повышения финансирования института со стороны самой ООН. Это давно назревшее решение. Директор ЮНИДИР Ярмо Сарева сформулировал свое четкое видение стратегии развития института.

— Когда завершится мандат нынешнего директора?

— В конце текущего года. Конкурс на должность директора ЮНИДИР открыт. Совет участвует в процессе отбора — своим советом, простите за тавтологию. Насколько я понимаю, Генеральный секретарь ООН должен будет определиться с результатами отбора до конца 2016 г.

— Консультативный совет по вопросам разоружения действует при Генеральном секретаре ООН. Насколько тесно организовано взаимодействие непосредственно с генсеком?

— Да, это именно взаимодействие, двусторонний процесс. Мы направляем Генеральному секретарю ООН наши рекомендации: ежегодно или даже чаще. Послед-

нее письмо Совета Генеральному секретарю было сконцентрировано на проблематике ЗСОМУ на Ближнем Востоке: это, пожалуй, самый тяжелый вопрос, стоящий на сегодняшней повестке дня.

Пан Ги Мун встречается с нами, определяет приоритетные темы. В этом году, по-моему, акценты расставлены очень своевременно.

1 июля, когда Генеральный секретарь снова встретился с нами, определенный отпечаток на разговор наложил тот факт, что Пан Ги Мун уходит. «Сегодня ровно 6 месяцев до того, как уйду, — ни днем раньше, ни днем позже», — сказал он нам во время рабочего обеда. — «Но я останусь к вашим услугам», — продолжил он, отметив, что проблематика ядерного разоружения, в отличие, например, от проблематики изменения климата, не стала прорывной за время его работы, а от этой проблематики все равно никуда не уйти.

Мы в откровенном диалоге обсудили, что можно было бы здесь реалистично сделать до истечения его мандата, а что достанется уже его преемнику. Я ознакомил Пан Ги Муна с некоторыми рекомендациями, содержащимися в майском докладе ПИР-Центра по вопросам укрепления международного режима ядерного нераспространения на 2016–2020 гг.

О чем говорили? Конечно, о Ближнем Востоке (в том числе о создании зоны, свободной от ОМУ в этом регионе). Конечно, о ситуации вокруг КНДР. О Договоре о запрещении ядерных испытаний — вопрос, к которому Генеральный секретарь очевидно неравнодушен. Мне показалось своевременным обратить внимание на важность расширения и укрепления системы мониторинга, которая действует в ПК ОДВЗЯИ.

Отдельная тема — как продвигать образование в области нераспространения и разоружения, включая новые инициативы в этой области, которые исходят от ПИР-Центра, МГИМО и Миддлберийского института международных исследований. Как вовлекать в этот процесс молодежь. Как работать в условиях по сути новой холодной войны, в условиях возрастания риска ядерной эскалации с гражданским обществом.

В последнем разговоре с Генеральным секретарем я поднял, среди других, вопрос о стратегическом оружии в неядерном оснащении, в частности гиперзвуковом, которое разрушает стратегическую стабильность. Считаю, что вопрос о предотвращении гонки вооружений в этой области требует дальнейшей проработки. ПИР-Центр в своих Рекомендациях предложил созвать конференцию для проработки данного вопроса на экспертном уровне. Поделился этой идеей с Пан Ги Муном.

Зашла речь и о новых угрозах — таких, как *сращивание* кибер- и ядерного терроризма. Было заметно, что этот вопрос особенно беспокоит руководство ООН.

И было приятно, когда на прощание Пан Ги Мун сказал мне «большое спасибо» на хорошем русском языке.

Вадим Козюлин
Альберт Ефимов

НОВЫЙ БОНД — МАШИНА С ЛИЦЕНЗИЕЙ НА УБИЙСТВО

Кто из киноманов не мечтал познакомиться с Джеймсом Бондом, агентом 007? Сегодня эксперты начинают верить, что в недалеком будущем это станет возможным. Только, вероятно, Джеймс Бонд будет железным, и его будут называть не *агент*, а *модель 007.* Но два ноля, как и в номере Бонда, будут означать *лицензию на убийство*.

Как будет выглядеть война будущего? Вот как ее описывает заместитель министра обороны США Боб Ворк: «Совместные действия пилотируемых и непилотируемых платформ станут обычной практикой. Потенциал автономных беспилотных систем будет постоянно возрастать. [...] Мы считаем, что будущие войны будут характеризоваться очень высокой степенью симбиоза человека и машины, что, например, позволит простейшим платформам контролировать целые скопления недорогих беспилотных систем, которые могут гибко комбинироваться и в большом количестве выдвигаться на поле боя»[1].

Со времен окончания Второй мировой войны технологическое превосходство над потенциальным противником является основой военной доктрины США. Разработка любого нового вида вооружений всегда вызывает так называемый *туман войны* [fog of war], который в нашем случае состоит из постоянного медийного шума вокруг возможного появления роботов-убийц, автономного оружия и т. п. Но факты боевого применения роботов уже невозможно скрыть, и, по мере появления на вооружении армий мира беспилотных и автономных видов вооружений, мировая общественность стала все решительнее ставить вопрос о необходимости ограничить или хотя бы упорядочить их применение.

Многочисленные жертвы среди мирных жителей в результате ракетных ударов американских беспилотников в Афганистане и Пакистане, или так называемый *побочный ущерб* [collateral damage], придавали и придают этой дискуссии особенную остроту. В обсуждение и осуждение бездушных роботов-убийц вовлеклись простые граждане и политики, а также известные ученые, популярные артисты и общественные деятели (например, Стивен Хокинг и Илон Маск). Энергии масс и авторитета политиков должно было хватить для принятия на международном уровне конвенции об ограничении применения боевых роботов, как это случилось, скажем, с противопехотными минами с принятием Оттавской конвенции

в 1997 г., или кассетными боеприпасами, запрещенными Дублинской конвенцией в 2008 г. Но возникло непредвиденное обстоятельство: боевые роботы оказались довольно скользкой субстанцией, ускользающей от регуляторов не хуже, чем жидкие терминаторы в фантастическом кино.

Как известно, дать название значит решить половину проблемы. Дать твердое определение понятию *боевой робот* оказалось непростой задачей. Обсуждение этого вопроса продолжается несколько лет, и пока сложился лишь рабочий вариант понятия *боевые автономные системы* — БАС [LAWS — Lethal Autonomous Weapon Systems]. Они определяются как вооружения, которые могут самостоятельно (независимо от человека) выбирать и атаковать цели, то есть автономно выполнять *критические* функции по обнаружению, отслеживанию, наведению и поражению объектов. Эта формулировка пока не получила юридического закрепления в международных документах, и дискуссия о ее надежности далеко не закончена. Однако такое определение позволило задать направление для рассмотрения проблемы с различных сторон.

Эксперты справедливо отмечают, что роботизированные системы заведомо страдают рядом опасных болезней: они не способны принимать сложных решений и учитывать многие обстоятельства, как это делает человек; они не в состоянии осознавать окружающую обстановку или адаптироваться к непредвиденным обстоятельствам — то есть они не могут действовать вне рамок заранее определенного и довольно ограниченного окружения. Однако они совершенствуются, что потенциально может привести как к впечатляющему успеху, так и к абсолютной катастрофе.

Термин БАС, естественно, включил в себя перспективные вооружения, а именно: нашумевшие автономные беспилотные летательные аппараты (дроны); успевшие проявить себя в конфликтах *умные* бомбы и пока не применявшиеся перспективные барражирующие боеприпасы; *умные* сетецентрические, то есть коварно поджидающие своего *клиента* мины. Кроме того, под определение попали вооружения, о разработке которых до сих пор только ходят слухи: подводные планирующие дроны, космические *терминаторы*, вредоносные всепроникающие нанороботы, а также гиперзвуковые ракеты.

Однако выяснилось, что определение не то чтобы хромает, но меряет слишком широким аршином: под него также подпадает значительное количество образцов вооружений, которыми человечество пользуется лет 50 и даже 100, и которые до этого никто не думал заподозрить в избыточной роботизированности. Под термин *боевые автономные системы* подошли и вполне архаичные торпеды, и ракетно-пушечные системы противовоздушной и противоракетной обороны, баллистические и крылатые ракеты, ракеты *воздух-воздух*, противокорабельные ракеты, корректируемые авиабомбы и системы активной защиты, которые уже лет 30 устанавливают на броню для защиты от противотанковых ракет. Такая ситуация создает проблему: как (и надо ли) выделять именно ту опасную степень автономности роботов среди множества функций, которые существующие вооружения уже десятилетия выполняют самостоятельно?

Организация Human Rights Watch предложила систему деления роботов по уровню человеческого контроля, которая постепенно получает распространение среди экспертов:

1. Вооружения под управлением человека [Human-in-the-Loop Weapons]: боевые роботы, способные выбирать цели и наносить удары только по команде человека.

2. Вооружения под наблюдением человека [Human-on-the-Loop Weapons]: боевые роботы, способные выбирать цели и наносить удары под наблюдением человека-оператора, который может отменить выполняемые роботами действия.

3. Вооружения без участия человека [Human-out-of-the-Loop Weapons]: боевые роботы, способные выбирать цели и наносить удары без участия человека[2].

Следом, естественно, возник вопрос о приемлемой степени автономности, то есть независимости от контроля со стороны человека, или, если идти от обратного, о необходимом уровне человеческого контроля над машиной и об ответственности человека за действия его продукта — боевого робота. Современные машины, которые претендуют на звание роботов, превосходят человека в таких областях, как количественный анализ, выполнение повторяемых операций, обработка больших объемов информации. Однако сегодня даже ребенок даст фору роботу в качественном анализе или логическом мышлении.

Непосвященному читателю эта проблема может показаться умозрительной. Между тем в международном праве имеется ряд документов, которые при появлении боевых роботов на международной арене обязаны обозначить свое присутствие в полный рост, как шериф при появлении преступника.

Важнейший из них — Дополнительный протокол I к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов. Статья 35 п. 2. этого документа гласит: «Запрещается применять оружие, снаряды, вещества и методы ведения военных действий, способные причинить излишние повреждения или излишние страдания».

В статье 36 *Новые виды оружия* говорится: «При изучении, разработке, приобретении или принятии на вооружение новых видов оружия, средств или методов ведения войны Высокая Договаривающаяся Сторона должна определить, подпадает ли их применение, при некоторых или при всех обстоятельствах, под запрещения, содержащиеся в настоящем Протоколе или в каких-либо других нормах международного права, применяемых к Высокой Договаривающейся Стороне».

Помимо прочего этот документ обязывает Международный комитет Красного Креста (МККК) следить за исполнением Дополнительного протокола. Статья 98 *Пересмотр Приложения I* сформулирована так: «Не позднее, чем через четыре года после вступления в силу настоящего Протокола, а затем через интервалы не менее четырех лет Международный комитет Красного Креста консультируется с Высокими Договаривающимися Сторонами относительно Приложения I к настоящему Протоколу и, если он сочтет необходимым, может предложить созвать совещание технических экспертов для пересмотра Приложения I и предложения таких поправок к нему, которые могут оказаться желательными».

Еще один документ, к которому сегодня нередко апеллируют борцы с роботами, — т. н. *оговорка Мартенса* (между прочим, российского дипломата). Она гласит, что в случаях, не охваченных положениями права, «население и воюющие остаются под охраной и действием начал международного права, поскольку они вытекают из установившихся между образованными народами обычаев, из законов человечности и требований общественного сознания». Это отрывок из вступительной части IV Гаагской конвенции 1907 г., созванной по инициативе российского императора Николая II в ответ на разворачивающуюся гонку вооружений. Сегодня эта оговорка оказалась особенно востребованной, что, безусловно, должно вызывать гордость россиян за идеи человеколюбивых предков.

Соединенные Штаты и Великобритания постарались первыми развеять подозрения на свой счет и опубликовали принципы своей политики в отношении боевых роботов. Великобритания заявила, что автономное применение вооружений недопустимо, а использование систем вооружений всегда будет осуществляться под контролем человека. При этом Лондон обозначил различие между полностью автономными системами вооружений и автоматическими системами. В этой связи Великобритания делает ставку не на автономные вооружения, а на использование систем с дистанционным управлением, что, в представлении британцев, дает абсолютную гарантию контроля и ответственности за применение силы. То есть Великобритания считает, что существующих норм международного права в отношении ведения войны вполне достаточно для того, чтобы регулировать применение автономных систем вооружения.

В ноябре 2012 г. Минобороны США приняло Директиву 3000.09, определяющую американскую политику в отношении автономных систем вооружения. США заявили, что автономные и полуавтономные системы вооружений будут создаваться с целью обеспечения командирам и операторам необходимого уровня контроля над применением силы. Американцы определили для себя три типа автономных систем вооружений: полуавтономные системы вооружений, которые возможно использовать для выполнения ударных миссий (сюда вошли боеприпасы с системами наведения; беспилотные летательные аппараты с бомбами, наводимыми по GPS, и межконтинентальные баллистические ракеты); автономные системы вооружений — они признаны пригодными к нелетальному использованию (например, электронному противодействию); а также контролируемые автономные системы вооружений, которые возможно применять для поражения подвижной техники и объектов в ходе локальных оборонительных операций (например, наземных и корабельных систем ПВО или ракетных установок).

О том, как другие государства планируют использовать боевых роботов, неизвестно. И это создает нервозность. Ведь использование роботов ставит под вопрос соблюдение международного гуманитарного права (МГП), которое, среди прочего, предусматривает определенные обязательства в процессе разработки и принятия на вооружения различных оружейных систем. МГП требует обеспечение *значимого* или, иными словами, полноценного контроля со стороны человека [meaningful human control]. Однако само это определение оставляет место для самых различных трактовок, и по поводу *значимого контроля* ведутся главные споры специалистов из различных стран.

Объективности ради следует отметить, что существует и совершенно обратная точка зрения на боевых роботов. Некоторые специалисты (назовем их *робо-оптимистами*) считают, что роботы могут быть гуманнее человека. У *робо-оптимистов* свои крепкие аргументы:

- условия вооруженного конфликта погружают человека в среду, к которой он не привык и для которой он не был создан, а робот железный, ему все равно;
- роботам неведома жестокость, страх, стресс, что свойственно человеку;
- роботам неведом инстинкт самосохранения, и они не будут стремиться защитить себя любой ценой;
- роботы не были замечены в случаях насилия, их не захлестнут эмоции, для них пока не придуманы программы пыток или казней;
- их сенсоры (инфракрасные, лазерные и другие) позволяют им лучше видеть некоторые параметры окружения, а электроника позволяет, в некотором смысле, лучше оценить обстановку;
- записывающие устройства позволят точно определить лицо, ответственное за выдачу роботу нелегитимного приказа, то есть расплата найдет героя по записи на флешке лучше Гаагского трибунала.

Робо-скептики, в свою очередь, указывают на ряд принципиальных недостатков современных технологий, которые на десятки, если не на сотни лет отодвигают срок возникновения по-настоящему автономных роботов-терминаторов.

Полноценный искусственный интеллект (ИИ), которым должны обладать железные убийцы, еще не создан и едва ли появится в обозримом будущем. Сегодня компьютер может обыграть человека в шахматы, *камень, ножницы, бумагу* или го. Для победы в игре с твердо определенными правилами машине достаточно всего лишь выбрать лучший ход из миллиона имеющихся в ее памяти или уметь делать простые движения быстрее человека. Но что происходит с машиной, когда условия, в которых роботу приходится применять свои запрограммированные навыки, заранее неизвестны, либо меняются с такой скоростью, что уследить за ними крайне сложно, а правила игры (которая и не игра вовсе) меняются по ходу самой игры? Прошедшие испытания Агентства по перспективным оборонным научно-исследовательским разработкам (DARPA) под названием DARPA Robotics Challenge показали, что задача открыть дверь в комнату для робота уже является довольно сложной.

Искусственный интеллект трудно создать, ибо пока люди не разобрались даже с пониманием того, что такое интеллект естественный. Ян Лекун, один из ведущих ученых в области искусственного интеллекта и искусственных нейронных сетей, комментируя победу компьютерной программы над чемпионом мира по го, написал на своей странице в Фейсбуке: «…Большая часть процесса обучения у людей и животных — это обучение без учителя. Если представить интеллект в виде торта, то обучение без учителя — это сам торт, обучение с учителем — глазурь на нем, а обучение с подкреплением — вишенка. Мы знаем, как сделать глазурь и вишенку, но не знаем, как сделать торт. Мы должны решить проблему обучения без учителя, прежде чем сможем даже задумываться о том, что приближаемся к созданию

подлинного ИИ. Но это лишь известное нам препятствие. А как быть с теми, о которых мы не знаем?»[3].

Современные системы программного распознавания образов несовершенны: они не в состоянии отличить гражданского человека от комбатанта, что является фундаментальным требованием международного гуманитарного права к участникам любого вооруженного конфликта. Сегодня машина способна отличить кота от собаки, сравнив животное с миллионом хранящихся в памяти образов. Но современный бой насыщен огромным количеством непредсказуемых образов и обстоятельств, осмыслить которые машинам не под силу.

И, наконец, *робо-скептики* справедливо отмечают, что ни в одной армии мира не найдется командира, который позволит, чтобы приказы за него отдавала машина, тогда как ответственность за ее действия будет нести он сам. Отдать право выбора машине значит потерять контроль над ситуацией. И кого же тогда считать командиром?

Американские ученые попытались измерить и сравнить разные степени автономности систем вооружения, для чего они классифицировали их по ряду функций: мобильность, наличие системы наведения, системы навигации, стабильность, оборонительный или наступательный характер, способность определять образ цели, наличие системы управления огнем, способ принятия решения об открытии огня, наличие автоматической системы обмена информацией, системы планирования операции, возможность изменения целеуказания.

Роботы на поле боя нужны: они сохраняют жизни солдат, создают новые возможности для разведки, потенциально уменьшая сопутствующие потери. Но насколько востребована полная или частичная автономность военных роботов? По нашему мнению, есть лишь две причины, которые оправдывают повышение степени автономности. Первая причина — в том, что любая система коммуникаций может быть прервана: радиосвязь заглушена противником, а дождь может сделать невозможной лазерную связь. Поэтому робототехнический комплекс, действующий удаленно, должен обладать возможностью самостоятельных действий, к примеру возвращения на базу. Вторая причина состоит в том, что только увеличение степени автономности отдельных боевых роботов позволит увеличить огневую мощь подразделения без увеличения его численности: один солдат командует одновременно стаей дронов и гусеничных машин, которые уже сами находят возможности для координации действий между собой, следуя поставленной задаче. По этим параметрам возможно разбить вооружения по клеточкам в таблице, но это никак не приближает нас к ответу на вопрос: следует ли ограничить или запретить применение роботов, и если да, то каких типов и каким образом?

НАЗЛО НАДМЕННОМУ СОСЕДУ

До 2015 г. Россия, вовлеченная в иные национальные проекты, относилась к роботам в целом без должного внимания. Несмотря на успешное завершение НИР, выполненных в рамках комплексной целевой программы (КЦП) *Роботизация ВВТ–2015* [вооружения и военной техники — *ред.*], начатой в 2000 г., и положительные результаты испытаний созданных в них экспериментальных и действующих макетных образцов наземных робототехнических комплексов (РТК), опытно-

конструкторские работы по ним так и не были осуществлены, что фактически привело к приостановке исследований и разработок в области наземной военной робототехники[4].

Вестник МГТУ им. Н.Э. Баумана писал в 2013 г.: «Отставание России от США в настоящее время составляет около 10–15 лет. Главной проблемой, которая в значительной мере определяет указанное отставание, является отсутствие выработанной технической политики в области роботизации ВВТ со стороны государства»[5].

Простой пример показывает, насколько *Вестник МГТУ* близок к истине: американский беспилотник *Предатор* был разработан в 1994 г. Первые пуски ракеты с борта БПЛА состоялись в 2001 г. В России ударные беспилотники еще только разрабатываются, то есть отставание составляет около 15 лет.

Некоторые эксперты выдвигают теорию о том, что международные санкции зачастую не ограничивают, а наоборот, способствуют развитию программ, против которых они были нацелены. Например, в 1989 г., после событий на площади Тяньаньмэнь, Китай лишился возможности приобретать вооружения на Западе. А с Ираном эта история произошла еще раньше — в 1984 г. Сегодня и Китай, и Иран имеют развитую оборонную промышленность и производят вполне современные системы вооружений.

За присоединением Крыма к России в 2014 г. последовали западные санкции против ряда российских банков, после чего Россия сформировала собственную платежную систему. Запрет на платные услуги Google и Windows на полуострове подтолкнул процесс создания в России собственных программных продуктов. Возможно, западным санкциям в отношении российских оборонных предприятий мы обязаны и прорыву в российской военной робототехнике.

В сентябре 2014 г. Европейский Союз запретил организацию долгового финансирования для трех крупнейших оборонных концернов России: *Уралвагонзавода*, *Оборонпрома* и Объединенной авиастроительной корпорации и включил в санкционный список девять российских оборонных концернов: концерн *Сириус*, *Станкоинструмент*, *Химкомпозит*, концерн *Калашников*, Тульский оружейный завод, *Технологии машиностроения*, НПО *Высокоточные комплексы*, концерн ПВО *Алмаз-Антей* и НПО *Базальт*.

Стало окончательно понятно, что принятый еще при Анатолии Сердюкове, в его бытность министром обороны, курс на налаживание совместного производства вооружений со странами Европы оказался в тупике, и России, как некогда Советскому Союзу, придется развивать оборонную промышленность с опорой на собственные силы.

В сентябре 2015 г. Минобороны России приняло комплексную целевую программу *Создание перспективной военной робототехники до 2025 г. с прогнозом до 2030 г.* (КЦП *Роботизация–2025*). Программа определила в качестве приоритета «создание безэкипажных машин в виде роботизированных систем и комплексов военного назначения различных сред применения». Тогда Генеральный штаб Вооруженных Сил РФ разработал концепцию применения робототехнических комплексов воен-

ного назначения до 2030 г. и утвердил общие технические требования к наземным робототехническим комплексам военного назначения.

Подготовка общих требований к необитаемым подводным аппаратам и безэкипажным катерам в настоящее время завершается. Также российские военные формулируют госстандарты для комплексов с беспилотными летательными аппаратами. Так, отрасль беспилотников получает ГОСТы, что позволит производителям и пользователям общаться на едином техническом языке.

В продолжение мер, принятых Минобороны, 16 декабря 2015 г. президент Путин подписал указ *О Национальном центре развития технологий и базовых элементов робототехники*, деятельность которого поручено обеспечивать Фонду перспективных исследований (ФПИ). А в январе 2016 г. Владимир Путин потребовал к осени разработать стратегию научно-технологического развития РФ на долгосрочную перспективу. «Наличие собственных передовых технологий — это ключевой фактор суверенитета и безопасности государства, конкурентоспособности отечественных компаний, важное условие роста экономики и повышения качества жизни наших граждан. В этой связи считаю необходимым рассматривать Стратегию научно-технологического развития как один из определяющих документов наряду со Стратегией национальной безопасности», — сказал глава государства на заседании совета по науке и образованию[6].

ЭЛЕКТРОНИК В ПОМОЩЬ СЫРОЕЖКИНУ

Так в России начала оформляться структура ответственных за военную робототехнику организаций. К ним сегодня можно отнести:

1. Фонд перспективных исследований, ведущий научно-технические работы по трем мегапроектам: *Солдат будущего*, *Оружие будущего*, *Кибероружие будущего*. Эти три направления дополняют мероприятия государственной программы вооружения, а также федеральные целевые программы в области обороноспособности и безопасности страны. По имеющимся данным, в настоящее время фонд работает более чем над 50 проектами, для чего создано 35 лабораторий в ведущих вузах и научных институтах страны. ФПИ продолжает поиск идей и научных коллективов на российских просторах.

2. Главное управление научно-исследовательской деятельности и технологического сопровождения передовых технологий Минобороны РФ (ГУНИД) выступает генеральным заказчиком РТК военного назначения, а также вырабатывает единую идеологию и порядок их создания.

3. Главный научно-исследовательский испытательный центр робототехники Минобороны РФ (ГНИИЦР), расположенный на базе бывшей Военно-воздушной инженерной академии им. Жуковского в Москве. В составе этой организации формируется центр экспертизы инновационных проектов. ГНИИЦР — одно из самых секретных военных подразделений в стране, его сотрудники имеют право говорить о своей работе только в общих чертах. По словам начальника центра полковника Романа Климова, его подчиненные занимаются «проведением прикладных научных исследований и испытаний в обла-

сти создания и разработки робототехнических комплексов военного назначения»[7].

4. Комиссия Минобороны по развитию робототехнических комплексов военного назначения, которой руководит лично министр обороны РФ Сергей Шойгу. Комиссия занимается выработкой единой идеологии и порядка создания робототехнических комплексов, сокращением типажа, унификацией и межведомственной координацией.

Роботизация ставит российских военных перед серьезными вызовами: очертить стандарты и сформировать перспективный облик боевых роботов — задача относительно понятная, с учетом имеющихся в стране технологий, а также понимания того, что сегодня Россия выступает в роли догоняющего и, значит, может строить свои планы на базе достижений передовых государств. Но тактика и стратегия использования РТК у каждой страны будет своя: кто-то может решить, что роботы должны стать составной частью различных воинских подразделений, но возможен и иной подход — создание самостоятельного совершенно нового вида воинских подразделений, что потребует значительного реформирования и самих Вооруженных сил. Следом появится необходимость отработать на практике тактику их применения в боевых условиях и внести соответствующие коррективы в боевые уставы и наставления.

В российских войсках уже создаются первые подразделения, назначением которых станет управление боевыми роботами. Их опыт, наверное, ляжет в основу широких исследований и реформ. Осмыслить перспективное применение боевых роботов была призвана и первая военно-научная конференция *Роботизация Вооруженных сил РФ*, которая состоялась 10 февраля 2016 г. на территории военно-патриотического парка культуры и отдыха Вооруженных сил РФ *Патриот*. Ожидается, что выставка, на которой было продемонстрировано порядка 100 перспективных образцов и технологий робототехники, станет ежегодной.

РОБОТ С ЧЕЛОВЕЧЕСКИМ ЛИЦОМ

Между тем самого понятия *автономные системы* в лексиконе Минобороны России нет. *Военный энциклопедический словарь* на официальном сайте Министерства обороны РФ оперирует понятием *боевой робот*: «(чеш. robot), многофункциональное техн. устройство с антропоморфным (человекоподобным) поведением, частично или полностью выполняющее функции чел. при решении определ. боевых задач. Включает сенсорную систему (датчики), воспринимающую информацию, систему управления и исполнит. устройства»[8].

Боевых роботов российские военные делят на три поколения:

- «Б. р. 1-го поколения с программным и дистанц. управлением, способные функционировать только в организованной среде.
- Б. р. 2-го поколения — адаптивные, имеющие своего рода *органы чувств* и способные функционировать в заранее неизв. условиях, т. е. приспосабливаться к изменениям обстановки.

- Б. р. 3-го поколения — интеллектуальные, имеют систему управления с элементами искусственного интеллекта (созданы пока лишь в виде лабораторных макетов).

К наиб. простым Б. р. следует отнести безэкипажные танк и торпед. катер, робота-солдата и т. п., применяемые для обеспечения боевой деятельности войск в неприемлемых для чел. условиях».

Военные рассматривают робота в качестве боевого товарища, который подставит бойцу плечо в трудную минуту. Военачальники объясняют необходимость в них заботой о сохранении здоровья солдат на поле боя, большой протяженностью сухопутных и морских границ России и необходимостью «сложных и трудоемких наземных, надводных и подводных работ в труднодоступных или опасных для людей районах, в том числе в Арктике»[9].

Российские командиры готовы делать из необстрелянных роботов настоящих отличников боевой и политической подготовки: «Робот должен обладать человеческими качествами, как взаимопонимание и взаимовыручка, способность к самопожертвованию при действиях в составе коллективных группировок. При этом уровень самостоятельности РТК ВН должен быть исключающим неповиновение человеку-оператору, несанкционированное поведение и потерю управляемости»[10].

Опыт использования роботов в российской армии до сегодняшнего дня нельзя назвать впечатляющим. «Если в 2011 г. в ВС РФ было только 180 систем, то сейчас мы имеем 1720 современных беспилотных летательных аппаратов», — сообщил министр обороны Сергей Шойгу в декабре 2015 г. Тут следует отметить, что речь идет о беспилотниках с ограниченным функционалом, ведь ударные беспилотники только разрабатываются. Две наиболее популярные у российских военных модели — *Орлан-10* и *Элерон-3СВ*.

Орлан-10[11] — БПЛА с максимальным взлетным весом до 18 кг, до пяти из которых может приходиться на полезную нагрузку. Скорость полета находится в пределах от 75 до 170 км/ч в зависимости от тактической необходимости. Потолок *Орлана* достигает пяти километров. *Орлан-10* может находиться в воздухе до 18 часов, при этом в большинстве случаев максимальное удаление от пульта управления не должно превышать 180–200 км, иначе будет невозможно принимать сигнал с видеоаппаратуры беспилотника. БПЛА может нести на борту 3–4 типа нагрузок: 12 камер высокого разрешения, видеокамеру, тепловизионное оборудование или ретранслятор связи.

Элерон-3СВ[12] предназначен для наблюдения наземной обстановки и объектов с воздуха. Удобен в обслуживании, ибо может запускаться с устройства, подобного рогатке, а на землю возвращается на парашюте. Электрический двигатель, малые размеры и особенности формы делают этот БПЛА малозаметным для оптических и акустических приборов. При этом беспилотник снабжен стабилизированной ТВ-системой и цифровой фотокамерой с передающей аппаратурой. Время полета ограничено полутора часами. Стоит отметить, что как минимум две эти модели БПЛА получили боевое крещение в Сирии, и полученный опыт, безусловно, бесценен как для разработчиков, так и для военных операторов и стратегов.

Что касается российских сухопутных войск, то на 2015 г. на снабжении ВС РФ состояли только два роботизированных образца наземной военной техники: комплекс подвижный робототехнический для радиационной разведки местности и транспортировки радиоизлучающих предметов (РТК *Разнобой*) и робот дистанционно управляемый радиационной и химической разведки (РТК *Берлога-Р*).

Дистанционно управляемый РТК *Берлога-Р*[13], предназначенный для ведения радиационной и химической разведки, поиска локальных источников гамма-излучения на труднодоступных участках местности, в промышленных и жилых помещениях, был принят на вооружение в войска РХБЗ ВС РФ в 2004 г. В состав комплекса входят: подвижное наземное транспортное средство, оснащенное манипулятором, телевизионная система, аппаратура радиационной и химической разведки, пульт дистанционного управления, сбора и обработки информации, радиокомандная система, программное обеспечение, зарядное устройство для зарядки аккумуляторных батарей, а также комплект запчастей. Масса робота — 270 кг, передвигается он со скоростью до 0,5 м/с, манипулятор РТК способен поднимать грузы массой до 10 кг, а время его непрерывной работы составляет 2 часа.

РТК *Разнобой*[14], предназначенный для ведения визуальной и радиационной разведки, гамма-поиска, отбора проб и транспортирования твердых радиоактивных материалов при работе в зонах с высокими уровнями радиации в составе отрядов и подразделений ликвидации последствий аварий, был принят на снабжение сухопутных войск Вооруженных сил РФ в 2003 г. В состав комплекса входят полноприводный автомобиль типа *КАМАЗ 43114* с прицепом, два мобильных робота (*МРК-46М* и *МРК-РХ*), пост дистанционного управления, канал связи и дополнительное оборудование (пробоотборники грунта и жидкости, отбойный молоток, перфоратор, вилы грузовые, углошлифовальная машина).

В гособоронзаказ 2016 г. включен саперный робот легкого класса *Кобра-1600*[15], который получат инженерные войска ВС РФ. Его назначение — дистанционное проведение визуальной разведки, поиска и первичного диагностирования подозрительных предметов с помощью телевизионных камер и специального навесного оборудования, дистанционное обезвреживание взрывных устройств, загрузка их в специальные контейнеры для эвакуации, а также выполнение технологических операций по обеспечению доступа к потенциально опасным объектам. Помимо указанных роботов, которые уже поставлены на вооружение ВС РФ, в войска для испытаний поступают небольшие партии робототехнических комплексов различного назначения, в частности РТК разминирования *Уран-6* и РТК пожаротушения *Уран-14.*

Робототехнические комплексы разминирования *Уран-6*[16] представляют собой гусеничное шасси с легкобронированным корпусом и защитой лобовой и боковых поверхностей верхнего и нижнего пояса машины от повреждения осколками. *Уран-6* позволяет проделать проход в минном поле, разрушая взрывоопасные предметы бойковым тралом в движении. Скорость траления составляет до 2 км/ч при ширине полосы сплошного траления 1,75 м. В перспективе оператор подразделения роботов сможет управлять со своего пульта сразу несколькими машинами, осуществляя сплошную очистку полей от взрывоопасных предметов. Аппараты управляются системой дистанционного управления, куда вхо-

дят приемопередатчик, пульт с джойстиком, а также монитор, на который поступает картинка с камеры, установленной на машине. Вероятно, суровую проверку этот комплекс пройдет в Сирии, в условиях, максимально приближенных к боевым.

Уран-14[17], другое название — *Робот-пожарный,* предназначен для пожаротушения опасных объектов. При дальности подачи сплошной водяной струи до 50 м и объеме цистерны в 2 тыс. л возможно его подключение к внешнему источнику воды. При скрытом очаге возгорания специальное инфракрасное оборудование способно нацеливать водяную струю под большим давлением непосредственно в эту зону. Оператор может находиться в безопасном месте на расстоянии до 1 км. Основная функция робота — ликвидация пожаров на особо опасных военных объектах, в том числе на складах и арсеналах с оружием и боеприпасами, базах хранения, тыловых пунктах.

При том что максимальную пользу российской армии, вероятно, принесут такие безоружные роботы-трудяги, безусловно, наибольший интерес и противоречивые мнения вызывают боевые роботы. На сегодня российские предприятия успели выдать довольно разнообразную линейку вооруженных *концепт-каров*, некоторые из которых уже проходят апробацию в российских Вооруженных силах.

Уран-9[18] — боевой многофункциональный робототехнический комплекс, некоторые данные о котором засекречены. Известно, что состав вооружения боевого модуля включает 30-миллиметровую автоматическую пушку *2А72* и спаренный с ней 7,62-мм пулемет с возможностью оснащения противотанковыми управляемыми ракетами *Атака*. *Уран-9* обладает системой предупреждения о лазерном облучении и оборудованием для обнаружения, распознавания и сопровождения целей, что по оснащению приближает аппарат к современному танку, экипаж которого сидит у мониторов на удалении и управляет боевой машиной при помощи радиосигналов.

Многофункциональный комплекс *Нерехта*[19] может в разных вариациях оснащаться гранатометом, 14,5-мм пулеметом типа *КПВТ* или двумя спаренными пулеметами калибра 12,7 мм. Он работает на расстоянии до 25 км от оператора и может вести разведку, в том числе боем, вести патрулирование, эвакуировать раненых или корректировать огонь. Машина на гусеничной платформе разработана заводом им. В. А. Дегтярева и Фондом перспективных исследований и в 2016 г. проходит испытания на полигоне.

Платформа-М[20] — дистанционно управляемая гусеничная машина небольшого размера, оснащенная четырьмя гранатометами и пулеметом Калашникова. Ее испытания показали высокую эффективность при ведении боя в населенных пунктах и нанесении ударов по стационарным и подвижным целям противника. *Платформа-М* предназначена для ведения разведки, обнаружения и поражения целей, огневой поддержки подразделений, патрулирования и охраны важных объектов. В условиях прямой видимости на дальности до 1500 м от оператора *Платформа-М* может передвигаться со скоростью до 12 км/ч. Время непрерывного движения достигает 10 часов.

Можно предположить, что в отношении боевых роботов сегодня перед российскими военными стоит задача понять, насколько они могут быть востребованы

и так ли велика сфера их применения, как это видится разработчикам. Ради получения государственного заказа инженеры готовы обеспечить роботу любой функционал: разведка и наблюдение, патрулирование и огневая поддержка, охрана объектов и проделывание проходов в заграждениях, подвоз боеприпасов и эвакуация раненых, установка минных полей и разминирование, постановка дымовых завес и даже мобильное обеспечение аудиопропаганды.

Но некоторые армии мира уже решали эту проблему, и в результате пришли к необходимости существенно ограничить полет инженерной мысли разработчиков военной робототехники. В существующих воинских подразделениях достаточно одного или двух бойцов, чтобы обслуживать пулемет. Но чтобы содержать вооруженный этим пулеметом РТК, нужна еще транспортная машина, машина связи, станция техобслуживания и вооруженная охрана для нового роботехнического подразделения. Насколько этот РТК оправдает ожидания удаленного оператора и командиров в условиях, например, радиопомех, могут показать испытания или боевое применение.

Как рассказывают американские эксперты, использование наземных РТК в условиях Ирака не оправдало ожиданий Пентагона, и программу свернули. Американцы утверждают, что главным при принятии этого решения были не риски нарушения гуманитарного права (хотя, вероятно, и это тоже), а низкая эффективность боевых роботов при проведении зачисток в условиях городской застройки.

Но это не означает, что американцы охладели к автономным системам вообще. Как раз наоборот. Самая продвинутая в техническом плане страна сегодня работает не над тем, как сделать самого совершенного робота-убийцу. Американские стратеги решают задачу другого порядка: как правильно организовать взаимодействие человека и машины, чтобы, используя анализ больших данных, поступающих из различных источников, включая роботов-разведчиков, дать возможность руководителям принимать решения с такой эффективностью, на которую сегодня не способен ни человек без машины, ни машина без человека. То есть на повестке дня появляется вопрос о *симбиозе человека и машины* и появлении платформ, способных «контролировать целые скопления недорогих беспилотных систем, которые могут гибко комбинироваться и в большом количестве выдвигаться на поле боя»[21], — как уже было отмечено в начале этой статьи словами заместителя министра обороны США Боба Ворка.

ВИНТОВКА М-16 НА ГУСЕНИЧНОЙ ТЯГЕ

Следует отметить, что поставить пулемет или гранатомет на шасси — вовсе не новая идея. Американская компания *Foster-Miller* уже полтора десятилетия изготавливает и продает линейку дистанционно управляемых роботов *Тэлон* по цене от 60 до 230 тыс. долл. Роботы способны вести химическую, газовую и радиационную разведку. Военные уважают этих роботов за то, что на одной зарядке они могут активно работать 8,5 часов, в режиме ожидания контролировать свой сектор обзора до 7 дней, а в случае обнаружения движения их датчики передают изображение в цветном, черно-белом или инфракрасном диапазоне. Многие годы эти

железные трудяги выполняют охранные миссии или *кладут свои жизни* при разминировании дорог в Афганистане.

Боевая версия изделий *Тэлон* под названием *SWORDS* (*Special Weapons Observation Reconnaissance Detection System*) была опробована Соединенными Штатами еще в декабре 2003 г. в Кувейте, а позже в паре с пулеметом *M249* применялась в Ираке в 2007 г[22]. Отзывы военных о ней оказались противоречивы. Система управляется дистанционно с расстояния до 1000 м с помощью прибора, напоминающего игровую консоль, либо с помощью очков виртуальной реальности. Точность стрельбы удостоилась похвал. По некоторым сведениям, в течение нескольких лет военные использовали их как стационарные пулеметные точки, но впоследствии отказались от их закупок и финансирования программы из-за опасения все того же побочного ущерба [collateral damage]. Дальность действия у пулемета была больше, чем у сенсоров этого мобильного орудия, и риски несчастных случаев тревожили боевых командиров.

Сегодня ударный *SWORDS* можно увидеть только в музеях. Однако компания *Foster-Miller* не теряет оптимизма и разрабатывает новую модель — *Modular Advanced Armed Robotic System* (*MAARS*). Сообщают, что появления следующего американского мобильного стрелка на сцене театра боевых действий можно ожидать в 2018 г.[23].

ВОЕННО-МОРСКИЕ БЕЗЭКИПАЖНЫЕ СИЛЫ

Гораздо сильнее впечатляют достижения США в подводном роботостроении. ВМС США делают ставку на модульные автономные подводные роботы *REMUS 600*, которые несут на борту комплект сенсоров, аналогичный тому, что установлен на многоцелевые АПЛ *Вирджиния*[24]. Точное назначение этого робота, сделанного под размер торпедного аппарата, неизвестно, но можно догадаться, что он будет выполнять разведывательные функции, операции по разминированию, обнаружению (и уничтожению) подводных лодок. Такие мобильные платформы смогут работать в группе, обмениваясь информацией и распределяя задачи и функции. Во время войны в Ираке подводные роботы уже доказали свою эффективность при разминировании портов, а позже оказались незаменимы при поиске останков пропавшего рейса MH370 Малайзийских авиалиний. Возможность программирования подводных платформ делает их чрезвычайно гибким инструментом, обладающим мощным потенциалом для дальнейшего развития.

Особенно, если их объединить в информационную сеть с другим новаторским прибором — боевым подводным планером (*Littoral Battlespace Sensing Glider — LBSG*), в создании которого сегодня участвуют 150 американских компаний. Подводные планеры способны на одной литиевой батарее плыть за счет изменения собственной плавучести в режиме планирования более месяца. Неспешно перемещаясь под водой, они могут пересекать океаны, делясь друг с другом и с оператором информацией об окружающей среде. В ближайшие годы они откроют ученым многие загадки подводного мира, и немногие военные тайны сумеют остаться для них секретом. Эффективность и стоимость такого подводного разведчика несопоставимы с существующими традиционными системами, и этот потенциал еще далеко не раскрыт.

Компанию подводным исследователям составит противолодочное беспилотное судно *ACTUV* — (*Anti-Submarine Warfare (ASW) Continuous Trail Unmanned Vessel*).[25] Это живое, точнее материальное, воплощение *Летучего голландца*, небольшое судно с запасом хода на несколько тысяч километров. Его экипаж не будет отсчитывать вахты, одна многомесячная вахта такого корабля будет посвящена единой задаче: обнаруживать и отслеживать, а при необходимости — уничтожать чужие подводные лодки. Представьте, что два десятка таких судов действуют, как стая волков, загоняющих одинокую лошадь. Именно так — стаей — и рассчитывает использовать их Пентагон. Эксперименты по автономной координации взаимодействия дюжины таких кораблей уже проводились. Слаженностью действий морские машины дали бы фору лучшим капитанам. Ожидается, что цена одного безэкипажного судна составит около 20 млн долл., что более чем на порядок меньше стоимости современного корабля с людьми на борту, обладающего подобными функциями. Это важно, ибо позволит в разы увеличить возможности ВМС без изменения бюджетных расходов. В случае окончательного успеха этой программы флот США получит первую партию беспилотных охотников в 2018 г.

Еще одна новация позволит не ждать, пока промышленность произведет серийные образцы, но даст возможность внедрять последние достижения науки немедленно, возможно — сразу на борту судна. Сегодня на базе 3D-принтеров возникает новая отрасль производства, получившая название *аддитивное производство* [additive manufacturing]. Похоже, военные оценили преимущества 3D-принтеров раньше гражданских. На протяжении столетий действия военных флотов были ограничены необходимостью наличия базы для хранения запчастей и боеприпасов. Оружие, в том числе и высокотехнологичное, служило по многу десятков лет. Например, новая торпеда разрабатывается примерно десять лет, затем ее производят в количестве нескольких сотен единиц и рассылают на хранение по флотским арсеналам. В арсеналах торпеды проходят регулярную проверку, периодически — модернизацию, до тех пор, пока не подойдет срок утилизации (реже — случай для боевого или учебного пуска).

Аддитивное производство подразумевает производство изделий прямо на борту: будь то торпеда, беспилотник, запчасть для двигателя или подводный сонар. Британские военные разработчики из компании *Qinetiq* опубликовали доклад *Тенденции в глобальных морских технологиях 2030* [Global Marine Technology Trends 2030][26], в котором объяснили, что производство изделий из металла, пластика и графена на 15-метровом принтере будет быстрым и дешевым. Боевые роботы позволят американским адмиралам обеспечивать эффективный контроль морских коммуникаций при меньших расходах, с большей эффективностью и с использованием оборудования и вооружений не из гигантских арсеналов, а из-под принтера, то есть свежих, прямо с чертежного стола инженера, как *пирожки с пылу, с жару*.

ВВС БУДУЩЕГО С ДРЕВНЕГРЕЧЕСКИМ УКЛОНОМ

В 2014 г. в истории мировой авиации произошло уникальное событие: американский беспилотный самолет *X-47B* самостоятельно сел на палубу авианосца. А в 2015 г. этот же беспилотник совершил дозаправку в воздухе. Эти достижения

стали прологом к следующему этапу: малозаметный авиадрон получил способность осуществлять бомбовые налеты на сверхдальней дистанции[27]. Теперь американские авианосцы смогут вести боевые действия, не входя в зону поражения самолетов и ракет противника. Автономные роботы позволят вести бесконтактную войну не только с архаичными танками и артиллерией, но и с высокотехнологичным противником, оставаясь вне досягаемости.

Разведку и наведение на цель большим железным собратьям обеспечат недорогие микродроны. Группа из 30 дронов-малышей, доставленная самолетом или ракетой, будет готова к выполнению различных заданий: отсканирует и передаст в центр картину будущего поля боя, создаст помеховую зону, а по команде сможет вывести из строя и систему ПВО противника[28]. «Мы проводили испытания, и это работает», — уверяет заместитель министра обороны США Роберт Ворк. В представлении Пентагона организованные дроны — это часть войн будущего[29].

Другая новация американского агентства по оборонным разработкам DARPA (Defense Advanced Research Projects Agency) — программа Gremlins — позволит возвращать стаи дронов после выполнения их миссии на борт бомбардировщика. Таким образом будет обеспечена сохранность секретных американских технологий и сэкономлен военный бюджет, ведь предполагается, что каждый *гремлин* будет рассчитан на 20 запусков, а техники смогут подготовить новую группу дронов для следующего боевого захода в течение 24 часов. На контракт с DARPA по данному проекту претендуют четыре компании, окончательно производитель будет определен к 2020 г.[30].

Командные или роевые атаки становятся совсем недорогими, если из них исключить человека с его ежедневными потребностями в тепле, питании и отдыхе, а также если вычесть зарплаты, пенсии, социальные пособия, инфраструктуру для обеспечения семей, медицину для здоровых и реабилитацию для раненых. Железные воины не ведут блоги, не разглашают секреты и не требуют компенсаций. Идеальной армии нужны беспилотные суда, где роботы прямо на борту изготавливают и чинят беспилотные самолеты и ракеты. Тогда для полного совершенства военной машине будет не хватать малости — искусственного интеллекта.

Но в его отсутствие есть замена — *тактика кентавра* [Centaur Warfighting]. Как раз над ней сегодня трудится передовая мысль Пентагона. В теории это командная работа человека и машины, сочетание возможностей человеческого интеллекта и мобильности, автономности, коммуникабельности, способности к координации и синхронности машин для достижения полного превосходства над противником[31]. Апологеты этой тактики считают, что если компьютер сегодня может выиграть в шахматы у человека, вместе они составят непобедимую команду[32].

На основе тактики, названной в честь древнегреческого человеко-коня, Пентагон делает еще одно многообещающее изобретение — *третью стратегию сдерживания*. Две первые стратегии — опора на ядерное, а позже на высокоточное оружие в связке с системой ПРО — в представлении американских военных себя изживают, поскольку русские и китайцы в этих сферах достигли или близки к достижению паритета. Стаи автономных роботов под управлением *кентавра* — симбиоза человека и машины — вот что сможет надолго восстановить глобальное военное доминирование США[33].

Для этого минобороны США налаживает тесное партнерство с разработчиками из Кремниевой долины. Специальный офис министерства в этом технопарке спонсирует стартапы, заключает секретные контракты и рекрутирует экспертов по перспективным технологиям, формируя то, что уже получило в среде технарей название *военно-информационный комплекс*[34].

АСИММЕТРИЧНАЯ ЗАГОГУЛИНА

В России тоже ведется поиск оптимальных комбинаций применения различных платформ: например, рассматривается сочетание беспилотного катера и БПЛА, которое позволит расширить радиус действия средств разведки до 100–200 км от корабля-носителя. Комплекс беспилотников может дополнить подводный беспилотный аппарат, в том числе те, что сегодня эксплуатируются на российских флотах (управляемые аппараты типа *Тайгер* и подводный комплекс *Пантера*, позволяющие именно в дистанционном режиме выполнять опасные работы под водой)[35].

На земле тоже ищут применение автономным триадам: например, изучается возможность применения мобильного ударно-разведывательного робототехнического комплекса вместе с боевой противодиверсионной машиной *Тайфун-М* и беспилотным летательным аппаратом. Предполагается, что эта команда сможет вести разведку, обнаруживать и уничтожать неподвижные и подвижные цели, осуществлять огневую поддержку подразделений, патрулировать режимные объекты и ликвидировать диверсионно-разведывательные формирования в составе автоматизированной системы охраны мобильной группировки РВСН[36].

Чтобы роботы стали эффективными и надежными, российские специалисты разрабатывают системы управления и связи. Основные из разрабатываемых в настоящее время технологий перечисляет начальник ГНИИЦР Минобороны РФ полковник Сергей Попов:

- супервизорное и автономное управление робототехническими комплексами;
- создание программно-алгоритмических средств бортовых систем группового управления РТК военного назначения (ВН) в однотипных, разнотипных и смешанных боевых порядках;
- разработка технологии создания интеллектуальных систем человеко-машинного интерфейса и поддержки принятия решений операторами управления РТК ВН при решении боевых (ударных, огневых), обеспечивающих и специальных задач;
- разработка технологий создания и применения РТК ВН неклассических конструктивных компоновок, биороботов, микроробототов, нанороботов;
- создание программно-алгоритмических средств, обеспечивающих самонастраивающееся контролируемое движение РТК ВН в неопределенных, динамически изменяющихся, подверженных влиянию случайных возмущений разнородных средах функционирования[37].

Также российским военным, вероятно, придется решить несколько прикладных задач: сформировать терминологическую базу в сфере робототехники; определить общие стандарты программирования, обработки, обмена и защиты информации; разработать теоретические основы и практические рекомендации по применению и обеспечению робототехники при подготовке и в ходе боевых действий; определить ответственность за действия боевого робота (кто будет виноват, если робот ошибется: производитель, программист, оператор, командир?) И наконец, определить собственную позицию относительно внедрения искусственного интеллекта в военной сфере. Пока это вполне умозрительная проблема, но, наверное, однажды она перестанет быть таковой. Достаточно ли средств в международном и национальном законодательстве, чтобы, например, предотвратить возможность восстания машин против человека и уничтожение человечества?

Пока разработка боевых роботов в России еще проходит этап полевых испытаний, остается открытым вопрос, который международные правозащитники, вероятно, однажды поставят перед российским руководством: хорошо ли будут отечественные роботы выполнять обязательства нашей страны по соблюдению международного гуманитарного права (МГП)?

Минобороны России готово дать утвердительный ответ. Положения МГП отражены в *Уставе внутренней службы*: «Военнослужащий обязан знать и неукоснительно соблюдать международные правила ведения военных действий, обращения с ранеными, больными, лицами, потерпевшими кораблекрушение, и гражданским населением в районе боевых действий, а также с военнопленными».

Разработанное Управлением по боевой подготовке сухопутных войск *Наставление по применению гуманитарного права в Вооруженных силах* объемом почти в сто страниц содержит детальное изложение норм МГП. Документ объясняет, как в боевой обстановке следует относиться к комбатантам, журналистам, медицинскому персоналу, парламентерам, шпионам, наемникам, раненым и больным, гражданскому населению, санитарному транспорту, культурным ценностям и особо опасным объектам. В документе описаны запрещенные способы ведения боевых действий и меры ответственности за нарушения. «Положения настоящего Наставления надлежит использовать, сообразуясь с обстановкой, решительно добиваясь безусловного выполнения боевых задач при соблюдении норм международного гуманитарного права», — говорится во вступительной части.

Нормы международного гуманитарного права включены в учебную подготовку курсантов высших военных училищ, где продолжительность курса МГП составляет около 80 часов. Для слушателей военных академий аналогичный курс немногим короче. В вопросах просвещения российских военных о положениях МГП российское Минобороны взаимодействует с МККК, представителей которого даже приглашают на учения в качестве наблюдателей.

Российские боевые роботы, проходящие сегодня испытания на полигонах, управляются дистанционно, то есть фактически эти образцы вооружений трудно назвать автономными. Но военные отмечают, что они «имеют ресурс модернизации», то есть по мере совершенствования программного обеспечения, сенсорно-

го и связного оборудования их автономность будет возрастать. Например, нынешними боевыми платформами, как правило, управляют не менее двух операторов: один отвечает за ходовую часть, другой управляет оружием. Но разработчики стремятся к тому, чтобы в перспективе один оператор мог управлять несколькими боевыми роботами. Будет ли он в состоянии обеспечить соблюдение принципа *полноценного контроля со стороны человека* [meaningful human control]? Разумеется, создатели новых вооружений обязаны позаботиться об этом еще на этапе разработки.

ПОЙДУТ МАШИНЫ В ЯРОСТНЫЙ ПОХОД

Появление на международной арене автономных вооружений изменило характер войны. Первой сенсационной демонстрацией их возможностей стала война в Югославии. На стенах домов в Белграде и нынче можно встретить надписи с призывом объединяться в ополчение против США. Но эти гневные лозунги лишь отчетливее показывают, насколько бессильна армия XX века перед высокотехнологичным противником, шагнувшим в XXI век.

Сегодня бóльшая часть стран мира стремится обзавестись собственной программой беспилотного авиастроения. Вовлечься в этот процесс несложно: первую модель можно собрать из компонентов, поставляемых по многочисленным интернет-каталогам. Более продвинутые технологии состоятельные клиенты могут купить в США или Израиле, те, что победнее, — в Турции. Клиенты с подмоченной репутацией могут обратиться в Китай, а то и в КНДР. Разработчики с амбициями и собственным инженерным потенциалом должны запастись терпением, а еще больше — бюджетом. Экономичный двигатель, система навигации, сенсоры и видеокамеры, надежная система связи — из этих кубиков складываются беспилотные ВВС. Все это пригодится потом при создании беспилотных сухопутных войск и беспилотных ВМС. Они дадут вооруженным силам шанс перейти на новый качественный уровень не позже, чем это сделает потенциальный противник, чтобы *избиение младенцев* по югославскому сценарию не повторилось.

Примерно такая логика движет сегодня технический прогресс в сфере военных автономных систем. И она же дает толчок процессу, который принято называть гонкой вооружений. Погоня за технологиями автономных роботизированных систем вовлекает новых участников. Гонку вооружений также питает взаимное недоверие и многочисленные обострившиеся в последние годы конфликты, которые отравляют современные международные отношения. В этих условиях никто не хочет быть отстающим, и значит, гонку вооружений ожидает новый виток. Вероятно, он будет связан в первую очередь с автономностью как с новым качеством систем вооружений.

Появление в небе, на море и под водой большого количества беспилотных систем будет представлять собой новое явление для традиционного воздухоплавания и мореходства. Отсутствие международных правил, регулирующих взаимодействие роботов, перемещающихся под разными флагами, может вызывать инциденты, которые будут иметь тем более серьезные последствия, чем секретнее будут технологии на борту. Вопрос о мерах по предупреждению инцидентов бес-

пилотных роботов, вероятно, может возникнуть в повестке международного сообщества в скором будущем.

Инциденты с автономными системами также возможны по причине потери связи с беспилотным роботом из-за помех, возникших случайно или вызванных целенаправленно, в связи с намеренным перехватом контроля над беспилотником, чему в истории уже были примеры. Отсутствие регулирования в области систем управления и кибербезопасности автономных систем может создавать опасные ситуации, в результате которых роботы могут вовлечь людей в конфликты, которых люди вовсе не предвидели.

Боевые роботы, бесспорно, будут существенно увеличивать военный потенциал, а их массовое принятие на вооружение может стать угрозой балансу сил в различных регионах, что повысит риски возникновения конфликтов. Важно своевременно оценить и обезвредить эту угрозу, чтобы искусственный интеллект и автономный дрон были синонимами всемирного блага, а не неведомой и необратимой опасности.

Комментарий эксперта

Активизировавшаяся в последнее время многосторонняя работа по проблематике смертоносных автономных систем (САС) на различных международных площадках с целью их включения в Конвенцию о «негуманном» оружии (КНО) [Convention on certain conventional weapons], выявила наличие ряда ключевых концептуальных проблем, способных оказывать значительное и долговременное влияние на ход дипломатических усилий в этой сфере.

Как известно, в рамках Конвенции — на стыке контроля над вооружениями и международного гуманитарного права — тема САС рассматривается в рамках неофициальных встреч экспертов. Такой статус в известном смысле подчеркивает незрелость проблемы, ее неоднозначность и недостаточную изученность.

После двух лет активных обсуждений так и не утихли споры вокруг того, что же следует понимать под термином САС. Например, включать ли в эту категорию ударные БПЛА и существующие прототипы автономным систем, которые уместнее было бы называть автоматизированными. И это несмотря на то, что в рамках КНО в целом договорились о неких рамках дискуссий: разговор должен вестись о САС следующего поколения, а БПЛА выводятся за скобки обсуждений.

Хотелось бы подчеркнуть, что такое самоограничение, которое, к слову, постоянно подвергается сомнению рядом радикально настроенных в этой сфере стран, таких как Пакистан и Куба, уже оказало парадоксальный эффект на рассмотрение проблемы САС в формате КНО.

С одной стороны, обсуждение этой темы в принципе стало возможным на такой международно-признанной экспертной площадке, как КНО. Сама рамочная Конвенция и прилагаемые к ней пять Протоколов (Россия активно участвовала в их выработке и присоединилась ко всем из них) является в известном смысле законодателем мод в области запретов и регулирования применения неизбирательных, особо негуманных видов вооружений. Поэтому превращать этот форум в арену политизированных споров, как это на обсуждениях БПЛА в Совете ООН по правам человека, большинству делегаций явно не хотелось бы. Собственно говоря, такое добровольно наложенное самоограничение и неформальный статус обсуждений и позволили при-

нять консенсусное решение о запуске неформальной работы по САС на Совещании государств-участников КНО в 2013 г.

С другой стороны, такое понимание рамок дискуссий придало им весьма условный характер. И действительно, как можно экспертно обсуждать еще не созданные вооружения. Ведь в полном смысле автономных боевых систем вооружений пока еще не существует.

Такое положение дел привело к наличию главной на данный момент проблемы — отсутствию универсально признаваемого определения САС. В дипломатическом смысле это делает обсуждение темы во многом теоретическим и оторванным от реальной почвы. Говорить об упреждающем характере разоруженческих усилий в этой сфере тоже не приходится. Превентивно ограничивать применение какого-либо вида оружия можно тогда, когда оно существует на практике. О превентивном же запрете можно в свою очередь говорить только при наличии универсального понимания того, что именно запрещается. Ведь из практики многосторонней дипломатии хорошо известно, что понятийный аппарат, и прежде всего базовые определения не существуют сами по себе. Они всегда затачиваются под конкретные дипломатические цели и инструменты.

В этом смысле весьма показательны итоги проведенного МККК в апреле 2016 г. в Женеве международного семинара по САС. Несмотря на доклады ключевых игроков в сфере робототехники и искусственного интеллекта о том, что работы в этих областях идут полным ходом, говорить об оформившихся типах вооружений, которые обладали бы ясно отличимыми признаками автономности, пока еще преждевременно.

Здесь мы и подходим к главному. Какие цели должен преследовать дипломатический процесс по САС? Позиции государств на площадке КНО здесь явно расходятся. По мнению традиционных гуманитарных радикалов, ратующих за широкие запреты различных видов вооружений, включая ядерное оружие, а также поддерживающих их многочисленных и влиятельных НПО, дело следует вести к превентивным запретам. При этом их не смущают приведенные выше нами аргументы. Технически продвинутым государствам, активно разрабатывающим вооружения, основанные на принципах автономности, было бы явно не выгодно ставить под удар свои собственные наработки. С их точки зрения, речь могла бы вестись скорее о разработке некоего свода правил или лучших практик, которым следует руководствоваться при разработке, создании, производстве и применении будущих автономных систем оружия.

Встает вопрос о том, какими критериями следует при этом руководствоваться. Женевский семинар МККК отчетливо продемонстрировал, что в качестве главного критерия выдвигается подход, согласно которому нормы международного гуманитарного права должны в полной мере распространяться и на САС с учетом императива сохранения этих систем вооружений под контролем человека. По большому счету, спорить с этим трудно. Все виды вооружений следует применять с учетом норм и принципов МГП (которые предусматривают различие между гражданскими и военными целями, соразмерность, пропорциональность и тому подобное). Однако в нашем случае речь идет о еще не существующем оружии.

При этом перечисляются некие критические признаки САС: значимый человеческий контроль, способность к самостоятельному выбору, сопровождению и поражению целей, предсказуемость с точки зрения постоянной управляемости человеком. Здесь мы сталкиваемся с другой концептуальной проблемой: что следует считать значимым человеческим контролем и как определить степень этой значимости?

Постановка вопросов в такой плоскости, на наш взгляд, способна привести к неизбежной политизации дискуссий, привнесению в них оценочных категорий, включая возможное разделение государств на ответственные, то есть обеспечивающие значимый контроль, и менее ответственные.

Более того, при такой логике на определенном этапе развития дискуссий по САС, вполне может возникнуть соблазн их деления на хорошие и плохие с использованием набора вышеприведенных или каких-либо других критериев. Такое мы уже видели применительно к проблематике кассетных боеприпасов (КБ). Конвенция о кассетных боеприпасах, подписанная рядом стран в Осло, (Россия не в их числе), как известно, вводит запрет на негуманные боеприпасы и выводит за скобки другие, действие которых основано на весьма схожих принципах, просто не называя их кассетными.

Из всего вышеизложенного следует вывод о том, что спешить переводить эту неоднозначную и в целом пока оторванную от объективной реальности тему в плоскость официального рассмотрения, а тем более с целью достижения неких договоренностей, не стоит. Проблематика явно нуждается в дополнительной предварительной экспертной работе. Да и «предмет» для рассмотрения еще только вызревает.

Андрей Малов,
советник Постоянного представительства РФ
при ООН и других международных
организациях в Женеве

Примечания

1 Roff Heather. The International-Relations Argument Against Killer Robots. Defense One, 19 August 2015, http://www.defenseone.com/ideas/2015/08/international-relations-argument-against-killer-robots/119275 (последнее посещение 17.04.2016)

2 Losing Humanity: The Case Against Killer Robots, Human Rights Watch, November 2012, P. 2, http://www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf (последнее посещение 17.04.2016)

3 LeCun Yann, Facebook, 14 March 2016, https://www.facebook.com/yann.lecun/posts/10153426023477143 (последнее посещение 17.04.2016)

4 Каляев Игорь, Рубцов Иван. Боевым роботам нужна программа. *Национальная оборона*. 2016. № 2, февраль, http://www.oborona.ru/includes/periodics/defense/2012/0801/20258963/detail.shtml (последнее посещение 17.04.2016)

5 Корсунский В.А., Наумов В.Н. Перспективы развития военных мобильных робототехнических комплексов наземного базирования в России. *Вестник МГТУ им. Н.Э. Баумана: электронное издание.* 2013. http://engjournal.ru/articles/413/html/files/assets/basic-html/page7.html (последнее посещение 17.04.2016)

6 Владимир Путин провел заседание Совета по науке и образованию. Путин сегодня, 21 января 2016 г., http://www.putin-today.ru/archives/19849 (последнее посещение 17.04.2016)

7 Попов Сергей, Фаличев Олег. Робот стреляет первым. Искусственный интеллект привлекает на службу молодых ученых. *Военно-Промышленный Курьер*. 2016, 24 февраля, http://vpk-news.ru/articles/29352 (последнее посещение 17.04.2016)

8 Военный энциклопедический словарь, официальный сайт Минобороны РФ, http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=3551@morfDictionary (последнее посещение 17.04.2016)

9 Разработку подводных роботов против авианосцев начали в России. Деловая газета «Взгляд», 24 декабря 2014, http://vz.ru/news/2014/12/24/721982.html (последнее посещение 17.04.2016)

10 Тихонов Александр. Военные роботы: вперед в будущее, Красная звезда, 10 февраля 2016, http://www.redstar.ru/index.php/news-menu/vesti/iz-dosaaf/item/27625-voennye-roboty-vperjod-v-budushchee (последнее посещение 17.04.2016)

11 Агеев Александр. Российский беспилотник «Орлан-10». Техкульт, 5 ноября 2015, http://www.techcult.ru/technics/2736-bespilotnik-orlan-10 (последнее посещение 17.04.2016)

12 Разведывательный БПЛА ближнего действия «Элерон-3 СВ». Энциклопедия БПЛА Сухопутных войск. Защищать Россию, 1 апреля 2015, https://defendingrussia.ru/enc/bpla_sv/razvedyvatelnyj_bpla_blizhnego_dejstvija_eleron3sv-1844/ (последнее посещение 17.04.2016)

13 Худолеев Виктор. «Берлога» для химразведки. Красная звезда, 13 декабря 2015, http://www.redstar.ru/index.php/syria/item/26964-berloga-dlya-khimrazvedki (последнее посещение 17.04.2016)

14 Кудряшов Владимир, Лапшов Владимир, Носков Владимир, Рубцов Иван. Проблемы роботизации ВВТ в части наземной составляющей. Известия ЮФУ, 5 марта 2014, http://izv-tn.tti.sfedu.ru/wp-content/uploads/2014/3/5.pdf (последнее посещение 17.04.2016)

15 Саперный робот легкого класса «Кобра-1600» включен в Гособоронзаказ 2016 года, журнал «Спецназ» 25 января 2016, http://www.specnaz.sb.by/novosti-spetsnaza/article/sapyernyy-robot-legkogo-klassa-kobra-1600-vklyuchen-v-gosoboronzakaz-2016-goda

16 Юферев Сергей. Робот-сапер «Уран-6». Военное обозрение, 14 ноября 2014, http://topwar.ru/62494-robot-saper-uran-6.html (последнее посещение 17.04.2016)

17 Уран-14, робототехнический комплекс пожаротушения. Информационное агентство «Оружие России», 29 марта 2016, http://www.arms-expo.ru/armament/samples/880/70957/ (последнее посещение 17.04.2016)

18 Робот-Боец Уран-9. Информационное агентство «Оружие России», 29 марта 2016, http://www.arms-expo.ru/video/uran-9-robot-boets-/ (последнее посещение 17.04.2016)

19 Рябов Кирилл. Проект робототехнического комплекса «Нерехта». 23 октября 2015, Военное обозрение, http://topwar.ru/84742-proekt-robototehnicheskogo-kompleksa-nerehta.html (последнее посещение 17.04.2016)

20 Будлянский Григорий. «Платформа-М»: Роботизированный комплекс широких возможностей. Информационное агентство «Оружие России», 6 октября 2014, http://www.arms-expo.ru/news/perspektivnye_razrabotki/platforma_m_robotizirovannyy_kompleks_shirokikh_vozmozhnostey/ (последнее посещение 17.04.2016)

21 Roff Heather. The International-Relations Argument Against Killer Robots. Defense One, 19 August 2015, http://www.defenseone.com/ideas/2015/08/international-relations-argument-against-killer-robots/119275 (последнее посещение 17.04.2016)

22 Foster-Miller TALON. Wikipedia, https://en.wikipedia.org/wiki/Foster-Miller_TALON (последнее посещение 17.04.2016)

23 Modular Advanced Armed Robotic System. Wikipedia, https://en.wikipedia.org/wiki/Modular_Advanced_Armed_Robotic_System (последнее посещение 17.04.2016)

24 De Silva Richard. The future role of the submarine. Defense IQ, 05 October 2015, http://www.defenceiq.com/naval-and-maritime-defence/articles/the-future-role-of-the-submarine (последнее посещение 17.04.2016)

25 Littlefield Scott. Anti-Submarine Warfare (ASW) Continuous Trail Unmanned Vessel (ACTUV). DARPA, http://www.darpa.mil/program/anti-submarine-warfare-continuous-trail-unmanned-vessel (последнее посещение 17.04.2016)

26 Global Marine Technology Trends 2030. August 2015, https://issuu.com/lr_marine/docs/55046_lr2030_web-lr_25mb (последнее посещение 17.04.2016)

27 Dyer Geoff. US military: Robot wars. Financial Times, 7 February 2016, https://next.ft.com/content/849666f6-cbf2-11e5-a8ef-ea66e967dd44 (последнее посещение 17.04.2016)

28 The Coming Age of the Military Micro-Drone. Futurism, Http://Futurism.Com/The-Coming-Age-Of-The-Micro-Drone/ (последнее посещение 17.04.2016)

29 «Perdix» Mini Air-Launched Swarming UAV Discussion in 'Aerospace Programs' started by AMDR, The American Military Forum. Feb 9, 2016, http://www.americanmilitaryforum.com/forums/threads/perdix-mini-air-launched-swarming-uav.579/ (последнее посещение 17.04.2016)

30 Chloe Olewitz, DARPA's new Gremlin drones fly back to their 'mothership' after completing recon missions, 2016, 15April, http://www.foxnews.com/tech/2016/04/15/darpas-new-gremlin-drones-fly-back-to-their-mothership-after-completing-recon-missions.html

31 Edwards Sean J. A. Swarming on the Battlefield: Past, Present, and Future. RAND Corporation, 2000. http://www.rand.org/pubs/monograph_reports/MR1100.html (последнее посещение 17.04.2016)

32 Markoff John. Report Cites Dangers of Autonomous Weapons. *The New York Times*, 2016, 28 February, http://www.nytimes.com/2016/02/29/technology/report-cites-dangers-of-autonomous-weapons.html?_r=0 (последнее посещение 17.04.2016)

33 Ignatius David. The exotic new weapons the Pentagon wants to deter Russia and China. The Washington Post. 2016, 23 February, https://www.washingtonpost.com/opinions/the-exotic-new-weapons-the-pentagon-wants-to-deter-russia-and-china/2016/02/23/b2621602-da7a-11e5-925f-1d10062cc82d_story.html (последнее посещение 17.04.2016)

34 Merchant Brian. The Military-Information Complex Is Growing in Silicon Valley. Motherboard, 20 June 2013, http://motherboard.vice.com/blog/the-military-information-complex-is-rising-in-silicon-valley (последнее посещение 17.04.2016)

35 Минобороны делает ставку на боевых роботов. Военное обозрение, 27 сентября 2015, http://militaryreview.ru/minoborony-delaet-stavku-na-boevyx-robotov.html (последнее посещение 17.04.2016)

36 Гаврилов Юрий. В российской армии создадут роты боевых роботов. *Российская газета*. 2014, 7 ноября, http://rg.ru/2014/11/07/roboti-site.html (последнее посещение 17.04.2016)

37 Тихонов Александр. Военные роботы: вперед в будущее, Красная звезда, 10 февраля 2016, http://www.redstar.ru/index.php/news-menu/vesti/iz-dosaaf/item/27625-voennye-roboty-vperjod-v-budushchee (последнее посещение 17.04.2016)

Константин Стальмахов
Андрей Шкарбанов

НЕКОТОРЫЕ ВОПРОСЫ РЕГУЛИРОВАНИЯ ГРАЖДАНСКОЙ ОТВЕТСТВЕННОСТИ ЗА ЯДЕРНЫЙ УЩЕРБ

Регулирование гражданской ответственности за ядерный ущерб — серьезный и чрезвычайно актуальный вопрос. Фукусимская трагедия 2011 г., на возмещение ущерба от которой уже затрачено 52 млн долл. США[1], в полной мере продемонстрировала необходимость создания в этой сфере единого правового режима, при котором ответственность эксплуатирующей организации (оператора ядерной установки) и государства была бы ограничена, а пострадавшие имели бы четкие гарантии своих прав и интересов и процедуры для их защиты. Отметим, что общие требования к ядерной и физической безопасности ядерных установок и ядерного материала должны выполняться на всех стадиях ядерного топливного цикла, эксплуатации АЭС и иных объектов использования атомной энергии. Однако характерной чертой механизма гражданской ответственности за ядерный ущерб является то, что он *включается* только в случае ядерного инцидента и служит для компенсации потерь в той степени, в какой это возможно.

Более того, актуальность вопроса обоснована объективными неюридическими фактами:

- ядерный ущерб является экстремальным по масштабу, а в отношении человека и окружающей среды длительное время может иметь латентный характер;
- последствия ядерных аварий не всегда могут быть локализованы в пределах границ одного государства;
- полностью исключить возникновение ядерных инцидентов невозможно.

Юридическим следствием этих особенностей является то, что общее деликтное право (совокупность норм гражданского права, регулирующих обязательства, возникающие из причинения вреда) не учитывает всей специфики ядерных рисков.

Право как регулятор общественных отношений безусловно находится под влиянием научно-технического прогресса. Поэтому большинство стран, в 50-е гг. прошлого века начавших использовать атомную энергию в мирных целях, осознали необходимость разработки специального законодательства, регулирующего гражданскую ответственность за ущерб в случае инцидентов. Возможность причинения огромного по масштабам ущерба гражданам нескольких стран в результате ядерного инцидента обусловила целесообразность сближения правовых

подходов как можно большего числа стран к регулированию данного вопроса. Поэтому одновременно с разработкой национального законодательства, а иногда и на предшествующем этапе, велась работа по заключению международных соглашений.

Необходимость международного регулирования поддерживали прежде всего государства европейского региона: члены тогдашней Организации европейского экономического сотрудничества, преобразованной впоследствии в Организацию экономического сотрудничества и развития, и Европейского сообщества по атомной энергии. Так появилась Парижская конвенция об ответственности перед третьей стороной в области ядерной энергии 1960 г., вступившая в силу только в 1968 г., а затем Брюссельская конвенция 1963 г. Она дополняла Парижскую конвенцию и увеличивала объем возмещения за ядерный ущерб, выплачиваемого за счет финансовых средств государств и международных структур.

Потребность в создании единого режима гражданской ответственности за ядерный ущерб осознавалась и на мировом уровне. Так, 21 мая 1963 г. под эгидой Международного агентства по атомной энергии была принята Венская конвенция о гражданской ответственности за ядерный ущерб (вступила в силу в 1977 г.), к которой могут присоединиться все государства — члены ООН или МАГАТЭ. Фактически она устанавливает аналогичный режим правового регулирования, но уже не ограничивается рамками отдельного региона.

В настоящей статье будут рассмотрены три блока вопросов: актуальные проблемы регулирования гражданской ответственности за ядерный ущерб в Российской Федерации, Протокол о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г. и несовершенство действующих международных правовых режимов гражданской ответственности за ядерный ущерб.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ ГРАЖДАНСКОЙ ОТВЕТСТВЕННОСТИ ЗА ЯДЕРНЫЙ УЩЕРБ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Модель регулирования гражданской ответственности за ядерный ущерб в Российской Федерации строится в первую очередь на Венской конвенции о гражданской ответственности за ядерный ущерб 1963 г., подписанной Российской Федерацией в 1996 г.[2] и ратифицированной в 2005 г.[3].

За год до подписания Российской Федерацией Венской конвенции о гражданской ответственности за ядерный ущерб 1963 г. и за десять лет до ее вступления в силу на территории России был принят Федеральный закон от 21 ноября 1995 г. № 170-ФЗ *Об использовании атомной энергии*. Поэтому значительная часть положений Федерального закона не согласуется с терминологией и положениями вышеупомянутой Венской конвенции. Далее будут рассмотрены базовые положения регулирования гражданской ответственности за ядерный ущерб в Российской Федерации путем сравнения и анализа Венской конвенции о гражданской ответственности за ядерный ущерб и действующего российского законодательства.

Для понимания базовых основ регулирования гражданской ответственности за ядерный ущерб и дальнейшего анализа проблематики российских правовых реалий необходимо отметить следующие общепризнанные принципы такого регулирования:

- тоннелирование ответственности — эксплуатирующая организация несет исключительную ответственность за ядерный ущерб;
- строгость ответственности — абсолютная ответственность эксплуатирующей организации, включая ответственность без вины;
- ограничение ответственности — ответственность может быть ограничена по объему (сумме возмещения) и иметь временные рамки;
- финансовые гарантии — эксплуатирующая организация должна обеспечивать страхование или другое финансовое обеспечение (государственные и независимые гарантии, участие в обществах взаимного страхования), покрывающее размер ее ответственности;
- исключительность юрисдикции — суды государства, на территории которого находятся ядерные установки, обладают исключительной юрисдикцией относительно вынесения решений по предъявляемым требованиям.

Кроме того, в рамках тоннелирования ответственности можно выделить принципы исключения права регрессного требования[4] эксплуатирующей организации (например, к поставщику о возмещении вреда в связи с некачественным оборудованием, по вине которого произошла ядерная авария) и участия государства в возмещении вреда. Безусловно, эти принципы являются общими правилами, которые могут иметь некоторые оговорки, исключения либо условия их применения.

Центральным понятием международно-правовых документов такого рода является ядерный ущерб. Согласно Венской конвенции о гражданской ответственности за ядерный ущерб оно включает[5]:

- смерть, любое телесное повреждение или любую потерю имущества, или любой ущерб имуществу, которые возникают или являются результатом радиоактивных свойств или комбинации радиоактивных свойств с токсическими, взрывными или другими опасными свойствами ядерного топлива, или радиоактивных продуктов или отходов на ядерной установке, или ядерного материала, поступающего с ядерной установки, произведенного в ней или направленного на ядерную установку;
- любую другую потерю или ущерб, возникающие таким образом или являющиеся результатом этого, если это предусмотрено национальным законом, и в пределах, установленных таким законом;
- если это предусмотрено национальным законодательством, смерть, любое телесное повреждение или любую потерю имущества, или любой ущерб имуществу, которые возникают или являются результатом другого ионизирующего излучения, испускаемого любым другим источником излучения внутри ядерной установки.

Согласно Федеральному закону *Об использовании атомной энергии*[6], возмещению подлежат: вред жизни и здоровью физических лиц и другие убытки физических и юридических лиц, обусловленные радиационным воздействием при выполнении работ в области использования атомной энергии либо сочетанием радиационного воздействия с токсическими, взрывными или иными опасными воздействиями, а также убытки за вред, причиненный радиационным воздействием окружающей среде.

Уже здесь встречается первое несовпадение предметов регулирования. Российский закон ограничивается случаями радиационного воздействия при выполнении работ в области использования атомной энергии, чего нет в Венской конвенции. Термин *выполнение работ* часто встречается в рассматриваемом законе, однако его значение нигде не раскрывается. Наряду с данным термином закон также оперирует понятием *деятельность в области мирного использования атомной энергии*, перечень основных видов которой приведен в статье 4. Возможно, под термином *выполнение работ* законодатель подразумевал осуществление деятельности в области использования атомной энергии.

При этом законом отдельно установлен перечень видов деятельности, осуществление которой требует лицензирования. На основании этого, а также учитывая то, что, в соответствии со статьей 56, необходимым условием для получения эксплуатирующей организацией разрешения (лицензии) на осуществление деятельности в этой сфере является наличие документального подтверждения финансового обеспечения, можно утверждать, что термин *выполнение работ* как минимум включает осуществление лицензируемых видов деятельности. Однако в отсутствие правоприменительной практики и опираясь на буквальное прочтение закона (так называемый *нормативистский подход*), остается неясным, нужно ли понимать *выполнение работ* дословно, исключая случаи осуществления иной деятельности в иной сфере. Например, оказание медицинских услуг, поставки в области сельскохозяйственного производства, где могут применяться ядерные материалы и радиоактивные вещества, а также использование атомной энергии в промышленности.

Если основываться на широком толковании понятия *выполнение работ*, то сфера регулирования Федерального закона *Об использовании атомной энергии* намного шире, чем Венской конвенции. Так, последняя прямо исключает ее применение в отношении следующих объектов использования атомной энергии:

- реактора, которым оборудовано средство морского или воздушного транспорта в целях использования его в качестве источника энергии для приведения в движение этого средства транспорта или для любой другой цели;
- природного урана в процессе транспортировки и на ядерной установке (за исключением того, когда он используется в качестве ядерного топлива);
- радиоизотопов, которые достигли окончательной стадии изготовления, став таким образом пригодными для использования в любых научных, медицинских, сельскохозяйственных, коммерческих или промышленных целях.

Российский закон таких исключений не содержит, исходя из чего любое радиационное воздействие потенциально подпадает под действие положений рассматриваемой главы 12 данного закона.

Закон *Об использовании атомной энергии*[7] дублирует принцип строгой ответственности, содержащийся в Венской конвенции: ответственность эксплуатирующей организации за убытки и вред, причиненные радиационным воздействием, наступает независимо от вины эксплуатирующей организации.

Однако при анализе взаимосвязи с иными нормами законодательства выявляются противоречия с российскими международными обязательствами. При этом важно помнить, что при сопоставлении норм закона *Об использовании атомной энер-*

гии в части регулирования гражданской ответственности за ядерный ущерб с нормами иных нормативных правовых актов первые должны рассматриваться как специальные по отношению, например, к положениям Гражданского Кодекса Российской Федерации и, соответственно, будут иметь приоритет над такими общими положениями.

Согласно закону[8] эксплуатирующая организация освобождается от ответственности за убытки и вред, причиненные радиационным воздействием, возникшим в результате непреодолимой силы, военных действий, вооруженных конфликтов и умысла самого потерпевшего. В соответствии с Гражданским кодексом Российской Федерации[9] юридические и физические лица, деятельность которых связана с повышенной опасностью для окружающих (в число видов которой входит использование атомной энергии) обязаны возместить вред, причиненный источником повышенной опасности, если не докажут, что вред возник вследствие непреодолимой силы (иными словами, форс-мажора) или умысла потерпевшего.

Форс-мажор является очень общим понятием, под которым может пониматься любое событие, подпадающее под соответствующие признаки (чрезвычайность и непредотвратимость при данных условиях). В соответствии с Венской конвенцией[10] на оператора не может быть возложена ответственность за ядерный ущерб, если ядерный инцидент произошел в результате вооруженного конфликта, военных действий, гражданской войны, восстания или, за исключением случаев, когда национальным законодательством установлено иное, в результате тяжелого стихийного бедствия исключительного характера.

В то же время в российском законе *Об использовании атомной энергии*[11] закреплено, что эксплуатирующая организация полностью или частично освобождается от ответственности, если убытки и вред полностью или частично причинены вследствие умысла пострадавшего. Но законодательство не учитывает иную форму вины потерпевшего, которая также нашла отражение в Венской конвенции как основание освобождения от ответственности — вину в форме грубой неосторожности[12].

В российском законе принцип исключительной ответственности оператора прямо не регулируется специальной нормой, но толкование статей 53 и 54 в целом подразумевает его наличие.

Гражданский кодекс Российской Федерации[13] по общему правилу предоставляет лицу, возместившему вред, причиненный другим лицом, право обратного (регрессного[14]) требования к причинителю вреда в размере выплаченного возмещения. В закрытом перечне не имеющих права регресса лиц эксплуатирующие организации не указаны. В статье приводятся примеры и делаются исключения только в отношении физических, но не юридических лиц. Однако без наличия четкой судебной практики формально снова возникает противоречие с Венской конвенцией в части общего принципа на запрет права регресса оператора, исключениями из которого являются только случаи, когда такое право прямо предусмотрено в контракте или в отношении физического лица, в связи с умыслом которого произошел ядерный инцидент (иными словами, когда само лицо своими действиями прямо или косвенно вызвало ядерный инцидент)[15].

С другой стороны, российским законодательством не предусмотрено важное правило Венской конвенции, смягчающее ответственность оператора. Так, согласно конвенции, оператор не несет ответственности за ядерный ущерб, причиненный:

- самой ядерной установке или любому имуществу на месте расположения этой установки, которое используется или должно использоваться в связи с этой установкой;
- средству транспорта, на котором этот ядерный материал находился во время ядерного инцидента[16].

Венская конвенция[17] устанавливает, что ответственность оператора может быть ограничена государством суммой не менее 5 млн долл. США за каждый ядерный инцидент. Стоимость доллара США в данном случае эквивалентна его золотому паритету на 29 апреля 1963 г.: 35 долл. за одну тройскую унцию чистого золота. При стоимости одного грамма золота 2800 руб. (на начало февраля 2016 г.) указанный лимит составляет 12,5 млрд руб. Неправильное прочтение данной нормы является распространенной ошибкой. Принципиально важно отметить, что в Венской конвенции не закреплен верхний предел ответственности, она лишь предоставляет государству право установить такой предел.

Отсюда в связке с российским законодательством возникает следующая ситуация. На основании закона *Об использовании атомной энергии*[18] максимальные пределы ответственности за убытки и вред, причиненные радиационным воздействием, в отношении любого одного инцидента не могут превышать уровень, установленный международными договорами Российской Федерации. То есть закон также не закрепляет конкретный лимит, а отсылает к международным договорам. При этом, как было показано, Венская конвенция такой лимит также не устанавливает. В этом случае приходится обращаться к общим правилам российского деликтного права[19].

Согласно Гражданскому кодексу Российской Федерации вред личности, имуществу гражданина, вред имуществу юридического лица подлежит возмещению в полном объеме лицом, причинившим вред[20]. Напрашивается логический вывод о том, что, согласно действующему российскому законодательству, ответственность эксплуатирующей организации не ограничена.

Более того, в силу закона *Об использовании атомной энергии*[21] Правительство Российской Федерации обеспечивает выплату сумм по возмещению убытков и вреда в той части, в которой причиненные убытки и вред превышают установленный для эксплуатирующей организации предел ответственности посредством предоставления необходимых сумм до полного возмещения причиненных убытков и вреда, а также в случаях, предусмотренных законодательством Российской Федерации. Это соответствует норме Венской конвенции о гражданской ответственности за ядерный ущерб[22]: «государство обеспечивает выплату возмещений по удовлетворенным исковым требованиям против оператора за ядерный ущерб путем предоставления необходимых средств в том размере, в каком размер страхования или другого финансового обеспечения недостаточен для удовлетворения таких требований, но не выше предела, если такой предел имеется».

Но поскольку указанный предел в настоящее время на определен, упомянутая норма об ответственности правительства фактически не является действующей.

После установления такого предела и при сохранении рассматриваемого положения гражданская ответственность за ядерный ущерб Правительства Российской Федерации станет неограниченной («до полного возмещения причиненных убытков и вреда»[23]). В этой связи представляется избыточной норма закона *Об использовании атомной энергии*[24], в соответствии с которой финансовое обеспечение эксплуатирующей организации может состоять, среди прочего, из государственной гарантии.

Ответственность оператора также ограничена по срокам. Согласно Венской конвенции, по общему правилу права потерпевших на возмещение ядерного ущерба теряют силу, если иск не возбужден в течение десяти лет со дня ядерного инцидента[25]. Тогда как российский закон[26], закрепляя для требований о возмещении вреда имуществу или окружающей среде общий срок в три года со дня, когда лицо узнало или должно было узнать о нарушении своего права, вовсе не распространяет исковую давность на требования о возмещении убытков и вреда, причиненных жизни и здоровью граждан. Что, учитывая ситуацию с неограниченной по объему ответственностью, также содержит колоссальные риски для эксплуатирующей организации и государства, но является неоценимым плюсом для потерпевших. В то же время ни одна страховая организация не станет обеспечивать страхование неограниченных рисков, которые невозможно оценить в денежном эквиваленте, а, значит, за пределами ограниченного по срокам и объемам договора страхования гражданской ответственности за ядерный ущерб риски оператора в любом случае остаются без страхового покрытия.

ПУТИ СОВЕРШЕНСТВОВАНИЯ НОРМАТИВНО–ПРАВОВОЙ БАЗЫ

Таким образом, действующее законодательство Российской Федерации содержит ряд пробелов и противоречий в части регулирования гражданской ответственности за ядерный ущерб. Ключевыми недостатками российского правового режима является несоответствие понятийного аппарата, в особенности применительно к термину *ядерный ущерб*, а также отсутствие норм о пределах ответственности эксплуатирующей организации.

Возможность прямого применения норм Венской конвенции о гражданской ответственности за ядерный ущерб в силу положений Конституции Российской Федерации и Гражданского кодекса Российской Федерации о приоритете обязательств Российской Федерации по международным договорам над национальным законодательством также однозначно не решает проблемы. С одной стороны, правило о приоритете международных договоров может иметь место, если положения международного договора применяются непосредственно.

Согласно Федеральному закону от 15 июля 1995 г. № 101-ФЗ *О международных договорах Российской Федерации*[27], положения официально опубликованных международных договоров Российской Федерации, не требующие для своего применения издания внутригосударственных актов, действуют в Российской Федерации непосредственно. Так, часть положений Венской конвенции о гражданской ответственности за ядерный ущерб может применяться непосредственно и, следовательно, будет превалировать над российским законодательством. Поэтому закон *Об использовании атомной энергии* применяется только в части, не противоречащей указанным нормам конвенции. С другой стороны, для реали-

зации положений международных договоров Российской Федерации иного характера принимаются соответствующие нормативные правовые акты. К признакам, свидетельствующим о невозможности непосредственного применения положений международного договора в Российской Федерации, относятся, в частности, содержащиеся в договоре указания на обязательства государств-участников по внесению изменений в их внутреннее законодательство[28]. Венская конвенция содержит множество норм, отсылающих к национальному законодательству, которого фактически может и не быть.

Все это указывает на необходимость комплексного реформирования законодательства (Федеральный закон от 21 ноября 1995 г. № 170-ФЗ *Об использовании атомной энергии*, Гражданский кодекс Российской Федерации, Федеральный закон от 10 января 2002 г. № 7-ФЗ *Об охране окружающей среды*, Арбитражного процессуального и Гражданского процессуального кодексов Российской Федерации в части определения единой юрисдикции суда) с учетом последних разработок в этой сфере. Речь идет о Протоколе о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г., который создает *модернизированный* режим гражданской ответственности за ядерный ущерб, однако участницей которого Российская Федерация не является.

Давней попыткой законодательно адаптировать положения Венской конвенции был внесенный еще в 1996 г. в Государственную Думу законопроект *О гражданской ответственности за ядерный ущерб и ее финансовом обеспечении*, который был принят в первом чтении, однако результативная работа по нему прекращена по настоящее время. Законопроект должен был установить четкий понятийный аппарат, соответствующий Венской конвенции, условия наступления ответственности эксплуатирующей организации и освобождения от нее, порядок финансового обеспечения ответственности, а также — и важность этого нельзя переоценить — конкретный размер пределов ответственности.

Поскольку речь зашла об эволюции международного правового регулирования рассматриваемого вопроса, целесообразно рассмотреть плоды этого развития и сопутствующие издержки. Поэтому далее будет рассмотрен Протокол о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г.

НЕКОТОРЫЕ КЛЮЧЕВЫЕ ТОЧКИ РЕФОРМИРОВАНИЯ

Цель Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г., как прямо говорится в его преамбуле, — внести поправки в Венскую конвенцию о гражданской ответственности за ядерный ущерб, чтобы «предусмотреть более широкую сферу применения, более высокие размеры ответственности оператора ядерной установки и усиленные средства обеспечения адекватного и справедливого возмещения». Согласно статье 18 Протокола в отношении его участников Венская конвенция и Протокол о внесении поправок «понимаются и толкуются вместе как единый текст, который может упоминаться как *Венская конвенция о гражданской ответственности за ядерный ущерб 1997 г.*».

Протокол прямо исключает из рамок своего действия ядерные установки военного назначения[29], тогда как в Венской конвенции этот вопрос затрагивается лишь очень косвенно. В преамбуле говорится, что одна из причин заключения Конвенции состоит в желательности «установления некоторых минимальных норм для обеспечения финансовой защиты от ущерба, возникающего в результате определенных видов мирного использования ядерной энергии». Хотя, учитывая объемы деятельности в области использования атомной энергии в военных целях, возмещение ядерного ущерба потерпевшим в связи с любыми ядерными инцидентами, не ограниченными деятельностью в мирных целях, является более чем оправданным. При этом Протокол не содержит расшифровки понятия *военных целей*, отсюда государства вправе не применять данный Протокол к ядерным установкам, выполняющим одновременно военные и гражданские функции.

Протокол уточняет понятие ядерного инцидента[30], который означает любое происшествие или серию происшествий одного и того же происхождения, которые причиняют ядерный ущерб или (но только в отношении превентивных мер) создают серьезную и непосредственную угрозу причинения такого ущерба. Соответственно, важно учитывать, что наличия только одного признака угрозы причинения ядерного ущерба (серьезность или непосредственность) для определения инцидента в качестве ядерного недостаточно.

Выше было показано достаточно лаконичное определение понятия *ядерный ущерб* в Венской конвенции. Протокол существенно его расширяет[31]. Согласно этому документу, в него включается:

i смерть или телесное повреждение;

ii потеря имущества или ущерб имуществу;

iii (по каждому следующему подпункту государство может в рамках национального законодательства определить, устанавливать ли данные виды ущерба в качестве ядерного либо ограничиться только первыми двумя вышеуказанными пунктами);

iv экономические потери, возникающие в результате потерь или ущерба, упомянутых в подпункте i или ii, постольку, поскольку они не охватываются этими подпунктами, если их несет лицо, имеющее право на предъявление иска в отношении таких потерь или ущерба;

v затраты на меры по восстановлению окружающей среды, состояние которой ухудшилось, за исключением незначительного ухудшения, если такие меры фактически были приняты или должны быть приняты и постольку, поскольку это не охватывается подпунктом ii;

vi потерю доходов, получаемых от экономического интереса в любом применении или использовании окружающей среды, в результате значительного ухудшения состояния этой среды и постольку, поскольку это не охвачено подпунктом ii;

vii затраты на превентивные меры и стоимость дальнейших потерь или ущерба, причиненных такими мерами;

viii любые другие экономические потери помимо любых потерь, вызванных ухудшением состояния окружающей среды, если это допускается общим законом о гражданской ответственности компетентного суда.

Как мы видим, почти каждый новый вид ядерного ущерба содержит какие-либо условия для его определения в качестве такового, а возмещение возможно в том случае и в той степени, как это определено национальным законодательством. Последнее условие делает спорными достоинства новых положений, поскольку право потерпевших на возмещение ядерного ущерба должно быть прямо предусмотрено в национальном законе.

Протокол о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г. точно определяет географические рамки его применения, точнее отсутствие данных рамок: «применяется к ядерному ущербу независимо от того, где он причинен»[32]. Данный вопрос прямо не урегулирован в Венской конвенции, в связи с чем ее применение основывается на соответствующем национальном законодательстве.

Однако Протокол о внесении поправок оставляет государству необходимую свободу выбора — национальное законодательство может исключать из-под его действия ущерб, причиненный:

- на территории государства, не являющегося участником Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г.; или
- в любых морских зонах, установленных государством, не являющимся участником Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г., в соответствии с международным морским правом[33].

Замысел этого положения в том, что государство, имеющее ядерную программу, должно либо присоединиться к Протоколу, либо предоставить *взаимные выгоды*, если оно хочет, чтобы средства, которые выделяются в соответствии с Протоколом, направлялись на возмещение ущерба, причиненного на ее территории[34].

В целом, описанная ситуация не является чем-то уникальным, международное право изначально формируется как некий компромисс между государствами. Поэтому логически имеет место несовершенство действующих международных правовых режимов гражданской ответственности за ядерный ущерб.

Существующие принципы гражданской ответственности за ядерный ущерб оставляют под вопросом ценность формируемого ими режима для жертв ядерного инцидента. Действительно, неограниченная ответственность оператора создает риск его банкротства и ухода с рынка. Стоимость электроэнергии, вырабатываемой АЭС, в таком случае значительно возрастет, а на страхование неограниченной ответственности не согласится ни одна страхования компания или пул (объединение) таких организаций. Однако ограничение ответственности оператора может серьезно нарушить интересы пострадавших. Достаточно сравнить возможные минимальные лимиты гражданской ответственности за ядерный ущерб, которые государство вправе установить согласно международным конвенциям, с фактически причиненным ущербом на примере аварии на Фукусимской АЭС. Кроме того, емкость рынка страхового обеспечения ограничена, и объем потенциального ущерба также может ее превышать. К этому можно добавить и временные рамки ответственности оператора, которые не всегда могут учитывать отложенный негативный эффект воздействия радиации на сле-

дующие поколения или окружающую среду, который, в свою очередь, может быть затруднительно выявить или доказать.

Фактически из всех принципов гражданской ответственности за ядерный ущерб серьезные и непосредственно ощутимые выгоды пострадавшим предоставляют только два: необходимость финансового обеспечения, гарантирующего как минимум частичное возмещение ущерба, и строгая ответственность оператора, которая избавляет пострадавших от ряда сложностей при доказывании своих требований о возмещении ущерба в ходе судебного процесса.

Модернизированные международные конвенции (Венская конвенция в редакции Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г. и Парижская конвенция об ответственности перед третьей стороной в области ядерной энергии в редакции Протокола к ней 2004 г.), несмотря на расширенную дефиницию понятия ядерного ущерба, все же оставляют государству широкую свободу относительно уточнения содержания этой ключевой категории. Так, Венская конвенция в редакции Протокола о внесении поправок[35] указывает на экономические потери как составляющую ядерного ущерба, одновременно оставляя вопрос на усмотрение национального законодательства. Иными словами, к примеру, упущенная выгода в связи с ущербом для туристической или сельскохозяйственной отраслей хозяйства не будет компенсирована. Хотя Парижской Конвенцией об ответственности перед третьей стороной в области ядерной энергии в редакции Протокола к ней 2004 г. такой вид ущерба не предусмотрен вовсе.

Также Венская конвенция в редакции Протокола[36] ограничивает ущерб окружающей среде признаками значительности ухудшения ее состояния и необходимостью принятия восстановительных мер. Каким образом определить такую значительность, как учитывать отложенный эффект радиационного воздействия и как вычислить затраты на восстановление окружающей среды — неясно. При этом из толкования нормы можно прийти к выводу о том, что если восстановление окружающей среды невозможно (то есть нет таких мер, которые могут и должны быть приняты), значит, и компенсация не должна предусматриваться.

Исключительность юрисдикции судов государства, на территории которого находятся ядерные установки, может быть рассмотрена как своего рода дискриминационная норма. Ведь если представить, что физическое или юридическое лицо подает иск в суд иностранного государства, на ядерной установке которого произошел ядерный инцидент, возникает сомнение в объективности и непредвзятости рассмотрения его дела. Во-первых, при защите интересов граждан и организаций государства, на территории которого произошел инцидент, и лиц иного государства приоритет с большой степенью вероятности будет отдан именно интересам и правам первых. Во-вторых, суд будет учитывать важность хотя бы частичного поддержания финансовой стабильности национального оператора, на установке которого произошел инцидент. С учетом изложенного можно с достаточной уверенностью предположить трудности реализации на практике норм международных конвенций о применении национального законодательства на недискриминационной основе по признаку гражданства, постоянного или временного местожительства.

Небогатые развивающиеся страны и их население могут столкнуться с отсутствием ресурсов для возмещения ущерба через суд иностранного государства, для чего также необходимо создание некоего механизма правовой помощи таким пострадавшим, включая их представительство на судебном процессе.

Еще один международно-правовой документ, регулирующий отношения в рассматриваемой сфере, — Конвенция о дополнительном возмещении за ядерный ущерб. Она была открыта для подписания в 1997 г. на 41-й сессии Генеральной конференции МАГАТЭ и вступила в силу только спустя почти 20 лет (15 апреля 2015 г.), когда были соблюдены необходимые для этого условия.

США активно продвигают Конвенцию на мировой арене как единственный международный инструмент, на базе которого может быть сформирован глобальный и универсальный режим регулирования гражданской ответственности за ядерный ущерб. Эта цель прямо сформулирована в преамбуле документа, что уже отличает его от рассмотренных выше. При этом в преамбуле признается значение Венской и Парижской конвенций, а также национальных законодательств, соответствующих изложенным в них принципам. Как известно, преамбула не имеет юридически обязывающей силы для государств-участников международного договора, однако имеет большое значение для применения документа в целом. В силу пункта 1 статьи 31 Венской конвенции о праве международных договоров 1969 г. договор должен толковаться добросовестно в соответствии с обычным значением, которое следует придавать терминам договора в их контексте, а также в свете объекта и целей договора.

Причина настойчивости США проста. В их национальном законодательстве, несмотря на общее соответствие базовым положениям Венской и Парижской конвенций, не закреплен один из основных принципов гражданской ответственности за ядерный ущерб: принцип исключительной ответственности оператора. Данное отличие не позволяет США стать членом одного из *старых* режимов, для полного соответствия которым необходимы значительные изменения законодательства. Исходя из этого, в статье 2 приложения к Конвенции о дополнительном возмещении за ядерный ущерб содержится специальная оговорка, в силу которой подразумевается, что законодательство США, как и иных государств, до 1995 г. уже имевших законодательство в рассматриваемой сфере регулирования ответственности, которое содержало и до сих пор содержит некоторые положения[37], соответствует требованиям приложения к данной конвенции. Это дает государству право присоединиться к Конвенции о дополнительном возмещении, даже если оно не является членом Венской или Парижской конвенции. Такого рода оговорки не способствуют равноправному восприятию государствами Конвенции о дополнительном возмещении и умаляют значение одного из ключевых принципов (исключительной ответственности оператора). Более того, наличие описанного исключения уже подрывает цель Конвенции по созданию единого глобального режима, устанавливая отличное от международных стандартов правовое регулирование в отношении четвертой части всех действующих в мире АЭС[38], которые находятся в США.

Для создания подлинно эффективного глобального режима гораздо предпочтительнее основываться на давно применяемых инструментах. Речь о триаде Венской и Парижской конвенций, а также Совместного протокола об их применении, объединяющего режимы первых двух документов[39]. Участниками Венской

и Парижской конвенций (в той или иной редакции, в зависимости от года принятия поправок к ним) уже являются 43[40] и 18[41] государств соответственно, а к Совместному протоколу присоединились 36 стран[42]. Тогда как Конвенцию о дополнительном возмещении подписали 20 государств, а вступила в силу она только в отношении восьми[43] из них.

Появление еще одного инструмента предсказуемо ведет к большей нерешительности стран-новичков в области использования атомной энергии относительно того, к какой конвенции присоединиться. Как следствие — еще большая фрагментированность международного режима гражданской ответственности за ядерный ущерб. Более того, участником Конвенции о дополнительном возмещении является Индия, для которой она вступает в силу 4 мая 2016 г.[44]. Однако широко известно, что в 2010 г. в Индии был принят Закон о гражданской ответственности за ядерный ущерб, предусматривающий право регресса[45] поставщика в отношении оператора, являющегося элементом принципа исключительной ответственности оператора, и имеющий преимущественную силу над нормами международного права. По всей видимости, индийский законодатель посчитал, что закрепление права одного государства на отход от принципов ответственности за ядерный ущерб может рассматриваться как право других участников на аналогичные действия. Таким образом, несмотря на указанное противоречие национального законодательства и Конвенции о дополнительном возмещении, при ратификации документа Индия заявила о том, что ее законодательство соответствует его требованиям. А ввиду того, что при ратификации Индия заявила о неприменении положения Конвенции, в котором речь идет об арбитражном порядке разрешения споров, у других участников фактически отсутствуют эффективные меры воздействия на эту страну по вопросу приведения ее национального законодательства в соответствие с этими требованиями. Полагаем, что такие случаи также свидетельствуют о подрыве основ международного режима гражданской ответственности за ядерный ущерб.

Переходя к содержательным пробелам новой конвенции, целесообразно отметить следующее. В отличие от модернизированных режимов, Конвенция о дополнительном возмещении не устанавливает в качестве общего правила возмещение ущерба независимо от того, где он причинен, а также не создает достаточной гибкости в отношении определения понятия *ядерная установка*. Тогда как Венская конвенция о гражданской ответственности за ядерный ущерб 1997 г. и Парижская конвенция об ответственности перед третьей стороной в области ядерной энергии в редакции Протокола к ней 2004 г. содержат указанное общее правило и предусматривают право МАГАТЭ и Агентства по ядерной энергии Организации экономического сотрудничества и развития соответственно дополнять определение ядерной установки иными установками, в которых присутствует ядерное топливо, радиоактивные материалы или радиоактивные отходы.

Конвенция о дополнительном возмещении не позволяет операторам государств, являющихся участниками только данной конвенции, закрепить в контракте момент перехода гражданской ответственности за ядерный ущерб от одного оператора к другому во время транспортировки ядерного материала. Это ведет к пересечению ответственности операторов, а, значит, накладывает на них ненужные дополнительные расходы на страхование ответственности. Такое случается, например, когда за транспортировку ядерных материалов на определенном участке пути несут ответственность оба оператора, поставщик и получатель. Кроме того, такая

ситуация также не создает однозначного понимания того, в судах какого именно государства будет рассматриваться спор о возмещении ядерного ущерба.

Механизм создания наднационального фонда возмещения[46] ядерного ущерба также создает вопросы. Базой для расчета взносов государств в такой фонд является тепловая мощность ядерных реакторов на территории соответствующего государства. Однако данная формула не учитывает такие ядерные установки, как заводы, использующие ядерное топливо для производства ядерных материалов или перерабатывающие облученное ядерное топливо, а также хранилища отработавшего ядерного топлива.

Более того, в отличие от Брюссельской дополнительной конвенции 1982 г.[47], которая также создает наднациональный уровень возмещения ядерного ущерба для государств-участников Парижской конвенции, Конвенция о дополнительном возмещении не обязывает ответственное за ядерную установку государство в случае ядерного инцидента сначала предоставить дополнительное возмещение сверх *базового* (например, выплачиваемого за счет страхования) до обращения к средствам межгосударственного фонда. Остается под вопросом, насколько будет приемлема для национальных парламентов и министерств финансов государств-участников конвенции ситуация, когда необходимость компенсации за ядерный ущерб, причиненный на другом конце планеты, может автоматически привести к использованию средств налогоплательщиков их государств[48].

Подводя итоги, отметим, что описанные факты и ситуации могут служить достаточным основанием для дальнейшего развития международного правового режима гражданской ответственности за ядерный ущерб. К совместным действиям государств по созданию глобального режима и развитию правового регулирования гражданской ответственности за ядерный ущерб призывает и МАГАТЭ[49]. Действительной базой такого режима закономерно должна стать триада Венской и Парижской конвенций, а также Совместного протокола об их применении с учетом целесообразности создания наднационального уровня возмещения ущерба для государств-участников Венской конвенции по образцу Брюссельской дополнительной конвенции 1982 г. Одним из возможных вариантов развития в этом направлении могло бы стать внесение изменений в Брюссельскую дополнительную конвенцию, которые бы позволили участникам венского режима присоединяться к ней. С учетом данных возможностей и тенденций в формировании международного режима гражданской ответственности за ядерный ущерб Российской Федерации как лидеру мирового атомного рынка целесообразно продолжить работу по развитию национального законодательства в своих интересах и интересах своих граждан.

Примечания

1 Records of Applications and Payoffs for Indemnification of Nuclear Damage http://www.tepco.co.jp/en/comp/images/jisseki-e.pdf (последнее посещение 19.02.2016)

2 Постановление Правительства РФ от 12.04.1996 № 415 «О подписании Венской конвенции о гражданской ответственности за ядерный ущерб»

3 Федеральный закон от 21.03.2005 № 23-ФЗ «О ратификации Венской конвенции о гражданской ответственности за ядерный ущерб»

4 Требование лица, совершившего платеж, например, пострадавшему, лицу (лицам), предъявляемое к третьему лицу, по вине которого, например, произошел инцидент, и был совершен платеж, о возврате первому лицу уплаченной им пострадавшему суммы.

5 Венская конвенция о гражданской ответственности за ядерный ущерб 1963 г., ст. I, п. 1 k

6 Федеральный закон от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии», ст. 53, 59

7 Федеральный закон от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии», ст. 54

8 Федеральный закон от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии», ст. 54

9 Гражданский кодекс Российской Федерации, ст. 1079

10 Венская конвенция о гражданской ответственности за ядерный ущерб 1963 г., ст. IV, п. 3

11 Федеральный закон от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии», ст. 54

12 Вид вины, характеризуемой как легкомыслие или небрежность. Совершенным по неосторожности признается проступок, если лицо, его совершившее, предвидело возможность наступления вредных последствий своего действия (бездействия), но без достаточных к тому оснований самонадеянно рассчитывало на предотвращение таких последствий либо не предвидело возможности наступления таких последствий, хотя должно было и могло их предвидеть.

13 Гражданский кодекс Российской Федерации, ст. 1081

14 См. пояснения выше.

15 Венская конвенция о гражданской ответственности за ядерный ущерб 1963 г., ст. X

16 Венская конвенция о гражданской ответственности за ядерный ущерб 1963 г., ст. IV, п. 5

17 Венская конвенция о гражданской ответственности за ядерный ущерб 1963 г., ст. V

18 Федеральный закон от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии», ст. 55

19 О сути деликтного права см. пояснения выше.

20 Гражданский кодекс Российской Федерации, ст. 1064

21 Федеральный закон от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии», ст. 57

22 Венская конвенция о гражданской ответственности за ядерный ущерб 1963 г., ст. VII

23 Там же.

24 Федеральный закон от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии», ст. 56

25 Венская конвенция о гражданской ответственности за ядерный ущерб 1963 г., ст. VI

26 Федеральный закон от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии», ст. 58

27 Федеральный закон «О международных договорах Российской Федерации» от 15.07.1995 № 101-ФЗ, ст. 5, ч. 3

28 Часть 3 Федеральный закон «О международных договорах Российской Федерации» от 15.07.1995 № 101-ФЗ, ст. 5, ч. 3

29 Венская конвенция в редакции Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г., ст. IB

30 Венская конвенция в редакции Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г., ст. I

31 Венская конвенция в редакции Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г., ст. I

32 Венская конвенция в редакции Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г., ст. IA

33 Венская конвенция в редакции Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г., ст. IA

34 Пояснительный текст к Венской конвенции 1997 г. о гражданской ответственности за ядерный ущерб и Конвенции 1997 г. о дополнительном возмещении за ядерный ущерб, МАГАТЭ, 2004, С. 37

35 Венская конвенция в редакции Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г., ст. I

36 Венская конвенция в редакции Протокола о внесении поправок в Венскую конвенцию о гражданской ответственности за ядерный ущерб 1997 г., ст. I

37 Положения, которые:

a) предусматривают строгую ответственность в случае ядерного инцидента тогда, когда имеет место значительный ядерный ущерб за пределами площадки ядерной установки, на которой произошел инцидент;

b) требуют компенсации убытков любому лицу, иному, чем оператор, ответственный за ядерный ущерб, в той мере, в какой это лицо на основании закона несет ответственность за предоставление возмещения; и

c) обеспечивают наличие как минимум 1000 млн. СПЗ в отношении гражданской атомной станции и как минимум 300 млн. СПЗ в отношении других гражданских ядерных установок для такой компенсации убытков.

38 Сколько атомных станций работает в мире и в России? Атомэнергомаш. http://www.aem-group.ru/mediacenter/informatoriy/skolko-atomnyix-stanczij-rabotaet-v-mire-i-v-rossii.html (последнее посещение 13 апреля 2016 г.)

39 Согласно Совместному протоколу в отношении ядерного инцидента применяется либо Венская, либо Парижская конвенция:

— при ядерном инциденте **на ядерной установке** — конвенция, участником которой является государство, на чьей территории расположена ядерная установка.

— при ядерном инциденте **вне ядерной установки** в связи с ядерным материалом в перевозке — та конвенция, участником которой является государство, на чьей территории расположена ядерная установка, оператор которой несет ответственность.

40 Список стран-участниц Венской конвенции о гражданской ответственности за ядерный ущерб по состоянию на 27 января 2014 г., МАГАТЭ http://www.iaea.org/Publications/Documents/Conventions/liability_status.pdf (последнее посещение 13 апреля 2016 г.)

41 Список стран-участниц Парижской конвенции об ответственности перед третьей стороной в области ядерной энергии по состоянию на 30 июля 2015 г. Агентство по ядерной энергии http://www.oecd-nea.org/law/paris-convention-ratification.html (последнее посещение 13 апреля 2016 г.)

42 Список стран-участниц Совместного протокола о применении Венской и Парижской конвенций по состоянию на 30 апреля 2014 г., МАГАТЭ. http://www.iaea.org/Publications/Documents/Conventions/jointprot_status.pdf (последнее посещение 13 апреля 2016 г.)

43 Список стран-участниц Конвенции о дополнительном возмещении за ядерный ущерб по состоянию на 4 февраля 2016 г. МАГАТЭ. https://www.iaea.org/Publications/Documents/Conventions/supcomp_status.pdf (последнее посещение 13 апреля 2016 г.)

44 Список стран-участниц Конвенции о дополнительном возмещении за ядерный ущерб по состоянию на 4 февраля 2016 г. МАГАТЭ. https://www.iaea.org/Publications/Documents/Conventions/supcomp_status.pdf (последнее посещение 13 апреля 2016 г.).

45 См. пояснения выше.

46 Средства фонда предполагается формировать за счет взносов государств-участников Конвенции о дополнительном возмещении.

47 Брюссельская дополнительная конвенция 1982 г., ст. 3, п. b, ii

48 Pelzer Norbert. The Convention on Supplementary Compensation for Nuclear Damage (CSC) — A Cornerstone of a Global Nuclear Liability Regime? *ATW — International Journal for Nuclear Power*. 2015 Vol. 60, Issue 6, June. P. 394

49 IAEA Action Plan on Nuclear Safety, 13 September 2011

Кямал Гасымов

ДРУГАЯ ВОЙНА: КОНФЛИКТ ВНУТРИ АНТИАСАДОВСКИХ СИЛ

Режим прекращения огня в Сирии, который вступил в силу в феврале 2016 г., высветил ряд интересных процессов и фактов, которые еще не получили должной оценки. В первую очередь, речь идет о глубоких политических и идеологических разногласиях между основными участниками антиасадовских сил.

Зыбкое *затишье* показало, что со временем эти разногласия будут только усиливаться и даже *внешняя угроза* — продвижение правительственных войск и вступление в войну ВКС РФ — не способствует их устранению.

АЛЬ-КАИДА ПРОТИВ ФЛАГОВ РЕВОЛЮЦИИ

Февральское прекращение огня дало толчок мирным демонстрациям[1] в окрестностях Дамаска и в городах провинций Дараа, Идлиб и Алеппо[2]. Начиная с 4 марта люди начали выходить на улицы с *флагом революции* (*алям ас-саура*)[3], скандируя лозунги о единении оппозиции и призывая к окончательному прекращению насилия. Отличительной чертой этих демонстраций является то, что они одновременно проходили в разных частях Сирии и в них приняли участие как представители *умеренной* и светской оппозиции (командиры отрядов, связанных со *Свободной сирийской армией*)[4], так и представители исламистских фракций[5] (например, лидеры движения *Ахрар аш-Шам*)[6].

Разумеется, СМИ и активисты сирийской оппозиции, как политической, так и военной, представили этот процесс как доказательство того, что выступления против режима Б. Асада изначально носили мирный характер и что как только режим останавливает боевые действия, люди выражают свой протест методами гражданского сопротивления. К тому же в контексте мартовских переговоров в Женеве оппозиции необходимо было показать миру, что она на самом деле придерживается демократических ценностей и что светские идеи и силы все еще способны мобилизовать сирийцев.

Однако 7 марта в Идлибе одна из подобных демонстраций была разогнана сторонниками *Джабхат ан-Нусры*[7] (ячейка *Аль-Каиды* в Сирии, обе организации признаны террористическими и запрещены на территории России). Они неожиданно ворвались в центр демонстрации, размахивая черно-белыми флагами, и растол-

кали ее участников. Исходя из дискуссий в социальных сетях между очевидцами событий, сторонники *Ан-Нусры* были недовольны чрезмерно светскими лозунгами и изобилием *неисламских* флагов.

На данное происшествие очень резко отреагировали журналисты, активисты, политики и военные, связанные, в основном, с США и *Национальной коалицией сирийских революционных и оппозиционных сил* (далее *Нацкоалиция*). В социальных сетях поднялась волна осуждения *Ан-Нусры*, которую стали обвинять в нетерпимости, фанатизме и предательстве *идеалов революции*. Юридический советник США Усама Абу Зайд написал в своем твиттере, что нет нужды ни в армии, ни в спецслужбах режима в Идлибе, когда под именем религии запрещаются демонстрации[8].

Отметим, что Идлиб с августа 2015 г. контролируется *Джайш аль-Фатах* (*Армией завоевания*), которая представляет собой объединение из 7 групп, самые крупные из которых — это движение *Ахрар аш-Шам* и *Ан-Нусра*.

После разгона демонстраций руководство *Ахрар аш-Шама* издало заявление, в котором объявило, что не причастно к данному инциденту[9]. В ответ официальный представитель *Ан-Нусры* заявил[10], что за порядок в Идлибе отвечают все группы, входящие в *Джайш аль-Фатах*, следовательно, все эти группы несут ответственность за то, что произошло. Он также добавил, что *Ан-Нусра* защищала демонстрации в 2011 г. и будет продолжать оберегать мирное население.

Позднее представители *Ан-Нусры* распространили документ о том, что приказа о разгоне демонстраций не было, а столкновение произошло по личной инициативе отдельных сторонников движения.

Однако не успели дискуссии вокруг разгона демонстрации утихнуть, как 13 марта отряды *Ан-Нусры* в союзе с отрядами *Джунд аль-Акса* неожиданно атаковали позиции *13-й дивизии* США в Идлибе. В результате атаки *Ан-Нусра* захватила главный штаб *дивизии* в городке Маарет аль-Нуман[11], несколько складов с оружием, а также взяла в плен свыше 20 солдат и несколько офицеров. Командир *дивизии* Ахмад ас-Сауд заявил, что его отряды сопротивлялись несколько часов, но, желая избежать разрушения города и гибели местного населения, сложили оружие рано утром.

В свою очередь, *Ан-Нусра* распространила заявление[12] о том, что на самом деле отряды *13-й дивизии* неожиданно напали на позиции и дома бойцов *Ан-Нусры*. Именно это и послужило причиной конфликта. Командование *13-й дивизии* назвало это заявление необоснованным и ложным.

Разгром *Ан-Нусрой дивизии* США вызвал острую реакцию как среди сторонников США, так и *Исламского фронта*. Например, известный оппозиционный активист Ахмад Абазид задался вопросом о том, сколько еще США и другие группы будут терпеть произвол *Ан-Нусры*, добавив: «а чего вы ожидали от *Аль-Каиды*?»[13]. Абу Анас аль-Канакри, один из шариатских судей *Джайш аль-Ислам* (*Армия ислама*), заявил, что если его организация и другие исламские группы не остановят преступников, то он покинет ее[14].

Сторонники США в Маарет аль-Нумане также выразили недовольство. Уже 14 марта, на следующий день после конфликта, в городе начались демонстрации против *Ан-Нусры*, с требованием отпустить пленных бойцов *13-й дивизии*[15]. Часть

демонстрантов ворвалась в штабы и дома, занятые бойцами *Ан-Нусры*[16]. В результате под давлением демонстрантов бойцы *Ан-Нусры* оставили некоторые позиции. Кроме того, *Ан-Нусра* освободила пленных, но *13-я дивизия* утверждает[17], что часть бойцов и несколько офицеров остаются в плену, и что *Ан-Нусра* так и не вернула захваченное оружие.

НЕОБЪЯВЛЕННАЯ ВОЙНА

Нужно отметить, что это далеко не первое столкновение между *Ан-Нусрой* и отрядами ССА. В 2013 г. *Ан-Нусра* атаковала отряды ССА в городе Аазазе на сирийско-турецкой границе, пытаясь взять под контроль границу с Турцией. В ноябре 2014 г. *Ан-Нусра* атаковала в районе Джабаль аз-Завия[18] *Сирийский революционный фронт* (*Джабхат ас-суввар ас-сурийа*) — крупное объединение, воевавшее под флагом ССА и получавшее помощь от США и КСА. В итоге ее лидер Джамал Ма'руф, которого сирийская оппозиция рассматривала как героя войны с режимом Б. Асада и с организацией *Исламское государство* (организация признана террористической и запрещена на территории России), а также как видного командира, защищающего *светские и национальные идеалы революции*, вынужден был бежать в Турцию.

С октября 2014 по январь 2015 г. отряды *Ан-Нусры* систематически уничтожали *Движение Хазм*[19] (*Стойкое движение*), захватывая штабы, склады с оружием и укрепления *Хазма* на северо-западе Сирии[20]. Бойцы и командование *Хазма* получали помощь от США в виде военной подготовки и американских ПТРК[21] и часто описывались американскими аналитиками как образец *умеренной оппозиции*[22].

Вслед за *Хазмом* жертвой[23] *Ан-Нусры* стала 30-я дивизия ССА, часть которой была разгромлена, а другая часть взята в плен. И на этот раз оружие (в том числе американские ПТРК) попало в руки джихадистов.

Отметим, что между *Ан-Нусрой* и военными силами оппозиции возникал конфликт не только в северных, но и в южных районах Сирии. На юге около 50 групп ССА в феврале 2014 г. объединились в единый *Южный фронт* (*Аль-джабха аль-джанубийа*), что изменило баланс сил в провинциях Дараа и Аль-Кунейтара. Серьезные разногласия между ЮФ и *Ан-Нусрой* возникли в апреле 2014 г., когда они вместе отбили у войск Б. Асада городок Насиб[24] (на границе с Иорданией), где находится пограничный КПП. Тогда ССА удалось отстоять у ячейки *Аль-Каиды* этот важный стратегический пункт.

Определяющее превосходство *Южного фронта* в живой силе и технике способствует тому, что *Ан-Нусра* ведет осторожную политику на юге. Но тем не менее представители ЮФ жаловались, что бойцы *Ан-Нусры* время от времени перекрывают дороги, арестовывают людей, пытаются навязать свою судебную систему[25] и периодически вмешиваются во внутренние дела ЮФ. Все закончилось тем, что в середине апреля 2014 г. *Южный фронт* издал официальное заявление, в котором объявил, что отвергает все формы сотрудничества с *Ан-Нусрой*[26]. Это еще больше осложнило отношения между сторонами.

Таким образом, силы, с которыми у *Ан-Нусры* чаще всего возникает конфликт, объединяют следующие аспекты: они ассоциируют себя с ССА, признают национальное государство, демократию и парламентскую систему и получают вооруже-

ние от США и ее союзников. Причем конфликту предшествуют рост популярности и военные успехи той или иной группы.

К примеру, *13-я дивизия* активно участвовала в боевых действиях против правительственных войск в северных и южных пригородах и селах провинций Алеппо, в северных районах Хамы, в Сахль аль-Габ, в провинции Латакия. Наличие большого количества ПТРК позволило ей уничтожить десятки танков противника, именно поэтому остальные группы привлекали *13-ю дивизию* к совместным боевым операциям. Например, она участвовала в захвате военных баз *Вади ад-Дайф* и *Аль-Хамидийя* в провинции Идлиб (в декабре 2014 г.) и в операции *Захват Алеппо* (май 2015 г.) вместе с *Ан-Нусрой* и *Ахрар аш-Шамом*.

Страницы *дивизии* в социальных сетях демонстрировали многочисленные фотографии и видео с боями против правительственных войск и курдских *Отрядов народной самообороны*, а также с уничтоженной техникой правительственной армии[27].

Со временем конструировался и героический образ лидера движения — подполковника Ахмад ас-Сауда, биография которого дает ему все основания занять важное место среди военных лидеров сирийской оппозиции: в начале гражданской войны покинул правительственную армию из-за политических разногласий с режимом, побывал в плену у организации *Исламское государство*, принимает участие во всех важных боях оппозиции на севере и северо-западе Сирии, придерживается идей *светского государства* и воюет под *флагом революции*[28].

Однако в итоге с *13-й дивизией* произошло то, уже что происходило с другими подобными группами ССА на территориях, где *Ан-Нусра* распространяет свою политическую и идеологическую гегемонию: солдаты взяты в плен, штабы разрушены, склады с оружием (в том числе и с американскими ПТРК) захвачены, а командир *дивизии* спасся бегством и скрывается в Турции[29] (как когда-то Джамал Ма'руф).

ИЗВЕЧНАЯ ПРОБЛЕМА ШАРИАТСКОГО СУДА

После конфликта как представители *Исламского фронта*, так и ССА выступили с инициативой формирования независимой шариатской комиссии или суда, который бы разрешил спор между сторонами и положил конец вражде. В данный момент с учетом продвижения правительственной армии и авиаударов российских ВКС ни одна из сторон, воюющих против Б. Асада, не заинтересована в затяжном междоусобном конфликте.

Однако за время гражданской войны шариатские институты показали свою полную неэффективность. Они не смогли разрешить конфликт между *Ан-Нусрой* и *Революционным сирийским фронтом*, между ИГ и *Ан-Нусрой*, между ИГ и *Исламским фронтом*, между *Ан-Нусрой* и движением *Хазм* и т. д. Каждый раз, когда происходит конфликт и стороны предлагают создать независимый суд, возникает проблема беспристрастного арбитра. Одним словом, конфликтующие стороны не могут договориться о судьях.

Обычно люди (чаще всего исламские авторитетные проповедники), которых стороны предлагают в качестве судей, имеют очень разные политические и идео-

логические предпочтения и совершенно по-разному смотрят на происходящие в Сирии процессы. И поэтому спор о составе шариатского комитета продолжается бесконечно и ничем не заканчивается. Даже если комитет все-таки создается, сильная сторона обычно отказывается подчиниться решению суда.

В случае с конфликтом между *13-й дивизией* и *Ан-Нусрой* произошло то же самое — руководители *дивизии* предложили в качестве судей шейха Абу Анаса аль-Канакри и Аймана Мухаммада Харуша[30], а *Ан-Нусра* — Абдаллаха аль-Мухайсини и Абд ар-Разика Махди.

Исходя из имен, видно, что первая сторона предпочитает шейхов, которые либо критически относятся к *Ан-Нусре* (как Аль-Канакри, которого, кстати, так и включили в комиссию), либо сохраняют определенную независимость от джихадистских движений (как Айман Харуш), в то время как вторая сторона предлагает своих основных идеологов (в частности, Аль-Мухайсини). В результате шариатский комитет был сформирован из представителей *Лиги исламских ученых Леванта* (*Рабита ахл аль-ильм фи-ш-Шам*). Однако данная организация основана по инициативе Аль-Мухайсини и состоит в основном из богословов Идлиба, сочувствующих *Ан-Нусре*.

В своем последнем заявлении Лига ограничилась призывом прекратить вражду и освободить пленных[31]. Интересно, что заявление также призывает пользователей социальных сетей остановить дискуссии о конфликте и не подливать масла в огонь (но дискуссии до сих пор продолжаются, и очень многие оппозиционные активисты, журналисты и политики требуют наказания *Ан-Нусры*).

Пока члены шариатского комитета призывали стороны к миру и уверяли в скором справедливом разрешении конфликта на основе норм исламского права, 19 марта пресс-служба *13-й дивизии* заявила, что бойцы *Ан-Нусры* и *Джунд аль-Аксы* на шестидесяти машинах въехали в Маарет аль-Нуман и опять заняли город[32].

После этого 21 марта члены шариатского комитета все-таки издали документ, в котором говорится, что *Ан-Нусра* и *13-я дивизия* заключили соглашение о прекращении боевых действий и призывов к вражде в социальных сетях и на демонстрациях. Однако *13-я дивизия* охарактеризовала этот документ[33] как отражающий интересы лишь одной стороны — *Ан-Нусры*[34].

В результате *13-я дивизия* потеряла всякую надежду на то, что комитет заставит *Ан-Нусру* вернуть захваченное оружие, и с отчаянием заявила, что «законы шариата применяются только в отношении слабых»[35]. В целом, ни одна из организаций или групп в Сирии не предприняла никаких мер, чтобы защитить это формирование. Но видимо наибольшее удивление *13-й дивизии* вызвало «странное молчание ССА»[36].

В итоге шариатский комитет прекратил свою работу, ссылаясь на то, что стороны не хотят сотрудничать, «а бойцы *Джунд аль-Аксы* и вовсе не являются на судебные заседания»[37].

ПРОЕКТ *ИСЛАМСКОГО ЭМИРАТА*

Мы уже писали о том, что *Ан-Нусра* медленно, но верно уничтожает все светские или национальные проекты в Сирии[38]. Однако, в отличие от ИГ, она при этом

сотрудничает и пытается вести диалог с более или менее идеологически близкими к ней сирийскими исламистскими движениями (как-то *Ахрар аш-Шам* и другие группы, входящие в *Исламский фронт*), не теряя надежды со временем привить им транснациональную джихадистскую идеологию *Аль-Каиды*. В сложном контексте гражданской войны в Сирии подпольная организация развила свои навыки по взаимодействию с населением и сотрудничеству с другими движениями. Кроме того идеологи *Ан-Нусры* внимательно следят за социально-политическими изменениями в Сирии и проводят свою политику в контексте меняющихся трендов и дискурсов.

Когда начались демонстрации, сторонники *Ан-Нусры* и бойцы из других формирований стали задаваться вопросом, можно ли принимать в них участие, если они проходят под *флагом революции*. Идеолог *Ан-Нусры* Абдаллах аль-Мухайсини ответил, что участие в подобных демонстрациях в целом не противоречит исламскому праву[39]. Как *факих*, ежедневно занимающийся *реальной политикой*, Аль-Мухайсини осознает, что флаг стал символом сирийской оппозиции, он важен и для ее союзников, и для определенного числа простых сирийцев. Данный контекст способствует тому, что идеолог боевого крыла *Аль-Каиды* в Сирии, который считает национальный флаг вещью в общем-то ненужной, находит прагматичное решение проблемы.

После разгона демонстраций в Идлибе сторонники и представители *Ан-Нусры* стали ссылаться на фетву Аль-Мухайсини и указывать на то, что люди во время демонстраций стояли как с *флагом революции*, так и с *черным флагом с шахадой* — и при этом не было столкновений (сирийские блогеры и журналисты выложили фотографии[40], подтверждающие это). Однако при внимательном прочтении текста Аль-Мухайсини становится ясно, что *Аль-Каида* не изменила своего отношения к светским символам, но изменила тактику и стратегию идеологической борьбы.

Дело в том, что, согласно Аль-Мухайсини, во *флаге революции* нет ничего плохого, если он поднят как символ борьбы против режима. Но если он воспринимается как символ будущего светского государства в Сирии, то поднимать его запрещено, ибо это означает неверие. По его мнению, если кто-то поднимает флаг с целью заменить одну секулярную систему на другую, то он «шахидом стать не сможет» (т. е. его борьба с точки зрения ислама незаконна)[41]. Таким образом, сторонникам *Ан-Нусры* советуют проявлять *терпимость* к флагу, так как он принят многими группами, положительно действует на бойцов, вдохновляет на войну с режимом и т. д. Однако ясно, что для отрядов ССА, таких как *13-я дивизия*, флаг оппозиции символизирует не только борьбу с режимом, но и национальное государство, временное сирийское правительство, парламент — все то, что *Ан-Нусра* отвергает (или интерпретирует радикально иначе)[42].

Подобные глубокие политико-идеологические противоречия между *Ан-Нусрой* и ССА чаще всего игнорируются — о них вспоминают только тогда, когда возникает военный конфликт. И хотя многие представители сирийской оппозиции понимают, насколько серьезны эти противоречия, из-за ряда причин (новый конфликт в условиях войны с Б. Асадом, военная мощь *Ан-Нусры*, союз между *Ан-Нусрой* и *Ахрар аш-Шамом* и т. д.) предпочитают не выносить их на обсуждение.

Таким образом, напав на *13-ю дивизию, Ан-Нусра* еще раз показала, что будет пресекать усиление идеологически отличных групп и распространение светских идей на территориях, которые контролирует. И это объяснимо: все *светские* или национальные проекты — прямые конкуренты *Аль-Каиды*, потому как представляют угрозу (и альтернативу) транснациональному проекту, с помощью которого *Аль-Каида* привлекает бойцов и материальные ресурсы.

С момента вступления в гражданскую войну в Сирии *Ан-Нусра* воздерживается от объявления исламского государства и заявляет, что будущее сирийского государства будет решаться представителями всех групп, которые воевали против Б. Асада[43], тем самым пытаясь представить себя как силу, принимающую во внимание интересы других политических объединений. Подобная примирительная политика в условиях сирийской войны оказалась эффективной. Сотрудничество с сирийскими *исламистскими* движениями, например *Ахрар аш-Шамом,* и участие в совместных военных операциях с отрядами США приносят *Ан-Нусре* славу и сторонников (к слову, в некоторых сирийских городах, в частности в Идлибе, прошли демонстрации и в поддержку *Ан-Нусры*).

Лидер *Аль-Каиды* Айман аз-Завахири, которому остается верен глава *Ан-Нусры* Абу Мухаммад аль-Джулани, не возражает ни против демонстраций, ни против выборов. Однако он считает, что демонстрации допустимы в том случае, если они проводятся с целью установления исламской системы, а не для замены одной неисламской формы правления на другую. Такое же отношение у него и к выборам — руководство *Аль-Каиды* отвергает монархию и считает, что мусульмане должны совещаться по социальным и политическим вопросам, особенно относительно избрания правителя. Однако кого бы они не избрали, править он должен по шариату. Иначе говоря, за долгие годы своей политической и военной борьбы *Аль-Каида* стала пересматривать методы и средства, дискутировать по частностям ради достижения главной цели — создания социального пространства и, в конечном итоге, политической системы исходя из собственной интерпретации ислама[44].

Подтверждением этому является и социальная политика *Ан-Нусры* в Идлибе, где она создает структуры правопорядка, суды, медресе, исламские институты и центры, школы для проповедников, издает книги и журналы, работает с населением, проводит публичные лекции и оказывает широкую гуманитарную помощь. Одним словом, претворяет в жизнь проект *Аль-Каиды* по построению исламского государства в отдельно взятом регионе.

В отличие от организации *Исламское государство*, *Ан-Нусра* из тактических соображений не делает заявлений о своем глобальном проекте, но систематически предпринимает шаги по его практической реализации на севере и северо-западе Сирии. Примечательно, что после взятия Идлиба *Ан-Нусра* не впустила представителей *Нацкоалиции* в город[45], еще раз подтвердив, что не желает делить власть со *светской* оппозицией. В принципе, Аль-Джулани не скрывал[46], что *Ан-Нусра* стремится к построению *Исламского эмирата* в Сирии, но он считает, что в условиях гражданской войны не время объявлять об исламском государстве. Это будет сделано, когда придет время, а пока *Ан-Нусра* через шариатские суды, гуманитарную помощь и иные социальные и политические проекты подготавливает почву для этого.

Осуществляя свой план, *Ан-Нусра,* в отличие от ИГ, старается не вступать в открытое противостояние с отрядами ССА — но только до тех пор, пока не видит в них реальную угрозу своему проекту. Кроме этого, одной из причин агрессии *Ан-Нусры* является желание приобрести оружие (особенно ПТРК), которым союзники снабжают отряды ССА.

ДВА ГОЛОСА ВНУТРИ *АН-НУСРЫ*

Конфликт с *13-й дивизией* интересным образом оживил противоречия и скрытые разногласия внутри *Ан-Нусры*.

Дело в том, что среди идеологов и командиров группировки есть люди, которые считают, что их движению следует быть более умеренными по отношению к другим формированиям (особенно к отрядам ССА), воюющим против Б. Асада. Согласно им, главными врагами *Ан-Нусры* являются ИГ, режим Б. Асада и *Хезболла*, а не *умеренная* оппозиция или отряды, воюющие под *светским* флагом.

Переосмыслив опыт *Аль-Каиды* в Афганистане и Ираке, эти люди стали воспринимать традиционную *аль-каидовскую* концепцию исламского эмирата как утопичную. *Ан-Нусру* они видят важным участником будущего политического процесса в постасадовской Сирии и понимают, что война с оппозицией ставит под угрозу это будущее.

Например, бывший религиозный авторитет и командир восточного фронта *Ан-Нусры* иракец Абу Мария аль-Кахтани и идеолог движения кувейтский богослов Али аль-Арджани резко критикуют определенные группы внутри *Ан-Нусры*, которые, по их мнению, разделяют идеологию ИГ (а именно обвиняют в неверии отряды ССА и некоторые группы *исламистской оппозиции*).

Сразу же после конфликта между *Ан-Нусрой* и *13-й дивизией* Аль-Кахтани сделал обращение, в котором заявил, что всецело поддерживает демонстрации под флагом революции против режима[47]. Он также добавил, что конфликты возникают, потому что во многих отрядах есть *игиловцы*, причем они могут не иметь институциональной связи с ИГ, но видят мир как ИГ. Аль-Кахтани описал это явление как *да'шана*, что означает становление *игиловцем*, человеком крайне нетерпимым и практикующим чрезмерное насилие (прежде всего, против мусульман). Он также отметил, что некоторые бойцы находятся под влиянием радикальных шейхов, которые призывают мусульман убивать друг друга несмотря на то, что живут за пределами боевых действий. По всей видимости, Аль-Кахтани имел в виду классиков джихадистской мысли Абу Мухаммада аль-Макдиси и Абу Катаду аль-Фаластини, которые живут в Иордании, но имеют сильное влияние на бойцов в Сирии, особенно из числа джихадистских групп[48].

На это указывает и критика Али аль-Арджани, который был более резок и конкретен, обвинив Абу Мухаммада аль-Макдиси в подстрекательстве и в распространении идей *такфиризма* среди бойцов *Ан-Нусры*[49]. Сразу же после этих заявлений некоторые представители *Ан-Нусры* обрушились на Аль-Кахтани и Аль-Арджани с резкой критикой. Последнему даже угрожали расправой.

Но наибольшие споры вызвали *откровения* шейха Хузайфы Аззама, известного исламского активиста и сына *духовного отца* афганского джихада Абдаллаха Юсу-

фа Аззама. Через несколько дней после разгрома *Ан-Нусрой* позиций *13-й дивизии* Аззам обрушился с пространной критикой на *Ан-Нусру* и ее лидеров. В серии статей Аззам обвинил их в том, что они ничем не отличаются от командиров ИГ — оправдывают насилие через *такфир*, целенаправленно уничтожают другие группы, воюющие против Б. Асада, и воплощают в жизнь собственный проект исламского эмирата[50]. Он также сообщил, что *Ан-Нусра* когда-то наладила хорошие отношения с лидером *Революционного сирийского фронта* Джамалом Ма'руфом, и последний даже передавал *Ан-Нусре* оружие, которое получал от Высшего военного совета ССА на границе с Турцией[51]. Однако, по его словам, *Ан-Нусра* использовла Ма'руфа, чтобы уничтожить его армию.

Это заявление важно по двум причинам. Во-первых, оно указывает на то, что отряды ССА время от времени отдают или продают джихадистам оружие, которое предоставляют им США и их союзники. Кстати, это было одной из причин, по которым США ограничили помощь ССА. Во-вторых, лидер *Ан-Нусры* Аль-Джулани не раз заявлял, что не получает оружие от Турции, КСА и Катара и не имеет никаких связей с западными странами. В одной из своих речей он даже назвал Высший военный совет ССА *вероотступниками*[52]. В этой связи слова Аззама наносят вред пропагандистскому дискурсу *Ан-Нусры* об автономности от каких-либо стран.

Кроме этого, Аззам упрекает *Ан-Нусру* в том, что она лукавит, утверждая, будто все силы, участвующие в войне против сирийского правительства, решают возникающие между ними проблемы в «течение 24 часов за чашкой чая». Что касается *Ан-Нусры,* ни один конфликт, в который она была вовлечена, разрешить не удалось. По его словам, до сих пор у *Ан-Нусры* был конфликт с 14 группами (в основном связанными с ССА), но шариатские комитеты ничего не смогли сделать — все закончилось тем, что *Ан-Нусра* либо уничтожила, либо изгнала их[53]. В итоге Аззам просит прощения у всех групп за то, что он не смог им помочь в разрешении конфликта с *Ан-Нусрой*.

Откровения Аззама вызвали отклик в арабских СМИ и широкие дискуссии в социальных сетях, а официальный представитель *Ан-Нусры* посвятил их опровержению 106 сообщений в Твиттере[54].

Таким образом трения среди идеологов *Ан-Нусры* показали, что внутри движения не все согласны с ее политикой по отношению к иным группам. Что касается разоблачительной информации Аззама, ее обнародование в данный момент говорит о растущем недовольстве политикой *Ан-Нусры* среди других сирийских исламистских движений. *Ан-Нусру* все чаще воспринимают как движение, которое ведет свою собственную игру и игнорирует интересы иных сторон.

ДИЛЕММА АХРАР АШ-ШАМА

Конфликт между *Ан-Нусрой* и *13-й дивизией* не только выявил противоречия внутри самой *Ан-Нусры,* но и поставил в сложное положение представителей *Исламского фронта*, а именно социально-политическое движение *Ахрар аш-Шам*.

Дело в том, что *Ахрар аш-Шам* — довольно сложное и эклектичное исламское движение, состоящее из сирийцев и *вплетенное* в местный контекст. Оно совмещает в себе сирийский салафизм во всем его многообразии, широкий опыт поли-

тической борьбы сирийских *Братьев-мусульман* (организация признана террористической и запрещена на территории России), а также подпольную деятельность и военный опыт *салафитского джихадизма* (*ас-салафийа аль-джихадийа*). В задачи *Ахрар аш-Шама* не входит построение халифата или эмирата. Все социальные и политические проекты этого движения осуществляются в границах современной Сирии. Оно видит себя как национальная исламская альтернатива баасистскому режиму, *светской* или *умеренной* сирийской оппозиции и ИГ.

Однако за период гражданской войны это движение сблизилось с *Ан-Нусрой*, которая считает *Ахрар аш-Шам* наиболее политически и идеологически близкой к себе группой. Во-первых, *Ахрар аш-Шам,* как и *Ан-Нусра,* не признает легитимность *Нацкоалиции* и Высшего военного совета ССА. Во-вторых, многих полевых командиров и религиозных авторитетов *Ан-Нусры* и *Ахрар аш-Шама* связывают близкие личные отношения. К тому же одним из основателей движения *Ахрар аш-Шам* был ветеран афганской войны, боевой товарищ и друг Аймана аз-Завахири Абу Халид ас-Сури (убит в результате теракта ИГ в феврале 2014 г.).

Благодаря своим тесным связям 24 марта 2015 г. *Ахрар аш-Шам* вместе с *Ан-Нусрой* создали *Джайш аль-Фатах* (*Армию завоевания*) для ведения боев на севере Сирии, прежде всего в провинции Идлиб. Эта союзная армия взяла под контроль практически всю территорию провинции Идлиб, в конце апреля захватила город Джиср аш-Шугур, а 9 сентября — военный аэропорт Абу аз-Зухур.

Однако с течением времени события в Сирии показали, что транснациональный джихадистский проект *Ан-Нусры* в долгосрочной перспективе представляет угрозу для проекта сирийского политического ислама *Ахрар аш-Шама*.

Лидеры *Ахрар аш-Шама,* как и другие представители *Исламского фронта,* всегда с тревогой наблюдали за конфликтами *Ан-Нусры* с отрядами ССА. А некоторые группы в самой *Ан-Нусре* критиковали *Ахрар аш-Шам* за излишнюю открытость по отношению к ССА и за сотрудничество с Катаром и Турцией.

В конце сентября 2015 г. один из богословов, руководящий образовательной программой *Ан-Нусры,* и ее бывший официальный представитель Абу Фирас ас-Сури опубликовал текст[55], в котором обвинил *Ахрар аш-Шам* в оппортунизме и лицемерии. Согласно ас-Сури, *Ахрар аш-Шам* заигрывает с Западом, пытаясь расположить к себе *страны куфра* (здесь можно усмотреть и намек на статьи в западных изданиях руководителя внешнеполитического ведомства *Ахрар аш-Шама* Лабиба ан-Наххаса, в которых последний пытался убедить западного читателя в том, что его движение осуждает террор и не возражает против демократических принципов[56]). Ас-Сури с сарказмом отмечает, что *Проект уммы* (*машру аль-умма*) — политическая программа *Исламского фронта*, которую разрабатывали лидеры *Ахрар аш-Шама,* — это на самом деле местечковый сирийский проект (т. е. не глобальный транснациональный проект, нацеленный на объединения всей уммы).

Однако главной причиной недовольства Абу Фираса ас-Сури и некоторых других сторонников *Ан-Нусры* стало то, что в мае 2014 г. командиры *Ахрар аш-Шама* подписали документ под названием *Революционная хартия чести*, который назвал целями сирийской революции достижение свободы, справедливости и безопасности для всех представителей сирийского общества. В документе также сказано, что сирийский народ стремится создать «государство закона, свобод и справед-

ливости»[57]. При этом ничего не говорится об исламском государстве и установлении шариата — на что и обратила внимание *Ан-Нусра*.

Таким образом после атаки *Ан-Нусры* на *13-ю дивизию* сторонники *Ахрар аш-Шама* выразили обеспокоенность и призвали стороны к примирению через шариатский суд. Однако *13-я дивизия*, а также оппозиционные активисты, журналисты, богословы и политики в Идлибе и в других городах Сирии ждали от *Ахрар аш-Шама* более резкого заявления.

Более ясная позиция *Ахрар аш-Шама* была выражена лишь 23 марта. В интервью газете *Аль-Ахд* глава отдела по внешнеполитическим отношениям движения *Лабиб ан-Наххас* сказал, что признает заслуги *Ан-Нусры* в борьбе против режима, но отметил, что «наш проект полностью отличается от их проекта и видения будущего Сирии», а также заявил, что «действия *Ан-Нусры* в последние месяцы вызывают беспокойство у всех»[58].

Дело в том, что *Ахрар аш-Шам* в данный момент находится в сложном положении. С одной стороны, оно представляет себя как исламскую политическую альтернативу, налаживает связи с другими оппозиционными силами, а также с Катаром, Турцией и Саудовской Аравией, и серьезно обдумывает участие в политических процессах после окончания гражданской войны. Именно поэтому в декабре 2015 г. *Ахрар аш-Шам* послало (хотя и неохотно) своего представителя на конференцию в Эр-Рияде[59] и согласилось поддерживать режим прекращения огня[60].

Кроме этого, лидеры *Ахрар аш-Шама* пытаются показать (особенно западной публике), что именно их движение, будучи сирийской суннитской политической силой, способно стать реальной заменой баасистскому режиму и одержать идеологическую и военную победу над ИГ[61].

С другой стороны, *Ан-Нусра* для *Ахрар аш-Шама* — стратегические партнеры, у них общие проповедники, крепкие личные отношения между полевыми командирами и бойцами, они проводят совместные военные операции.

В этой ситуации некоторые группы в самом движении *Ахрар аш-Шам*, а также командование ССА и некоторые члены *Исламского фронта*, например *Джайш аль-Ислам* (*Армия ислама*), настоятельно советуют *Ахрар аш-Шаму* прекратить тесное сотрудничество с ячейкой *Аль-Каиды*. Многие силы сирийской оппозиции крайне недовольны подобным сотрудничеством, и давление на *Ахрар аш-Шам* постоянно растет. Представитель *Ахрар аш-Шама* заявил, что некоторые структуры сирийской политической оппозиции (не уточняя, какие именно) пытаются убедить Запад в том, что *Ахрар аш-Шам* — террористическая организация[62].

В свою очередь, *Ан-Нусра* требует от *Ахрар аш-Шама* определиться с идеологией, выразить четкую политическую позицию о будущем устройстве Сирии (светское оно будет или исламское) и прервать свои отношения с определенными силами, представляющими *светскую* сирийскую оппозицию.

Сложный выбор, который стоит сегодня перед *Ахрар аш-Шамом*, характерен для многих современных исламистских движений и наиболее точно описан исламоведом Оливье Руа — приспособиться к идеям, институтам и структурам национального государства или раствориться в транснациональном радикальном неофундаменталистском движении.

ЗАКЛЮЧЕНИЕ

Последние события в Сирии показали, что даже прекращение огня и вывод российских войск не способствовали объединению групп, воюющих против Б. Асада. Напротив, глубокие идеологические противоречия и политические разногласия между представителями *умеренной оппозиции* (*13-я дивизия* США), транснационального джихадизма (*Ан-Нусра*) и *политического ислама* (*Ахрар аш-Шам*) еще более обострились. В связи с этим опасения тех, кто уверен, что в случае окончания гражданской войны между сирийскими группами начнется междоусобная война (как между афганскими муджахидами после вывода советских войск), далеко не беспочвенны. Кроме того, отсутствие внятной реакции на враждебные действия *Ан-Нусры* в отношении *13-й дивизии* со стороны военных групп внутри Сирии (прежде всего, отрядов США) говорит о том, что США не функционирует как единая структура. Кроме того, даже идеологически и политически близкие друг другу группы, по всей видимости, находятся в постоянном соперничестве за финансовые ресурсы и военную помощь и не спешат оказать поддержку в случае, если одна из групп сталкивается с агрессией джихадистов. В третьих, конференция по объединению сирийской оппозиции в Эр-Рияде (на которую возлагали большие надежды как оппозиция, так и КСА) не достигла своей основной цели.

К тому же стало ясно, что внутри *Ан-Нусры* есть как радикальные группы, которые всеми силами пытаются уничтожить инакомыслящих среди оппозиции (особенно отряды, связанные с США) и преобразовать сирийские исламистские движения в ячейки *Аль-Каиды*, так и группы, занимающие примирительную позицию и желающие видеть *Ан-Нусру* в политическом будущем Сирии. Отметим, что вторая группа малочисленна, поэтому трения вряд ли приведут к расколу движения в ближайшем будущем.

Атака на *13-ю дивизию* и дискурс, который возник вокруг нее, показали, что *Ан-Нусра* продолжает проект по созданию в Сирии социально-политической и правовой системы в интерпретации *Аль-Каиды* и не собирается порывать с транснациональным джихадизмом. Дело в том, что сирийская политическая оппозиция[63] и некоторые союзники *Ан-Нусры* из числа исламистов (прежде всего, *Ахрар аш-Шам*)[64] считают, что ей пришло время разорвать связи с *Аль-Каидой*. На наш взгляд, это вряд ли когда-то произойдет, так как без этой связи *Ан-Нусра* перестанет существовать. *Ан-Нусра,* как и *Ахрар аш-Шам,* состоит преимущественно из сирийцев. Но командование и идеологи *Ан-Нусры* по большей части институционально связаны с *Аль-Каидой*. К тому же связь с *Аль-Каидой* привлекает к ней иностранный капитал и иностранных бойцов. Под командованием *Ан-Нусры* воюют такие группы, как *Армия переселенцев и помощников* (*Джейш аль-Мухаджирун ва аль-Ансар*), состоящая в основном из граждан стран СНГ (присягнула *Ан-Нусре* в сентябре 2015 г. из-за ослабления *Имарата Кавказ* — организация признана террористической и запрещена на территории России), батальон *Имам Бухари*, который состоит в основном из жителей среднеазиатских республик, *Джунд аль-Акса*, которая состоит из афганских, европейских, постсоветских и арабских бойцов и т. д. Одним словом, *Аль-Каида* для *Ан-Нусры* — международный бренд, основной источник и *мягкой*, и *жесткой* силы.

Примечания

1 Начиная с первой пятницы после вступления в силу режима прекращения огня Сирию охватили мирные демонстрации. Аль-Арабийя, 5 марта 2016 г., http://www.alarabiya.net/ar/arab-and-world/syria/2016/03/05/المظاهرات-السلمية-تعم-سوريا-في-أول-جمعة-منذ-بدء-الهدنة.html (последнее посещение: 14.06.2016).

2 Сирийские демонстрации подтверждают мирный характер революции. 5 марта 2016 г., http://alkhaleejonline.net/articles/1457119436464487200/-مظاهرات-سوريا-تأكيد-على-سلمية-الثورة-وسط-تأهب-لاستئناف-المعارك/ (последнее посещение: 14.06.2016).

3 Флаг с зеленой, белой и черной полосами и тремя красными звездами посередине. В 1932 г. стал флагом Сирийской республики (1930–1958). Объявлен *флагом революции*, в 2012 г. принят *Национальной коалицией сирийских революционных и оппозиционных сил* в качестве нового флага страны.

4 Под *умеренной, или светской* вооруженной оппозицией понимаются прежде всего отряды или бригады, воюющие под флагом *Свободной сирийской армии* (ССА). Группировка была сформирована в Турции в июле 2011 г. из офицеров, *отколовшихся* от правительственной армии и перешедших на сторону повстанцев. Одним из таких офицеров был полковник Рияд аль-Асаад, впоследствии ставший верховным главнокомандующим ССА. В 2012 г. был сформирован Высший военный совет ССА под председательством бригадного генерала Салима Идрисса. На данный момент во главе Совета находится бригадный генерал Абд аль-Карим аль-Ахмад. Командование ССА входит в состав Сирийского национального совета и признает в качестве своего политического руководства Национальную коалицию сирийских революционных и оппозиционных сил. Однако в то же время ССА не раз критиковало политическую оппозицию и временное сирийское правительство за неэффективность в вопросах управлении и оказания финансовой помощи, отсутствие четкой политической программы и так далее. В то же время *Нацкоалиция* обвиняет некоторых генералов ССА в злоупотреблении служебным положением и в нежелании координировать свои действия с политической оппозицией. Кроме этого, Высший военный совет ССА так и не смог стать легитимной и авторитетной структурой для некоторых вооруженных отрядов, действующих на территории Сирии. Проблемы в управлении, разногласия между лидерами политической оппозиции, а также между Саудовской Аравией и Катаром привели к тому, что некоторые отряды ССА перешли на сторону других сил: *Исламского фронта*, *Джабхат ан-Нусры* и ИГ. Некоторые отряды, воюющие под флагом ССА, лишь номинально признают командование Высшего военного совета. На данный момент некоторые вооруженные группировки ассоциируют себя с ССА, ее флагом и символами прежде всего для того, чтобы подчеркнуть *светский* характер своей борьбы и непричастность к джихадистам — что дает возможность получать финансовую и военную помощь от США и ЕС. Отряды, воюющие под флагом ССА, дают понять, что они признают национальное государство, светский характер Сирии, парламент и выборы и отвергают радикальную идеологию *аль-Каиды* и ИГ. Однако реальное положение дел на фронте вынуждает отряды ССА проводить совместные военные операции с различными силами, представляющими транснациональный джихадизм, в частности с *Джабхат ан-Нусрой* (представитель *Аль-Каиды* в Сирии). Нужно отметить, что по своему военному потенциалу и техническому обеспечению ССА сильно уступает и своим союзникам, исламистским объединениям *Ахрар аш-Шам* и *Джейш аль-Ислам*. В то же время отряды, входящие в *Южный фронт* ССА на юге Сирии, намного более влиятельны и лучше оснащены, чем отряды на севере. Дело в том, что южные группы получают военную и финансовую помощь через Центр военных операций, созданный США в Аммане при содействии Турции, КСА, Франции и других стран, поддерживающих сирийскую оппозицию. Несмотря на то что аналогичный центр был создан в Турции, северные отряды ССА не смогли стать лидирующей силой — на севере Сирии им приходится считаться с наличием крупных исламистских объединений и балансировать между ними.

5 Под исламистскими фракциями понимаются прежде всего группы, входящие в *Исламский фронт* (*Аль-Джабха аль-Исламийа*) — военное объединение из 7 групп, возникшее в ноябре 2013 г. Ключевыми организациями *Фронта* являются *Армия ислама* (*Джейш аль-Ислам*) и *Исламское движение свободных людей Леванта* (*Ахрар аш-Шам*). Одна из основных причин его возникновения — угроза со стороны ИГ. В то же время *Исламский фронт* был создан в качестве политической и идеологической альтернативы как радикальным джихадистам — *Исламскому государству* и *Ан-Нусре*, так и светской ССА. Лидеры *Исламского фронта* не признают Национальную коалицию в качестве своего политического представителя, хотя и осуществляют военные операции совместно с отрядами ССА. Идеология этого объединения — сирийский салафизм. Поэтому убеждения и поведение его членов не являются для сирийцев чем-то необычным и не противоречат их традициям. В вопросах установления шариата они принимают во внимание общественное мнение и не идут против общепринятых норм и правил поведения в сирийском обществе. Благодаря такой позиции они пользуются определенной поддержкой населения тех районов, которые контролируют или на территории

которых ведут бои. В этом одно из основных различий между исламистскими фракциями и транснациональными джихадистскими группами.

6 Лидеры *Ахрар аш-Шама* участвуют в демонстрации в Аазазе. Газета *Enab baladi*, 11 марта 2016 г., http://www.enabbaladi.org/archives/68818 (последнее посещение: 14.06.2016).

7 Что происходит на демонстрациях в Идлибе?. *Orient News*, 7 мая 2016 г., http://www.orient-news.net/ar/news_show/105290/ماذا-جرى-في-مظاهرة-ادلب-اليوم (последнее посещение: 14.06.2016).

8 https://twitter.com/oabozayd/status/706849491241070592 (последнее посещение: 14.06.2016).

9 *Ахрар аш-Шам* отрицает свою причастность к разгону демонстраций в Идлибе и призывает к наказанию виновных. Информационный портал *Заман аль-Васль*, 8 марта 2016 г., https://www.zamanalwsl.net/news/69344.html (последнее посещение: 14.06.2016).

10 https://twitter.com/Ammari011/status/706873901457018880 (последнее посещение: 14.06.2016).

11 Столкновения между *Джабхат ан-Нусрой* и 13-й дивизией в Маарет ан-Нуман в Идлибе. Aranews, 12 марта 2016 г., http://aranews.org/2016/03/ اشتباكات-بين-جبهة-النصرة-والفرقة-13-في-م / (последнее посещение: 14.06.2016).

12 *Джабхат ан-Нусра* захватила позиции 13-й дивизии в Идлибе. Orient News, 13 марта 2016 г., http://www.orient-news.net/ar/news_show/105817/ جبهة-النصرة-تقتحم-مقرات-الفرقة-13-بريف-إدلب (последнее посещение: 14.06.2016).

13 Абазид Ахмад Мы ждали от *Аль-Каиды* чего-то иного? Syria Noor, 13 марта 2016 г., http://syrianoor.net/revto/16658 (последнее посещение: 14.06.2016).

14 https://twitter.com/thtt2015/status/708789469109993473 (последнее посещение: 14.06.2016).

15 https://twitter.com/13alferqa13/status/709344192275689472 (последнее посещение: 14.06.2016).

16 Люди ворвались в штабы *Джабхат ан-Нусры* и освободили пленных бойцов 13-й дивизии. Orient News, 14марта2016г.,http://www.orient-news.net/ar/news_show/105981/-معرة-النعمان-الأهالي-يقتحمون-مقراً-للنصرة ويخرجون-مقاتلين-للفرقة-13 (последнее посещение: 14.06.2016).

17 https://twitter.com/alferqa13/status/710103013126492160 (последнее посещение: 14.06.2016).

18 *Джабхат ан-Нусра* выбила Сирийский революционный фронт из Джабаль аз-Завии в Идлибе. CNN Arabic, 2 ноября 2014 г., http://arabic.cnn.com/middleeast/2014/11/02/isis-nusra-syria-update-idlib (последнее посещение: 14.06.2016).

19 *Джабхат ан-Нусра* захватывает позиции движения *Хазм* в районах Идлиба. Orient News, 1 марта 2015 г., https://www.youtube.com/watch?v=p1emmdNM_2Y (последнее посещение: 14.06.2016).

20 *Джабхат ан-Нусра* захватывает штаб движения *Хазм* в Идлибе. аль-Джазира, 28 февраля 2015 г., http://www.aljazeera.net/news/arabic/2015/2/28/ جبهة-النصرة-تسيطر-على-مقار-حركة-حزم-بريف-حلب (последнее посещение: 14.06.2016).

21 Rupar Terri. Nine questions for the Syrian rebel commander entrusted with the first U.S. missiles of the war. *The Washington Post*. 28 апреля 2014 г., https://www.washingtonpost.com/news/worldviews/wp/2014/04/28/nine-questions-for-the-syrian-rebel-commander-entrusted-with-the-first-u-s-missiles-of-the-war/(последнее посещение: 14.06.2016).

22 White Jeffrey. Rebels Worth Supporting: Syria's Harakat Hazm. Washington Institute, 28 апреля 2014 г., http://www.washingtoninstitute.org/policy-analysis/view/rebels-worth-supporting-syrias-harakat-hazm (последнее посещение: 14.06.2016).

23 *Ан-Нусра* атакует штабы 30-й дивизии на севере Сирии. Газета *Аль-Хайат*, 31 июля 2015 г., http://www.alhayat.com/Articles/10318742/-النصرة-تشن-هجوماً-على-مقار--الفرقة-30--شمال-سورية (последнее посещение: 14.06.2016).

24 Контрольно-пропускной пункт Насиб вызвал разногласия между *Ан-Нусрой* и США на юге Сирии. *Аль-Араби аль-Джадид*, 6 апреля 2015 г., https://www.alaraby.co.uk/politics/2015/4/5/-معبر-نصيب-يؤجج-خلافات-النصرة والجيش-الحر-جنوب-سورية (последнее посещение: 14.06.2016).

25 Али Аднан. Сирия: *Южный фронт* обеспокоен расширением *Ан-Нусры*». *Аль-Араби аль-Джадид*, 18 апреля 2015 г., https://www.alaraby.co.uk/politics/2015/4/17/-الجنوبية سورية-هاجس-تمدد-النصرة-يسيطر-على-الجبهة (последнее посещение: 14.06.2016).

26 Отряды *Южного фронта* объявили о начале холодной войны с *Джабхат ан-Нусрой* в Дараа и о прекращении с ней всех отношений. *Step agency,* 13 апреля 2015 г., http://stepagency-sy.net/archives/40599 (последнее посещение: 14.06.2016).

27 См. https://twitter.com/13alferqa13; https://www.facebook.com/alfrka13/?fref=ts

28 Beck John. Syria rebel recounts his time in an ISIL jail, Aljazeera. 10 марта 2014 г., http://www.aljazeera.com/indepth/features/2014/03/syria-rebel-recounts-his-time-an-isil-jail-20143911113109123.html (последнее посещение: 14.06.2016).

29 https://twitter.com/GebeilyM/status/708976603435560961 (последнее посещение: 14.06.2016).

30 https://twitter.com/13alferqa13/status/709474325489917952 (последнее посещение: 14.06.2016).

31 https://twitter.com/ahl_al3lm/status/709823118274138112 (последнее посещение: 14.06.2016).

32 https://twitter.com/13alferqa13/status/711339066982326277 (последнее посещение: 14.06.2016).

33 http://baladi-news.com/ar/news/details/4377/%D8%A7%D8%AA%D9%81%D8%A7%D9%82_%D8%A8%D9%8A%D9%86_%D8%A7%D9%84%D9%86%D8%B5%D8%B1%D8%A9_%D9%88%D8%A7%D9%84%D9%81%D8%B1%D9%82%D8%A9_13_%D9%88%D8%A7%D9%84%D8%A3%D8%AE%D9%8A%D8%B1%D8%A9_%D8%AA%D8%B7%D8%A7%D9%84%D8%A8_%D8%A8%D8%AA%D9%88%D8%B6%D9%8A%D8%AD%D8%A7%D8%AA

34 Аль-Хасан Умар. Между *Ан-Нусрой* и *13-й дивизией* было заключено соглашение — последняя требует объяснений». Baladi News, 22 марта 2016 г., http://baladi-news.com/ar/news/details/4377/اتفاق_بين_النصرة_والفرقة_13_والأخيرة_تطالب_بتوضيحات (последнее посещение: 14.06.2016).

35 Шухада Амир, 13-я дивизия осуждает молчание *братьев по оружию*, а Аль-Мухайсини выражает свою позицию». Orient News, 13 марта 2016 г., https://twitter.com/13alferqa13/status/713468748531908613 (последнее посещение: 14.06.2016).

36 http://orient-news.net/ar/news_show/105879/0/الفرقة-تعاتب-صمت-رفاق-السلاح-والمحيسني-يبدي-موقفه (последнее посещение: 14.06.2016).

37 Аль-Хасан Бараа, Шариатский комитет отказывается выносить решение по поводу конфликта между Ан-Нусрой и 13-й дивизией и объясняет причины. Ana Press, 27 марта 2016 г., http://www.anapress.net/ar/articles/186336467480944/-اللجنة-الشرعية-تعتذر-عن-الحكم-بين-النصرة-و-الفرقة-13-وتبين-الأسباب تقارير/ (последнее посещение: 14.06.2016).

38 Гасымов Кямал. Джихад без особых причин. Против кого воюет *Джабхат ан-Нусра* — ячейка *Аль-Каиды* в Сирии. Lenta.ru, 27 октября 2015 г., https://lenta.ru/articles/2015/10/27/evilones/(последнее посещение: 14.06.2016).

39 Собрание записей шейха Аль-Мухайсини в *Твиттере* о правовом статусе *флага революции*, 4 апреля 2015 г., https://justpaste.it/kc44 (последнее посещение: 14.06.2016).

40 https://twitter.com/MousaAlomar/status/708270405610561537 (последнее посещение: 14.06.2016).

41 Собрание записей шейха Аль-Мухайсини в *Твиттере* о правовом статусе *флага революции*, 4 апреля 2015 г., https://justpaste.it/kc44 (последнее посещение: 14.06.2016).

42 К слову, неприятие любых символов, связанных с национальным государством, и конфликт с политическими группами, которые эти символы воспринимают и защищают, — характерные черты всех движений, идеологически связанных с салафитским джихадизмом. Достаточно вспомнить дискуссии между салафитами и национально-ориентированными силами в Чечне о гербе с изображением волка, происходившие в начале 1990-х гг.

43 Абу Мухаммад аль-Джулани. *Ан-Нусра* и будущее Сирии. Аль-Джазира, 19 декабря 2013 г., https://www.youtube.com/watch?v=DIr1HoHJIQA (последнее посещение: 14.06.2016).

44 Гасымов Кямал. Разлад в стане джихадистов: идеологическая борьба *Аль-Каиды* с организацией *Исламское государство*. *Индекс Безопасности*. 2015. № 3 (114). С. 61–82.

45 Влиятельный лидер *Джабхат ан-Нусры* отказывает *Нацкоалиции* во въезде в Идлиб. Газета *аль-Кудс аль-Араби*, 31 марта 2015 г., http://www.alquds.co.uk/?p=318978 (последнее посещение: 14.06.2016).

46 *Ан-Нусра* провозглашает собственный эмират вслед за ИГИЛ. Аль-Арабийя, 12 июля 2014 г., http://www.alarabiya.net/ar/arab-and-world/syria/2014/07/12/الجولاني-يعد-مقاتلي-جبهة-النصرة-بإقامة-إمارة-اسلامية.html (последнее посещение: 14.06.2016).

47 Абу Мария аль-Кахтани: если бы не демонстрации, мы бы не смогли взяться за оружие в Шаме, http://all4syria.info/Archive/300511 (последнее посещение: 14.06.2016).

48 См.: Гасымов Кямал. Разлад в стане джихадистов: идеологическая борьба *Аль-Каиды* с организацией *Исламское государство*. *Индекс Безопасности*. 2015. № 3 (114). С. 61–82.

49 https://twitter.com/abazeid89/status/709401665363910657 (последнее посещение: 14.06.2016).

50 Хузайфа Аззам обвиняет Аль-Джулани в убийстве и во лжи и призывает его ответить на критику. Араби 21, 21 марта 2016 г., http://arabi21.com/story/896280/حذيفة-عزام-يتهم-الجولاني-بالقتل-والكذب-ويدعوه-للمباهلة (последнее посещение: 14.06.2016).

51 Аззам: Ан-Нусра получила оружие от Высшего военного совета несмотря на его *неверие*. Араби 21, 17 марта 2016 г., http://arabi21.com/story/895383/عزام-النصرة-حصلت-على-السلاح-من-الأركان-رغم-كفرها (последнее посещение: 14.06.2016).

52 Речь Абу Мухаммада аль-Джулани на смерть шейха Абу Халида ас-Сури, 24 февраля 2014 г., https://www.youtube.com/watch?v=vgJpyMCQJ8U (последнее посещение: 14.06.2016).

53 Свидетельство Хузайфа Аззама о событиях, связанных с *Джабхат ан-Нусрой*. Syria Noor, 17 марта 2016 г., http://www.syrianoor.net/revmarsad/16722 (последнее посещение: 14.06.2016).

54 https://twitter.com/Ammari011/status/711660310143356928 (последнее посещение: 14.06.2016).

55 Ас-Сури Абу Фирас. Я нагой увещеватель — спасайтесь же, спасайтесь! https://justpaste.it/abofiras1 (последнее посещение: 14.06.2016).

56 Al Nahhas Labib. The deadly consequences of mislabeling Syria's revolutionaries. *The Washington Post*. 10 июля 2015 г., https://www.washingtonpost.com/opinions/the-deadly-consequences-of-mislabeling-syrias-revolutionaries/2015/07/10/6dec139e-266e-11e5-aae2-6c4f59b050aa_story.html (последнее посещение: 14.06.2016).

57 Сирийские отряды подписывают Революционную хартию чести, Aljazeera, 17 мая, 2014, http://www.aljazeera.net/news/arabic/2014/5/17/فصائل-سورية-مقاتلة-توقع-ميثاق-شرف-ثوريا (последнее посещение: 14.06.2016)

58 Интервью с Лабибом ан-Наххасом. газета *аль-Ахд*, 22 марта 2016 г., С. 4–5, http://al3ahdnewspaper.com/wp-content/uploads/2016/03/al3ahd58.pdf (последнее посещение: 14.06.2016)

59 Ahrar al-Sham signs Syria statement, opposition to meet government. Reuters, 10 декабря 2015 г, http://www.reuters.com/article/us-mideast-crisis-syria-conference-state-idUSKBN0TT2VA20151210 (последнее посещение: 14.06.2016).

60 *Ахрар аш-Шам* приняла участие в конференции, прошедшей 10 декабря в Эр-Рияде, однако позже покинула переговоры по причине того, что к мнению *исламских фракций* недостаточно прислушались, а также из-за того, что на конференции присутствовали политики, которых движение рассматривает как пособников Б. Асада. В итоге представители *Ахрар аш-Шама* все-таки подписали итоговый документ конференции о создании *Высшего переговорного комитета* для участия в переговорном процессе в Женеве.

61 Al-Nahhas Labib. I'm a Syrian and I fight Isil every day. It will take more than bombs from the West to defeat this menace. *The Telegraph*, 21 июля 2015 г., http://www.telegraph.co.uk/news/worldnews/islamic-state/11752714/Im-a-Syrian-and-I-fight-Isil-every-day.-We-need-more-than-bombs-from-the-West-to-win-this-battle.html (последнее посещение: 14.06.2016).

62 Интервью с Лабибом ан-Наххасом. Газета *аль-Ахд*, 22 марта 2016 г., С. 4–5, http://al3ahdnewspaper.com/wp-content/uploads/2016/03/al3ahd58.pdf (последнее посещение: 14.06.2016).

63 Ходжа призывает *Ан-Нусру* разорвать связи с *аль-Каидой*. Аль-Иттихад Пресс, 23 ноября 2015 г., http://aletihadpress.com/2015/11/23/خوجة-يدعو-النصرة-إلى-الانفصال-عن-القاع/(последнее посещение: 14.06.2016).

64 *Ахрар аш-Шам* призывает *Ан-Нусру* разорвать связь с *Аль-Каидой*. Orient News, 1 февраля 2016 г., http://orient-news.net/ar/news_show/101557/0/أحرار-الشام-تدعو-جبهة-النصرة-لفك-ارتباطها-بالقاعدة (последнее посещение: 14.06.2016).

Ольга Михайлова

КИБЕРУГРОЗЫ И ФИЗИЧЕСКАЯ ЯДЕРНАЯ БЕЗОПАСНОСТЬ

Растущая автоматизация производственных процессов и применение цифровых технологий при эксплуатации ядерных установок и обращении с радиоактивными материалами увеличивают риск нападения на автоматизированные системы (АС) с использованием программно-технических средств и телекоммуникационных сетей. Иначе говоря, создают риск кибератак.

Обеспечение кибербезопасности — проблема, актуальная для всех объектов критической инфраструктуры, в которых используются АС. Несмотря на то, что общие принципы и подходы к защите различных отраслей несомненно существуют, необходимо учитывать специфику и потенциальные последствия кибератак для каждой из них.

Применительно к ядерной отрасли это могут быть: сложившаяся практика регулирования деятельности ядерных объектов; технические особенности их функционирования, включая необходимость непрерывного осуществления технологических процессов в течение долгого времени; исторически сложившаяся обособленность и закрытость ядерной отрасли; недостаточная осведомленность работников ядерных объектов о киберугрозах и их потенциальных последствиях для безопасности радиоактивных материалов и ядерных установок, а также ложное чувство защищенности ядерных объектов от киберугроз.

Чтобы оценить масштаб проблемы надо иметь в виду, что АС используются для управления реакторами и установками по обогащению урана, сбора и анализа данных о параметрах ядерного объекта, управления транспортно-техническими операциями с ядерными материалами и изделиями из них (например, перегрузкой топлива в активной зоне реактора) и т. п. Кроме того, на ядерных объектах[1] автоматизированными являются системы физической защиты ядерных объектов, учета и контроля ядерных материалов, различные системы документооборота и бухгалтерского учета.

Чтобы разобраться в этом подробнее, зададимся вопросом: что, если в результате кибератаки автоматизированные системы ядерного объекта прекратят выполнять свои функции или будут выполнять их с измененными параметрами, *забыв* сообщить об этом операторам?

Теоретически неожиданное *своенравие* систем, обеспечивающих управление ядерной установкой, процессами обращения с ядерными материалами, а также элемен-

тами безопасности, призванными не допустить аварии, может привести к инциденту, последствия которого могут быть сравнимы с чернобыльской катастрофой.

Не менее пугающими выглядят сценарии отказа или ненадлежащего функционирования системы физической защиты ядерного объекта либо автоматизированной системы учета и контроля ядерных материалов вследствие кибератаки, равно как и хищение данных, с помощью которых злоумышленники могли бы найти способ обойти меры безопасности и похитить ядерные материалы с целью последующего создания ядерного взрывного устройства или *грязной* бомбы. Физическое воздействие на элементы ядерной установки, доступ к которым был получен при помощи кибератаки, может привести к радиационному загрязнению окружающей среды и облучению населения.

Помимо вышеупомянутых рисков, применение АС на ядерных объектах может создавать и другие, менее катастрофические риски, как-то: убытки в результате нарушения бизнес-процессов ядерного объекта, репутационные потери в результате хищения информации о функционировании объекта или разрушения имиджа объекта как надежно защищенного от злоумышленных воздействий.

В зависимости от того, какую цель преследуют злоумышленники (спровоцировать аварию, завладеть радиоактивными материалами или получить доступ к информации), кибератаки могут быть направлены на доступ, уничтожение, модифицирование, блокирование или копирование информации в соответствующих автоматизированных системах ядерного объекта.

В рамках данной статьи мы ограничимся рассмотрением кибератак с целью спровоцировать аварию с неприемлемыми радиационными последствиями или похитить ядерные материалы. Иначе говоря, будем обсуждать угрозы физической ядерной безопасности (ФЯБ).

КИБЕРУГРОЗЫ В КОНТЕКСТЕ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

Обеспечение ФЯБ на ядерных объектах заключается в предотвращении, обнаружении и пресечении хищений ядерных материалов; диверсий (саботажа) в отношении ядерных материалов или ядерных установок, создающих угрозу здоровью или жизни людей в результате воздействия радиации или приводящих к радиоактивному загрязнению окружающей среды; незаконной передачи или других злоумышленных действий в отношении ядерных материалов и установок[2].

Для этого на ядерных объектах проектируются и создаются системы ФЯБ, включающие оборудование, персонал и регламенты. Исходными данными для проектирования таких систем являются результаты анализа уязвимости ядерных объектов: составление перечня предметов, которые необходимо защитить, а также описания возможных сценариев осуществления угроз.

К предметам защиты относят элементы ядерных установок, несанкционированные действия в отношении которых могут привести к аварийной ситуации, облучению людей или радиоактивному загрязнению окружающей среды, например, системы управления реакторной установкой, включая управление цепной реакцией деления.

Список элементов установки, подлежащих защите, составляется для каждого ядерного объекта с учетом результатов вероятностного анализа безопасности,

потенциального масштаба облучения и радиоактивного загрязнения, характеристик ядерного объекта, особенностей ядерной установки и технологического процесса, а также других факторов.

К предметам защиты систем ФЯБ также относятся ядерные материалы, имеющиеся на объекте. Для определения приоритетов при проектировании систем ФЯБ ядерные материалы категорируют по степени привлекательности с точки зрения хищения, а элементы ядерных установок — исходя из масштабов последствий, которые может вызвать направленная против них диверсия. Чем привлекательнее ядерный материал или масштабнее последствия, тем более интенсивными должны быть меры ФЯБ.

Разработчикам систем ФЯБ важно правильно оценивать *проектные угрозы*, то есть понимать, кто и каким образом может попытаться совершить противоправные действия в отношении предметов защиты. Возможные злоумышленники разнятся от фанатиков-одиночек, смутно представляющих себе принципы функционирования ядерного объекта, до хорошо вооруженных преступных групп, обладающих знаниями и технологиями, необходимыми для управления ядерной установкой, имеющих возможность удаленного доступа к управлению системами объекта и действующих в сговоре с персоналом ядерного объекта.

Чтобы выявить реальные угрозы и сценарии их осуществления для каждого конкретного объекта необходимо провести тщательный анализ криминогенной и социальной обстановки, угроз безопасности, признанных на уровне государства и отрасли, степени риска для имеющихся радиоактивных материалов, потенциальных последствий аварий и возможных путей воздействия на элементы ядерной установки с целью вызвать ядерный инцидент.

Кибератаки могут осуществляться удаленно, либо с территории ядерного объекта. Во втором случае злоумышленнику необходимо получить физический доступ к элементам ядерной установки или обеспечить подключение носителя с вредоносным программным обеспечением к элементам установки. Проще всего сделать это при содействии персонала ядерного объекта или подрядных организаций.

Сценарии осуществления угроз могут включать кибератаки следующих типов:

- Кибератаки на автоматизированные системы управления технологическими процессами (АСУ ТП) ядерной установки. Они могут быть направлены на изменение или блокирование управляющих команд, блокирование доступа операторов к информации о состоянии ядерного объекта или искажение такой информации, а также на перепрограммирование промышленных контроллеров. Целью кибератаки может быть инициирование аварии или создание условий для возникновения аварийной ситуации. В результате возможно радиационное заражение местности и/или облучение персонала и населения.
- Кибератаки на автоматизированные системы ФЯБ, включая систему физической защиты и систему учета и контроля ядерных материалов. В данном случае целью кибератаки может быть нарушение функционирования систем физической защиты и/или учета и контроля с целью подготовки хищения радиоактивных материалов или совершения диверсий, в том числе удаленное отключение средств контроля и управления доступом в помещениях с предметами защиты

или изменение настроек измерительных систем, применяемых для учета и контроля ядерных материалов.

- Кибератаки на автоматизированные информационные системы ядерного объекта. Доступ, уничтожение или фальсификация данных дает злоумышленникам возможность осуществить хищение или диверсию, преодолеть меры ФЯБ и т. п. В результате атаки могут быть изменены данные об инвентарных количествах ядерных материалов с целью сокрытия факта их хищения в течение как можно большего срока. Другой пример — несанкционированный доступ к системе документооборота ядерного объекта, где могут находиться сведения о графике проведения технического обслуживания элементов системы физической защиты, транспортирования ядерных материалов или порядке действий персонала по обнаружению и пресечению несанкционированных действий.

Кибератаки на системы ядерного объекта, которые не могут привести к хищению ядерных материалов или диверсии, в контексте ФЯБ не рассматриваются.

Для оценки возможных последствий кибератак с точки зрения ФЯБ рассмотрим несколько сценариев, основанных на данных об имевших место киберинцидентах.

В качестве первого примера возьмем кибератаку в отношении обогатительной установки в иранском городе Натанз. Как известно, для нападения использовался вирус Stuxnet[3], перепрограммировавший промышленные контроллеры таким образом, что они отдавали установке *несовместимые с жизнью* управляющие команды, игнорируя данные датчиков, которые в нормальных условиях должны были привести к выдаче команды на перевод установки в безопасный режим. Пострадавший объект считался защищенным от вирусов в связи с отсутствием физического подключения к интернету, однако вредоносная программа была занесена в его систему управления с внешнего носителя.

Теперь представим, что системы безопасности АЭС, призванные локализовать и/или предотвратить аварию, построены на основе программируемых контроллеров[4], а каналы защиты с жесткой логикой не предусмотрены или выведены из строя. Атака вируса, действующего подобно Stuxnet, может перепрограммировать контроллеры систем безопасности таким образом, что при достижении определенных параметров (например, давления, температуры или реактивности), они не сработают, но сообщат оператору о срабатывании. Другими словами, произойдет отказ систем безопасности, который не будет вовремя обнаружен персоналом. При бездействующих системах безопасности авария, спровоцированная действиями злоумышленников или случайным стечением обстоятельств, может принять катастрофические масштабы[5].

Другим примером может стать получение удаленного доступа к автоматизированной системе с помощью программного обеспечения для создания VPN, применяемого поставщиком оборудования системы физической защиты, IP-адресов оборудования системы физической защиты, имени пользователя и пароля, используемых по умолчанию. Эта информация может быть получена различными способами, включая кибератаки на поставщиков оборудования, подкуп, обман или шантаж персонала. Путем удаленного управления элементами системы физической защиты злоумышленники могут обеспечить себе беспрепятственный проход в охраняемые зоны объекта и выход из них, одновременно заблокировав проход для персонала. Изображение с камер видеонаблюдения может быть *зациклено* таким образом,

чтобы демонстрировать оператору отснятую ранее картинку пустого помещения в то время, как в нем находятся злоумышленники. В результате преступники смогут совершить задуманное, например, похитить ядерные материалы или осуществить диверсию и беспрепятственно покинуть объект[6].

Весьма эффективный способ скомпрометировать корпоративную сеть — рассылка во внутренней сети предприятия фишинговых сообщений, через которые может быть загружен вирус, способный выкрасть чертежи и схемы ядерной установки[7]. Полученная информация может затем быть использована преступниками для выявления наиболее эффективных способов диверсии или хищения радиоактивных материалов.

При этом важно понимать, что вышеописанные сценарии могут иметь комбинированный характер. Злоумышленники могут совершать кибератаки не только с непосредственно диверсионными целями, но и для подготовки диверсий или усиления их негативных последствий.

ЗАЩИТА ОТ КИБЕРУГРОЗ, ЗНАЧИМЫХ С ТОЧКИ ЗРЕНИЯ ФЯБ: ПОДХОДЫ И ПЕРСПЕКТИВЫ

Необходимость осмысления проблемы кибербезопасности в контексте ядерной отрасли в целом и физической ядерной безопасности в частности в настоящее время признана на международном уровне. Происходит активное обсуждение и выработка подходов к ее решению при непосредственном участии и поддержке МАГАТЭ. Ярким примером такой деятельности является проведенная МАГАТЭ в июне 2015 г. международная конференция, посвященная компьютерной безопасности в ядерной отрасли, *Компьютерная безопасность в ядерном мире: дискуссия экспертов и обмен мнениями.*

В рамках конференции широко обсуждались вопросы безопасности информации в автоматизированных информационных системах, системах управления технологическими процессами, а также физической защиты, применяемых в ядерной отрасли. Помимо прочего, были охвачены все вышеописанные киберугрозы, значимые для ФЯБ, а также отмечена необходимость разработки указаний и рекомендаций по вопросам кибербезопасности с учетом особенностей ядерной отрасли. В материалах конференции МАГАТЭ[8,9] отмечены три направления обеспечения кибербезопасности, которым необходимо уделить внимание как важной составляющей обеспечения безопасности ядерных объектов и других организаций ядерной отрасли:

- кибербезопасность автоматизированных систем управления технологическими процессами ядерных объектов;
- кибербезопасность автоматизированных информационных систем;
- кибербезопасность систем физической защиты ядерных объектов.

В настоящее время существует ряд исследований и публикаций по каждому из трех направлений, содержащих описание соответствующих киберугроз, подходов к их выявлению и подходов к выявлению уязвимостей автоматизированных систем, которые могут быть использованы для реализации угроз. Также публикации описывают уже предпринятые усилия для создания методической, нормативной и технической базы в области защиты от киберугроз, значимых с точки зрения

ФЯБ, а также приводят рекомендации по дальнейшим усилиям, которые необходимо предпринять.

Говоря о кибербезопасности автоматизированных систем ядерных объектов хотелось бы отметить исследования, посвященные состоянию и перспективным направлениям работ по этому вопросу, проведенные Chatham House (Британским Королевским институтом международных отношений), а также работы фонда *Инициатива по снижению ядерной угрозы* и Университета прикладных наук Бранденбурга[10,11,12].

Первое исследование в основном посвящено кибербезопасности автоматизированных систем управления ядерными установками, другие касаются мер по обеспечению кибербезопасности в контексте ФЯБ. Публикации по результатам данных исследований содержат общее описание киберугроз, которые необходимо учитывать, а также описывают инструменты и подходы, используемые для обеспечения защиты от них в различных станах (в том числе — Соединенных Штатах Америки и Российской Федерации). В работах также представлены рекомендации по созданию, совершенствованию и развитию указанных подходов и инструментов.

В числе прочего, в упомянутых публикациях обозначена проблема недостаточной осведомленности о киберугрозах и возможных мерах защиты от них как на уровне ядерной отрасли в целом, так и на уровне специалистов, эксплуатирующих и проектирующих автоматизированные системы. В связи с этим рекомендовано наращивать обмен информацией о киберугрозах АСУ ТП и практиках защиты от них как внутри ядерной отрасли, так и со специалистами других отраслей, в которых эксплуатируются потенциально опасные объекты, например, химической промышленности или гидроэнергетики, имеющими опыт разработки и применения мер по защите от киберугроз.

Примеры использования ядерной отраслью опыта других отраслей в обеспечении кибербезопасности АСУ ТП описаны в материалах ежегодных конференций Института управления ядерными материалами[13,14].

В качестве одной из проблем, которую необходимо решить для создания эффективных мер обеспечения кибербезопасности, обозначено отсутствие продолжительной практики внедрения таких мер в проектируемые АСУ ТП, неспособность профессионалов в области киберпространства и специалистов, проектирующих и эксплуатирующих ядерные установки, найти общий язык и эффективно сотрудничать, а также отсутствие практики такого сотрудничества на постоянной основе.

В качестве пути решения проблемы предлагается разработка обучающих программ, которые дали бы специалистам по кибербезопасности представление об особенностях проектирования и функционирования автоматизированных систем управления ядерного объекта, а также систем ФЯБ, а проектировщикам и эксплуатирующему персоналу атомной установки — представление о мерах обеспечения кибербезопасности и порядке их разработки. Это должно привести к отсутствию конфликтов мер ФЯБ и кибербезопасности, включая меры по реагированию на несанкционированные действия, меры по обслуживанию систем и т. п.

Кроме того, рекомендована разработка методик и инструментов, направленных на объединение процессов анализа уязвимости в обеих сферах обеспечения безопасности ядерных объектов. Результатом объединения процессов должно стать выявление программно-технических средств и сетей обмена данными; информации, к которой необходимо применять меры кибербезопасности во избе-

жание реализации угроз ФЯБ, а также оборудования и сетей, физический доступ к которым необходим для совершения кибератаки, с последующим включением их в перечень предметов защиты систем ФЯБ.

Подробнее об этих процессах можно узнать из материалов ежегодных конференций Института управления ядерными материалами[15,16,17,18,19]. В публикациях, ссылки на которые даны в этой части статьи, представлены конкретные технические и организационные меры, которые следует предпринять ядерным объектам для снижения рисков, связанных с применением автоматизированных систем.

СОСТОЯНИЕ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ

В настоящее время вопросам кибербезопасности в обеспечении ФЯБ уделяется внимание как в рекомендациях МАГАТЭ, так и в документах профильных национальных ведомств. Подходы к регулированию этого вопроса могут быть различны. Их сравнительный анализ можно найти в отчетах фонда *Инициатива по снижению ядерной угрозы* и Университета прикладных наук Бранденбурга[20], упомянутых выше. Существующие подходы можно условно разделить на два типа.

В первом случае кибербезопасность на ядерных объектах обеспечивается в соответствии с требованиями законов и подзаконных актов в области защиты критической инфраструктуры, а также государственной тайны и другой конфиденциальной информации. При этом ядерное законодательство и документы ядерного регулятора (органа, осуществляющего регулирование безопасности при использовании атомной энергии: лицензирование, установление требований к обеспечению безопасности, надзор за их соблюдением) содержат отдельные общие требования необходимости обеспечения кибербезопасности. Ядерные регуляторы в этом случае не занимаются данной проблемой, а документы в этой области, которыми руководствуются ядерные объекты, в большинстве своем не учитывают специфику отрасли, за исключением методических документов, издаваемых органами управления использованием атомной энергии (например, Росатом, Минпромторг, и.т.д.) для подведомственных объектов. Именно этот подход принят в Российской Федерации.

Во втором случае вопросы кибербезопасности регламентируются документами, издаваемыми уполномоченным органом в области регулирования безопасности ядерных установок. Такие документы учитывают специфику ядерной отрасли, а ядерный регулятор занимается в том числе и проблемами кибербезопасности атомных установок (в той мере, в которой это связано с обеспечением ФЯБ). Такой подход принят, например, в Соединенных Штатах Америки. Подробнее о деятельности Комиссии по ядерному регулированию США в этой сфере можно ознакомиться в материалах ежегодных конференций Института управления ядерными материалами[21,22]. Далее мы несколько подробнее рассмотрим рекомендации МАГАТЭ и требования, имеющиеся в российских документах.

РЕКОМЕНДАЦИИ МАГАТЭ

Документы, входящие в серию изданий МАГАТЭ по вопросам ФЯБ, содержат рекомендации по обеспечению кибербезопасности, начиная с базовых и заканчивая конкретными указаниями по разработке и внедрению соответствующих мер на ядерных объектах. Базовые рекомендации даны в основополагающем докумен-

те серии № 20 *Цель и основные элементы государственного режима ФЯБ*. Согласно его тексту, чувствительная информация (информация, несанкционированные действия в отношении которой могут поставить под угрозу физическую ядерную безопасность), а также средства, используемые для взаимодействия с ней, являются потенциальными целями злоумышленников (нарушителей) и должны быть защищены в рамках деятельности по обеспечению ФЯБ. Кибербезопасность в этом случае только подразумевается. Также в документе прямо указано на необходимость проведения регулярного анализа факторов, негативно влияющих на способность обеспечивать физическую ядерную безопасность, включая киберугрозы.

Рекомендации МАГАТЭ № 13 *Рекомендации по ФЯБ, касающиеся физической защиты ядерных материалов и ядерных установок (INFCIRC/225/Rev. 5)*[23], описывающие конкретные меры физической защиты, которые должны быть предприняты для выполнения основополагающего документа, конкретизируют рекомендации к мерам по обеспечению кибербезопасности автоматизированных систем, также необходимым для обеспечения ФЯБ. Согласно документу, «компьютеризированные системы, используемые для обеспечения физической защиты, ядерной безопасности, а также учета и контроля ядерных материалов, следует защищать от компрометации (например, кибератак, манипуляции или фальсификации) в соответствии с оценкой угроз или проектной угрозой» (см. пп. 4.10 и 5.19). Рекомендации INFCIRC/225 рассматриваются ядерными регуляторами и ядерными объектами как описание минимально необходимых на объекте мер физической защиты. В некоторых случаях данным рекомендациям придается обязательный характер путем включения требований об обеспечении физической защиты на уровне не ниже рекомендуемого INFCIRC/225, в международные договоры, связанные с транспортированием радиоактивных материалов или с развитием ядерной энергетики. Таким образов включение пп. 4.10 и 5.19 в этот документ способствует тому, что киберугрозы, значимые с точки зрения обеспечения ФЯБ, будут учтены при проектировании систем ФЯБ большинства ядерных объектов.

INFCIRC/225 рекомендует обеспечивать кибербезопасность исходя из вызовов, предусмотренных проектной угрозой. Практическое руководство № 10 *Разработка, применение и актуализация проектной угрозы* предусматривает необходимость учета возможностей потенциальных нарушителей по использованию уязвимостей автоматизированных систем ядерного объекта для непосредственной поддержки физической атаки на нем, сбора данных при подготовке к физической атаке и других целей.

Еще одно практическое руководство в этой серии — № 23-G *Безопасность информации в области ядерной энергетики* — содержит рекомендации МАГАТЭ по выявлению информации, чувствительной с точки зрения ФЯБ, и обеспечению защиты такой информации — в первую очередь с точки зрения обеспечения конфиденциальности. Документ касается общих мер по защите информации без привязки к киберугрозам.

Наиболее детальные рекомендации по обеспечению кибербезопасности в контексте обеспечения ФЯБ даны в справочном руководстве № 17 *Компьютерная безопасность на ядерных установках*. В документе приведены рекомендации, предназначенные для органов, осуществляющих регулирование в ядерной сфере и области кибербезопасности. Они включают в себя замечания о необходимости учета специфики ядерных объектов при определении требований к кибербезопасности, для чего регуляторы должны взаимодействовать друг с другом при анализе и согла-

совании имеющихся требований законодательства и нормативных документов как в области ФЯБ, так и в области кибербезопасности. В документе содержатся подробные рекомендации по учету возможностей потенциальных злоумышленников при формировании проектной угрозы, а также при разработке сценариев диверсий или хищений в ходе подготовки к проектированию систем ФЯБ. Даны рекомендации по выявлению на ядерных объектах конкретных программных и технических средств и телекоммуникационных сетей, которые необходимо защитить от киберугроз, а также рекомендации по дифференциации мер защиты от кибератак в зависимости от их возможного влияния на обеспечение ФЯБ. Помимо этого, приведены рекомендации по созданию программы обеспечения кибербезопасности на ядерном объекте, которую необходимо согласовать с мерами по обеспечению ФЯБ.

В настоящее время ожидается пополнение серии изданий МАГАТЭ публикациями в области кибербезопасности (практические руководства, технические руководящие материалы и документы серии TECDOC), которые должны оказать государствам и ядерным объектам практическую помощь в разработке мер по обеспечению ФЯБ[24].

РОССИЙСКАЯ НОРМАТИВНО-ПРАВОВАЯ БАЗА

Практика регулирования кибербезопасности в контексте обеспечения ФЯБ, сложившаяся в РФ, отличается от рекомендаций МАГАТЭ. Обеспечение физической ядерной безопасности регламентируется в основном документами, касающимися физической защиты, а также учета и контроля ядерных материалов, издаваемых правительством и ядерным регулятором — Ростехнадзором. Эти документы требуют обеспечивать защиту информации в системах учета и контроля и физической защиты, но не определяют конкретные меры защиты информации, а содержат общие ссылки на нормативные правовые акты в области защиты информации. Например, указывается, что защита информации должна быть обеспечена в соответствии с законодательством Российской Федерации.

Документов правительства и Ростехнадзора, применимых ко всем ядерным объектам и дающих детальные указания по обеспечению кибербезопасности в контексте ФЯБ, не существует. Обеспечение безопасности автоматизированных систем управления ядерными установками и процессами обращения с ядерными материалами, а также автоматизированных информационных систем не относится к задачам обеспечения физической защиты или учета и контроля и, соответственно, не регулируется российскими нормативными правовыми документами в области ФЯБ. Соответствующие требования установлены законодательством в области защиты государственной тайны, защиты информации, не составляющей государственную тайну, безопасности критической информационной инфраструктуры Российской Федерации, а также методическими и нормативными документами ведомств, имеющих регуляторные полномочия в этих областях — Федеральной службы безопасности и Федеральной службы по техническому и экспортному контролю.

В настоящее время кибербезопасность АСУ ТП ядерных установок и обращения с ядерными материалами обеспечивается в соответствии с применимыми во всех отраслях документами, устанавливающими требования и конкретные меры по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации. Эти документы еще не образуют четкую структуру, а являются скорее набором разрозненных актов, объединенных общей тематикой. К ним относятся:

- *Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации,* утвержденные президентом Российской Федерации 3 февраля 2012 г.; указ президента Российской Федерации от 15.01.2013 № 31 С *О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации*, *Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации* утвержденная президентом 12 декабря 2014 г. Эти документы определяют базовые термины и требования в отношении защиты критической информационной инфраструктуры, а также основные факторы, влияющие на состояние защищенности объектов.
- Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. *Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды*. Документ является обязательным для критически важных объектов, включая ядерные.
- Методические документы Федеральной службы по техническому и экспортному контролю, касающиеся защиты информации в ключевых системах информационной инфраструктуры:
  - Информационное сообщение Федеральной службы по техническому и экспортному контролю России от 25 июля 2014 г. по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа Федеральной службы по техническому и экспортному контролю России от 14 марта 2014 г.
  - *Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры*, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю России 18 мая 2007 г.
  - *Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры*.
  - *Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры*.
  - *Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры* от 19 ноября 2007 г.

Конкретные рекомендации по защите информации в автоматизированных системах, а также по аттестации таких систем, применимые в том числе к системам учета и контроля, а также физической защиты, определены в методических документах Федеральной службы по техническому и экспортному контролю, таких как *Специальные требования и рекомендации по технической защите конфиденциальной информации* и *Автоматизированные системы. Защита от несанкционированного*

доступа к информации. Классификация автоматизированных систем и требования о защите информации.

В соответствии с Законом о государственной тайне и Указом Президента РФ № 1203 от 30 ноября 1995 г. (ред. от 28 февраля 2016 г.) *Об утверждении Перечня сведений, отнесенных к государственной тайне,* к ней относится информация, значимая для обеспечения ФЯБ: сведения о проектировании, сооружении, эксплуатации, обеспечении безопасности объектов ядерного комплекса, о физической защите ядерных материалов, изделий на их основе, ядерных установок, пунктов хранения ядерных материалов, об охране радиационно-опасных объектов. Требования к обеспечению безопасности такой информации, в том числе кибербезопасности, включают требование о лицензировании ядерного объекта на право ведения работ с использованием указанных сведений и о применении только сертифицированных средств защиты информации в соответствующих автоматизированных информационных системах. Сертификация осуществляется в соответствии с требованиями государственных стандартов, создаваемых Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности.

Основные документы в области ФЯБ в Российской Федерации[25,26,27] устанавливают следующие требования в части обеспечения кибербезопасности:

- Система государственного учета и контроля ядерных материалов должна обеспечивать ограничительный порядок доступа к информации в целях защиты сведений, отнесенных к государственной тайне или служебной информации ограниченного распространения.
- Системы физической защиты должны включать подсистемы защиты информации, обеспечивающие в том числе секретность (конфиденциальность) информации об организации, составе и функционировании системы физической защиты, ее целостность и санкционированную доступность, нарушение которых может приводить к снижению эффективности системы физической защиты в целом или ее отдельных элементов (оборудование, соответствующее программное обеспечение, организационные и технические меры)[28].
- Технические и программные средства защиты информации, составляющей государственную и служебную тайны, подлежат обязательной сертификации на соответствие требованиям безопасности.
- На этапе ввода в действие автоматизированной системы физической защиты (до завоза ядерных материалов на объект) должна выполняться ее аттестация на предмет соответствия требованиям информационной безопасности.

Ядерные объекты также руководствуются документами федеральных органов управления использованием атомной энергии (например, Росатома и Минпромторга) и эксплуатирующих организаций (например, требования концерна *Росэнергоатом*, предназначенные для АЭС), выпущенными с целью оказания помощи подведомственным объектам в выполнении требований к обеспечению ФЯБ. Набор документов, доступных конкретному ядерному объекту, зависит от того, какому органу власти и какой эксплуатирующей организации он подчиняется. Некоторые из них накопили значительный практический опыт обеспечения кибербезопасности и согласования его с мерами ФЯБ.

В целом разработка мер кибербезопасности описанных в вышеуказанных документах, включает выявление информации, программных и технических средств, а также телекоммуникационных сетей, защиту которых необходимо обеспечить, определение перечня угроз безопасности информации и моделей нарушителей. Затем определяются требования к организационным и техническим мерам. Интенсивность мер и применимые требования определяются исходя из вида защищаемой информации и ее значимости.

ЗАКЛЮЧЕНИЕ

Рекомендации МАГАТЭ по обеспечению кибербезопасности, в контексте ФЯБ, а также рекомендации в этой области, опубликованные по результатам различных исследований, предусматривают учет киберугроз и последствий их реализации при проектировании систем ФЯБ. Также необходимо учитывать значимость с точки зрения ФЯБ информации в автоматизированных системах объекта, а также соответствующего программного обеспечения и оборудования. Кроме того, опубликованные рекомендации предполагают необходимость согласования мер ФЯБ и кибербезопасности, а также принятия ряда организационных мер на уровне государства и ядерных объектов.

В настоящее время в российских документах нет целостного универсального набора требований и рекомендаций, которыми могли бы воспользоваться специалисты для того, чтобы обеспечить всесторонний учет значимых с точки зрения ФЯБ киберугроз. Для обеспечения эффективности программ кибербезопасности и ФЯБ на всех ядерных объектах, а также распространения имеющихся лучших практик необходимы:

- дальнейшее совершенствование и структурирование национального законодательства, нормативных документов и рекомендаций в области защиты критической информационной инфраструктуры и защиты информации;
- активное участие специалистов ядерной отрасли в обсуждении проектов документов в области кибербезопасности (включая проекты документов, касающихся критической информационной структуры);
- адаптация и применение рекомендаций МАГАТЭ, связанных с обеспечением кибербезопасности в контексте ФЯБ, в том числе терминологии, к российским реалиям, включение их, например, в рекомендации Ростехнадзора и практическое применение на ядерных объектах;
- включение в документы Ростехнадзора, применимые ко всем мирным ядерным объектам, положений, предусматривающих учет сценариев реализации угроз, включающих кибератаки, при проектировании систем ФЯБ;
- анализ совокупности применимых к ядерным объектам требований в области обеспечения кибербезопасности, включая документы федеральных органов власти, которым подведомственны объекты, и оценка их достаточности и согласованности с требованиями в области ФЯБ;
- развитие и поощрение совместной работы специалистов в области кибербезопасности, ФЯБ и проектирования ядерных установок для обеспечения внедрения мер кибербезопасности на ранних стадиях проектирования систем ядерного объекта;

- дальнейшее совершенствование методов анализа уязвимостей, применяемых для целей ФЯБ и для целей кибербезопасности, а также методов оценки эффективности мер ФЯБ и мер кибербезопасности, направленное на учет сценариев, связанных с кибератаками на системы ФЯБ и системы управления ядерными установками, а также с физическим доступом злоумышленников к элементам автоматизированных систем атомных установок;
- обмен опытом между федеральными органами власти, осуществляющими управление использованием атомной энергии и координирующими вопросы безопасности на подведомственных объектах, между ядерными объектами, подведомственными различным органам управления, а также между ядерной отраслью и отраслями, в которых эксплуатируются объекты критической инфраструктуры, для взаимного обмена лучшими практиками обеспечения кибербезопасности и выполнения требований, установленных в нормативных правовых документах.

Примечания

1 Организация, на территории которой осуществляется использование ядерных материалов, размещаются и/или эксплуатируются ядерные установки

2 International Atomic Energy Agency. Division of Nuclear Security. Nuclear Security Series Glossary: Version 1.3 (November 2015). P. 18, http://www-ns.iaea.org/downloads/security/nuclear-security-series-glossary-v1-3.pdf (последнее посещение — 21 марта 2016 г.).

3 Описание кибератаки можно найти, например, в Baylon Caroline, Brunt Roger, Livingstone David. Chatham House Report. Cyber Security at Civil Nuclear Facilities: Understanding the Risks. P. 3–4. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005 CyberSecurityNuclearBaylonBruntLivingstone.pdf (последнее посещение — 21 марта 2016 г.).

4 В примере описан гипотетический случай, не учитывающий требования российских документов к проектированию систем, обеспечивающих безопасность ядерных объектов, и практику, сложившуюся в этой области.

5 Упомянутая кибератака описана, например, в Baylon Caroline, Brunt Roger, Livingstone David. Chatham House Report. Cyber Security at Civil Nuclear Facilities: Understanding the Risks. P. 3–4. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf (последнее посещение — 21 марта 2016 г.)

6 Приведенный пример описан в Anderson Robert S., Bjornard Trond, St. Michel Curtis, Schanfein Mark, Moskowitz Paul. Cyber Threats to Nuclear Infrastructures. Proceedings of 51st Annual Meeting of the Institute of Nuclear Materials Management. 11–15 July 2010

7 Упомянутая кибератака описана, например, в Baylon Caroline, Brunt Roger, Livingstone David. Chatham House Report. Cyber Security at Civil Nuclear Facilities: Understanding the Risks. P. 5. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf (последнее посещение — 21 марта 2016 г.) .

8 IAEA's Amano Calls for Strengthened Computer Security in a Nuclear World (Press Release). International Atomic Energy Agency. 1 June 2015, https://www.iaea.org/newscenter/news/iaea%E2%80%99s-amano-calls-.strengthened-computer-security-nuclear-world (последнее посещение — 21 марта 2016 г.).

9 Secure Computer Systems Essential to Nuclear Security, Conference Finds (Press Release). International Atomic Energy Agency. 8 June 2015, https://www.iaea.org/newscenter/news/secure-computer-systems-essential-nuclear-security-conference-finds (последнее посещение — 21 марта 2016 г.).

10 Cyber Security at Nuclear Facilities: National Approaches An ISS Research Project in Cooperation with the Nuclear Threat Initiative (NTI), http://www.nti.org/media/pdfs/Cyber_Security_in_Nuclear_FINAL.pdf?_=1445548675 (последнее посещение — 21 марта 2016 г.)

11 Chamales George. A New Approach to Nuclear Computer Security, http://www.nti.org/media/pdfs/A_New_Approach_to_Nuclear_Computer_Security.pdf?_=1445875704&_=1445875704 (последнее посещение — 21 марта 2016 г.)

12 Baylon Caroline, Brunt Roger, Livingstone David. Chatham House Report. Cyber Security at Civil Nuclear Facilities: Understanding the Risks. P. 3–4. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf (последнее посещение — 21 марта 2016 г.)

13 Bjornard Trond, Schanfein Mark, Moskowitz Paul, Anderson Robert. DOE/DHS Industrial Control System Cyber Security Programs: A Model For Use in Nuclear Facility Safeguards and Security. Proceedings of 52nd Annual Meeting of the Institute of Nuclear Materials Management. 17–21 July 2011.

14 Ibid.

15 Anderson Robert, Price Joseph. Cyber Informed Engineering: The Need for a New Risk Informed and Design Methodology. Proceedings of 56th Annual Meeting of the Institute of Nuclear Materials Management. 12–16 July 2015.

16 Anderson Robert S., Bjornard Trond, St. Michel Curtis, Schanfein Mark, Moskowitz Paul. Cyber Threats to Nuclear Infrastructures. Proceedings of 51st Annual Meeting of the Institute of Nuclear Materials Management. 11–15 July 2010.

17 MacDonald Doug, Key Brad, Clements Sam, Hutton William, Craig Philip, Patrick Scott, Crawford Cary. Cyber/Physical Security Vulnerability Assessment Integration. Proceedings of 52nd Annual Meeting of the Institute of Nuclear Materials Management. 17–21 July 2011.

18 Whattam Kevin, Gastelum Zoe N., Cramer Nick O., Conklin K. Examining Impacts, Challenges and Next Steps for Nuclear Nonproliferation and the Cyber Environment. Proceedings of 55th Annual Meeting of the Institute of Nuclear Materials Management. 20–24 July 2014.

19 Masica Kenneth, Porter Jeremiah, Porter Stephen J. Physical Protection Systems and the Cyber Security Component. Proceedings of 56th Annual Meeting of the Institute of Nuclear Materials Management, 12–16 July 2015.

20 Cyber Security at Nuclear Facilities: National Approaches An ISS Research Project in Cooperation with the Nuclear Threat Initiative (NTI), http://www.nti.org/media/pdfs/Cyber_Security_in_Nuclear_FINAL.pdf?_=1445548675 (последнее посещение — 21 марта 2016 г.)

21 Smith Brian W., Rivers Joseph, Harris Larry, Sapountzis Alexander, Richardson Rebecca. Development of an Approach for the Creation of a Cyber Security Program for Fuel Cycle Facilities regulated by the Nuclear Regulatory Commission. Proceedings of 54th Annual Meeting of the Institute of Nuclear Materials Management, 14–18 July 2013.

22 Rivers Joseph, Opara Stella, Lee Eric, Bergemann Brad, Felts Russell, Westreich Barry. Cyber Security Program for Facilities regulated by the U.S. Nuclear Regulatory Commission. Proceedings of 55th Annual Meeting of the Institute of Nuclear Materials Management. 20–24 July 2014.

23 Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок. Международное агентство по атомной энергии. Вена, 2012 г. http://www-pub.iaea.org/books/IAEABooks/8814/Nuclear-Security-Recommendations-on-Physical-Protection-of-Nuclear-Material-and-Nuclear-Facilities-INFCIRC-225-Revision-5 (последнее посещение — 20 мая 2016 г.)

24 Подробнее о вышедших и будущих публикациях МАТАГЭ см: Лукацкий Алексей. Кибербезопасность ядерных объектов. *Индекс Безопасности.* 2015. № 4 (115). С. 123–125, а также Gates, Guards, Guns and Geeks: The Changing Face of Nuclear Security and the IAEA's Leading Role in Promoting Computer Security for Nuclear Facilities, https://www.iaea.org/NuclearPower/Downloadable/Meetings/2015/2015-05-27-05-29-NPES/Day2/21.NSNI_CompSecurity__.pdf (последнее посещение — 21 марта 2016 г.)

25 Постановление правительства Российской Федерации № 456 от 19 июля 2007 г. (ред. от 14 марта 2014 г.) *Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов*

26 Приказ Ростехнадзора № 343 от 8 сентября 2015 г. *Об утверждении федеральных норм и правил в области использования атомной энергии «Требования к системам физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов*.

27 Постановление правительства РФ от Российской Федерации 6 мая 2008 г. № 352 (ред. от 4 февраля 2011 г.) «Об утверждении Положения о системе государственного учета и контроля ядерных материалов»

28 Постановление Ростехнадзора от 4 октября 2004 *Об утверждении и введении в действие федеральных норм и правил в области использования атомной энергии «Требования к управляющим системам, важным для безопасности атомных станций»*

Алена Махукова

ГУМАНИТАРНАЯ ИНИЦИАТИВА: КРИТИЧЕСКАЯ МАССА АНТИЯДЕРНЫХ АКТИВИСТОВ

В феврале 2016 г. в Женеве начались заседания Рабочей группы открытого состава — вспомогательного органа Генеральной Ассамблеи ООН, созванного с целью дальнейшего развития процесса многосторонних переговоров по ядерному разоружению[1]. Одной из задач группы было рассмотреть «конкретные и эффективные правовые меры, <...> которые потребуется принять для построения и сохранения мира, свободного от ядерного оружия». Одним из предложений государств-участников группы был запрет на обладание ядерным оружием, его приобретение, накопление, разработку, перемещение, размещение и развертывание[2]. Австрия, активно участвующая в Рабочей группе, в мае представила от лица 126 государств документ, озаглавленный *Правовая лакуна: рекомендации Рабочей группе открытого состава по продвижению вперед переговоров по ядерному разоружению*[3], в котором продвигалась идея ядерного разоружения как необходимого условия обеспечения гуманитарной безопасности [imperative of human security] и содержался призыв к скорейшему принятию дополнительных юридически обязывающих документов, направленных на запрещение и искоренение ядерного оружия. Группа государств, пытающихся продвинуть ядерное разоружение из соображений гуманитарной безопасности, не смогла добиться внесения подобных радикальных положений в заключительный документ Обзорной конференции Договора о нераспространении ядерного оружия (ДНЯО) 2015 г., однако смогла распространить идею о необходимости скорейшего принятия Генеральной Ассамблей ООН[4] резолюции, запрещающей ядерное оружие.

Такая впечатляющая поддержка идеи ускорения ядерного разоружения в связи с *катастрофическими гуманитарными последствиями любого применения ядерного оружия* возникла сравнительно недавно — в 2012 г., а сама идея, несмотря на кажущуюся очевидность, была озвучена лишь в 2010 г. Группа стран, поддерживающих эту инициативу, в дипломатических и академических кругах известна как Гуманитарная инициатива (Humanitarian Initiative), или *Движение за признание гуманитарных последствий применения ядерного оружия* (Humanitarian Impact Movement) и стала одним из новых объединений, активно участвующих в обзорном процессе ДНЯО. В декабре 2015 г. резолюцию ГА ООН *Гуманитарные последствия применения ядерного оружия*[5] поддержали 144 страны, а более радикальное *Гуманитарное обязательство* (Humanitarian Pledge) по состоянию на 1 мая 2016 г. поддерживали 127 государств[6].

Стремительно расширяющаяся *антиядерная коалиция*, куда могут быть отнесены страны, официально поддерживающие *Гуманитарное обязательство* или заявления о гуманитарных последствиях[7], заслуживает предметного изучения и с теоретической точки зрения как яркий пример неформальных межгосударственных объединений в рамках международного договора, и в практическом плане, поскольку является важным фактором международных отношений в сфере ядерного нераспространения и разоружения. В настоящей статье предпринята попытка дать ответ на вопросы о том, как устроена Гуманитарная инициатива и какое будущее ее ждет.

ПОЯВЛЕНИЕ ГУМАНИТАРНОЙ ИНИЦИАТИВЫ

Предпосылкой для образования Гуманитарной инициативы стал вывод, содержащийся в заключительном документе Обзорной конференции ДНЯО 2010 г., отнесенный к *принципам и целям* ядерного разоружения: «Конференция выражает глубокую озабоченность по поводу катастрофических гуманитарных последствий любого применения ядерного оружия и подтверждает необходимость того, чтобы все государства всегда соблюдали применимые нормы международного права, включая нормы международного гуманитарного права»[8]. Инициатором включения этого положения в текст документа можно считать Швейцарию: 4 мая 2010 г. на общих прениях Обзорной конференции ДНЯО глава Департамента иностранных дел Швейцарии М. Кальми-Ре заявила, что цель ее страны — «привнести в основу нынешнего обсуждения ядерного разоружения гуманитарный аспект»[9]. Стоит отметить и выступление министра иностранных дел Норвегии Й. Г. Стере в феврале 2010 г., посвященное смене установок в области разоружения и обращению к *гуманитарному разоружению*[10].

Следует сделать оговорку относительно терминологии. Поскольку большая часть документов, касающихся гуманитарных аспектов, публиковалась на английском языке, приведем три формулы, которыми авторы этих документов и выступлений оперируют: *humanitarian consequences [of any use of nuclear weapons], humanitarian impact [of nuclear weapons]* и *humanitarian dimensions [of nuclear weapons]*. Чаще всего в заявлениях встречается первое понятие, которое в русскоязычных документах, посвященных ядерному оружию и другим сферам международной безопасности, переводится как *гуманитарные последствия*. Вторая приведенная формула в документах, касающихся ядерного оружия, звучит как *гуманитарные последствия применения [ядерного оружия]*[11]. Однако ранее в документах Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие, или Конвенции о негуманном оружии (КНО) это выражение переводилось и как *последствия*, и как *издержки* применения вооружений[12]. Далее в цитатах, приведенных в работе, будет использоваться термин *последствия*, хотя автор считает термин *издержки* более удачным в данном случае.

В 2011 г. Австрия, Мексика и Норвегия (получившие в ооновском *закулисье* прозвище *Новое Движение неприсоединения*[13, 14]) представили в Первом комитете ГА ООН проект резолюции, озаглавленной *Продвижение вперед процесса многосторонних переговоров по разоружению*[15]. Формулировка *выражая глубокую озабоченность по поводу катастрофических гуманитарных последствий любого применения ядер-*

ного оружия прозвучала в одном из первых положений преамбулы. В мае 2012 г. на первой сессии Подготовительного комитета к Обзорной конференции ДНЯО представитель Швейцарии зачитал *Совместное заявление о гуманитарных аспектах ядерного разоружения* от имени Группы шестнадцати[16] (Group of 16)[17]. В состав этой группы помимо Швейцарии вошли все страны *Нового Движения неприсоединения* и некоторые участники двух действующих в обзорном процессе объединений государств: Движения неприсоединения и Коалиции за новую повестку дня (КНПД). Аналогичное *Совместное заявление о гуманитарных последствиях ядерного оружия* было зачитано в том же году в Первом комитете ГА ООН уже от лица 35 государств[18] — к группе примкнули Белоруссия и Казахстан (члены Организации Договора о коллективной безопасности (ОДКБ), находящиеся под *ядерным зонтиком*[19]; Казахстан помимо этого входит в центральноазиатскую безъядерную зону), Исландия (страна — член НАТО), Лихтенштейн и Мальта, а также государства Юга — представители Движения неприсоединения.

В 2013 г. в Осло прошла первая конференция под названием *Гуманитарные последствия применения ядерного оружия*, в которой участвовали официальные представители 127 государств, не обладающих ядерным оружием (НЯОГ)[20]. Основным итогом конференции ее участники назвали подтверждение того факта, что ни одно государство или международный орган «не смогут должным образом справиться с чрезвычайной ситуацией гуманитарного характера, возникшей из-за применения ядерного оружия, и предоставить необходимую помощь пострадавшим. Более того, даже если будут предприняты попытки организовать такую помощь, вероятно, ее не удастся наладить».[21] Результаты конференции были представлены на второй сессии Подготовительного комитета Конференции 2015 года по рассмотрению действия ДНЯО в мае 2013 г. Тогда же посол ЮАР от имени 80 государств представил совместное заявление о гуманитарных последствиях применения ядерного оружия[22], подчеркнув важность выполнения плана действий, принятого на Обзорной конференции в 2010 г. Кроме членов Движения неприсоединения заявление поддержали Босния и Герцеговина, Грузия, Кипр, Люксембург (страна НАТО), Сербия и Украина. В том же 2013 г. Новая Зеландия представила в Первом комитете ГА ООН совместное заявление от лица 123 государств[23] под названием *О гуманитарных последствиях применения ядерного оружия*. Помимо стран, ранее поддерживавших аналогичные заявления, и большой группы государств Юга, в основном входящих в Движение неприсоединения, к заявлению присоединилась Япония.

В 2014 г. Мексика и Австрия провели еще две Конференции по гуманитарным последствиям применения ядерного оружия: в февральской встрече в Наярите приняли участие официальные делегации 146 стран[24], а в конференции в Вене в декабре 2014 г. участвовали официальные представители 158 государств[25] — в том числе США[26] и Великобритании[27], а Китай, по некоторым данным, отправил на конференцию высокопоставленного чиновника под видом эксперта[28]. Предполагалось, что четвертая гуманитарная конференция, посвященная последствиям применения ЯО, пройдет в 2015 г. в ЮАР, а следующая — в 2016 г. в Малайзии, однако по состоянию на май 2016 г. очередная конференция так и не была проведена.

Именно на Венской конференции делегация Австрии в своем национальном качестве представила так называемое *Австрийское обязательство*[29] — документ с призывом заполнить *правовую лакуну* (legal gap) в отношении запрещения и ликвидации ядерного оружия — то есть принять некую декларацию, конвенцию или дру-

гой международно-правовой документ, в котором четко прописывалась бы незаконность обладания ядерным оружием. После завершения конференции постоянное представительство Австрии при ООН и других международных организациях в Женеве разослало в постпредства всех стран письмо с призывом присоединиться к обязательству, направив вербальную ноту в адрес правительства Австрии[30]. На Обзорной конференции ДНЯО в мае 2015 г. после того, как к документу присоединилось несколько десятков стран, было объявлено о его переименовании в *Гуманитарное обязательство*.

Важно отметить, что у группы государств, выступавших в поддержку вышеупомянутых заявлений, не было никакого координатора. Их тексты вырабатывала Группа шестнадцати, которая, однако, не прилагала практически никаких усилий для мобилизации массовой поддержки[31]. Почему в таком случае этой группе так быстро удалось привлечь к своей инициативе столь значительную группу стран? На то есть несколько причин.

Гуманитарная риторика в дебатах, касающихся международных отношений и особенно вооружений, за последние 20–25 лет стремительно набирает обороты. Здесь можно упомянуть Оттавскую конвенцию 1997 г., Конвенцию о кассетных боеприпасах, открытую для подписания в 2008 г., и риторику вокруг принятия Международного договора о торговле оружием, и даже набирающее обороты движение за запрет автономных боевых систем. Немалую роль в этом сыграло гражданское общество, широко представленное на некоторых межправительственных площадках неправительственными организациями (НПО) — в первую очередь, Международным комитетом Красного Креста (МККК).

В последние годы НЯОГ все чаще указывали государствам, обладающим ядерным оружием (ЯОГ), на необходимость дальнейших шагов и решительных действий в сфере разоружения и даже предлагали планы действий. Нарастающее недовольство было использовано *антиядерными активистами* для продвижения новой повестки дня в противовес стратегической стабильности и ядерному сдерживанию — традиционным позициям ЯОГ. Австрийский посол А. Кментт в марте 2015 г. указывал, что выводы, сделанные в результате обсуждения гуманитарных последствий применения ЯО, «должны привести к глубокому пересмотру теории сдерживания»[32].

Еще одну причину приводят в своем исследовании Дж. Нильсен и М. Хансон[33], которые отмечают возросшую после окончания холодной войны роль *средних держав*[34] в обсуждении вопросов и принятии решений, касающихся контроля над вооружениями.

ГРУППА ШЕСТНАДЦАТИ

На этапе формирования гуманитарного движения (2010–2012 гг.) выделились его лидеры: Австрия, Мексика, Новая Зеландия, Норвегия, Швейцария и ЮАР. Заметим, что эти страны занимались *антиядерным активизмом* на протяжении всей истории обзорного процесса ДНЯО и в их позиции нет ничего нового. Все они вошли в Группу шестнадцати — ситуативное объединение государств, в 2012–2015 гг. согласовывавших свои позиции и заявления в обзорном процессе ДНЯО и на заседаниях ГА ООН.

По мнению некоторых дипломатов из ЯОГ, Группа шестнадцати была создана для того, чтобы способствовать принятию Конвенции о ядерном оружии[35], и представители группы, по имеющейся информации, это предположение подтверждали[36]. Все участники Группы шестнадцати, как показано в таблице ниже, одновременно входили в состав других коалиций, действующих в обзорном процессе ДНЯО, в том числе тех, что объединяли свои усилия по продвижению повестки разоружения в течение десятков лет. Возможно, дипломатические связи, сформировавшиеся в ходе совместной работы на форумах по нераспространению и разоружению, позволили представителям объединения обсуждать интересующие их вопросы в более тесном формате и по существу.

Страны, входящие в основные коалиции в обзорном процессе ДНЯО, и их членство в других группах и альянсах

	Группа шестнадцати	Страны Гуманитарного обязательства	Коалиция за новую повестку дня (New Agenda Coalition, NAC)	Движение неприсоединения (Non-Aligned Movement, NAM)	Венская группа десяти (Vienna Group of 10)	Инициатива в области нераспространения и разоружения (Non-Proliferation and Disarmament Initiative, NPDI)	Группа за снятие с боевого дежурства (De-alerting group)	НАТО
Австрия	+	+			+			
Ватикан	+	+						
Дания	+				+			+
Египет	+	+	+	+				
Индонезия	+	+		+				
Ирландия	+	+	+		+			
Коста-Рика	+	+						
Малайзия	+	+		+			+	
Мексика	+	+	+			+		
Нигерия	+	+		+		+	+	
Новая Зеландия	+		+		+		+	
Норвегия	+				+			+
Филиппины	+	+		+		+		
Чили	+	+		+		+	+	
Швейцария	+						+	
ЮАР	+	+	+	+				

Существование группы прекратилось после Обзорной конференции ДНЯО 2015 г., эстафета была *перехвачена* австрийским Гуманитарным обязательством. Впрочем, никаких инициатив на 70-й сессии ГА ООН в том же году[37] выдвинуто не было.

Подводя итог под описанием состояния *гуманитарного процесса* на конец 2014 г., приведем основные тезисы всех совместных заявлений о гуманитарных последствиях, сформулированных Группой шестнадцати. В 2012 г. составление текста заявления в группе координировала Швейцария, в 2013 г. — ЮАР, в 2014 г. — Новая Зеландия, а в 2015 г. — Австрия[38]. В документах говорилось о применимости международного гуманитарного права к вопросам использования ЯО; о принятой в 2011 г. резолюции Совета делегатов МККК[39]; о необходимости и важности искоренения ЯО под эффективным международным контролем через выполнение Статьи VI ДНЯО; необходимости исполнения плана действий, принятого на Обзорной конференции ДНЯО в 2010 г. Кроме того, обращалось внимание на значительную роль гражданского общества в осознании последствий применения ЯО. В заявлениях 2013–2015 гг. добавились указания на важность проведения конференций о гуманитарных последствиях применения ядерного оружия и некоторые их результаты.

В 2013 г. Группа шестнадцати поставила перед собой цель заручиться поддержкой со стороны ряда государств, в том числе Австралии, Канады, Нидерландов и Японии. Однако одно из положений предложенного текста совместного заявления вызывало у этих государств неприятие, так как противоречило их концепциям национальной безопасности. Это положение звучит так: «Чрезвычайно важно, чтобы эти (ядерные — *А. М.*) вооружения никогда и ни при каких условиях не были использованы вновь». Эта формулировка, к примеру, весьма смутила Японию[40], однако ничто не могло убедить Группу шестнадцати отказаться от нее.

Австралия, в силу национальных интересов и особенностей концепции национальной безопасности не имеющая возможности согласиться с формулировкой *ни при каких условиях,* но понимая, что антиядерные активисты не откажутся от нее, приняла решение выработать собственное гуманитарное заявление с учетом того, что ранее она частично поддерживала подобную риторику. Ей удалось склонить на свою сторону Канаду и Нидерланды[41], а в итоге к заявлению присоединились 17 государств-членов НАТО, а также Финляндия, Швеция и Япония[42].

Антиядерные НПО и даже некоторые государства осудили решение Австралии о выдвижении собственного заявления, посчитав его своего рода *спойлером.* Однако лидеры Группы шестнадцати — Австрия и Швейцария — согласились с тем, что оба гуманитарных заявления дополняют друг друга[43]. МИД Австралии заявил, что целью этого шага была демонстрация поддержки гуманитарной повестки дня, пусть и с определенными оговорками — представители министерства указывали, что гуманитарная риторика не может исходить от одной-единственной группы[44].

В 2015 г. вышеупомянутая спорная формулировка вошла в резолюцию ГА ООН[45]. Это можно назвать одним из итогов работы Гуманитарной инициативы как в обзорном процессе ДНЯО, так и за его пределами. Риторика, обозначенная на Обзорной конференции и получившая развитие благодаря образовавшейся в рамках обзорного процесса Группе шестнадцати, распространилась далеко за пределы этого небольшого объединения государств, став одним из самых спорных моментов Обзорной конференции ДНЯО 2015 г.

ОБЗОРНАЯ КОНФЕРЕНЦИЯ ДНЯО-2015

Дебаты относительно гуманитарных последствий ядерного оружия и необходимости выработки юридически обязывающего инструмента для выполнения Статьи VI ДНЯО были, по словам представителя Швейцарии посла Б. Лаггнера, жесткими как атмосферно, так и по существу[46]. Эта дискуссия еще до начала Обзорной конференции ДНЯО 2015 г. отразила значительную разницу в подходах. На Обзорной конференции эти различия только усугубились.

С самого начала конференции гуманитарная риторика звучала практически в каждом заявлении — в первый и второй день мероприятия о гуманитарных аспектах не упомянули только ядерные государства (исключая, впрочем, Великобританию) и некоторые страны НАТО. Можно предположить, что вопрос о гуманитарных последствиях существования ядерного оружия, поднятый за рамками обзорного процесса, действительно повысил ожидания от конференции абсолютного большинства НЯОГ и укрепил в них надежду на перелом в понимании глобальной безопасности и уход от ее интерпретации через призму стратегической стабильности. На второй день конференции федеральный министр европейских и международных дел Австрии С. Курц представил очередное *Совместное заявление о гуманитарных последствиях*[47], к которому в этот раз присоединились 159 государств. Кроме того было объявлено, что *Австрийское обязательство* поддержали более 100 государств[48], а представитель Австрии заявил о его интернационализации[49] — то есть обязательство из исключительно австрийского превратилось в международное.

Впрочем, десятки стран, упоминавших гуманитарные последствия в своих заявлениях, практически не предпринимали усилий для того, чтобы эти идеи были включены в заключительный документ конференции. Наиболее активно в этом направлении действовали делегация Австрии, страны Коалиции за новую повестку дня и Коста-Рика. В результате в первом представленном проекте доклада указывалось, что большинство стран-участниц ДНЯО «считает необходимым установление правовых рамок для выполнения Статьи VI»[50], в связи с чем конференция должна призвать всех участников Договора начать выработку правовых норм, которые могут быть воплощены в отдельном документе (составленном в форме договора о запрещении ядерного оружия либо всеобъемлющей конвенции о ядерном оружии, включающей в себя план поэтапного уничтожения ЯО к определенной дате, или иных формах). Первый проект полностью не устраивал ЯОГ из-за своей риторики (главным образом, это касается упоминаний *катастрофических последствий применения ядерного оружия* и связанных с ними вопросами, то есть гуманитарной повестки[51]).

В начале четвертой недели председатель конференции сформировала группу друзей председателя, состоящую из 19 стран, призванных выработать консенсусную формулировку относительно ядерного разоружения. В группу вошли постоянные члены Совбеза ООН, все государства КНПД, представители Группы шестнадцати и других коалиций обзорного процесса. В качестве председателя выступала либо председатель конференции Т. Ферухи, либо председатель вспомогательного органа 1 (в задачи которого входит рассмотрение вопросов ядерного разоружения и гарантий безопасности[52]) посол Б. Лаггнер[53].

Новый вариант доклада, представленный Б. Лаггнером[54], был мягче предыдущего, однако не устроил ни антиядерных активистов, которые сочли текст слишком мягким (например, КНПД указывала на то, что текст в должной мере не отражает глубины обеспокоенности государств — участников гуманитарных конференций ужасающими последствиями существования ЯО, а также не обеспечивает должного признания представленных в поддержку этой позиции фактов[55]), ни представителей ЯОГ и стран, находящихся под *ядерным зонтиком*, которые посчитали его слишком жестким[56]. Однако именно в таком виде председатель конференции включила положения, касающиеся разоружения, в проект заключительного документа[57].

Таким образом, антиядерные активисты не смогли добиться принятия *жесткого* заключительного документа. В то же время продвигаемая ими повестка дня была представлена в нем весьма широко. Проявились разногласия внутри Группы шестнадцати: представитель одного из ее лидеров, Швейцарии, посол Б. Лаггнер, старался смягчить положения, в то время как представитель Австрии настаивал на их ужесточении[58].

РАСКОЛ ДВИЖЕНИЯ И ИСПОЛЬЗОВАНИЕ ГУМАНИТАРНОЙ РИТОРИКИ ДРУГИМИ ГРУППАМИ СТРАН

Выработка *Австрийского обязательства* и его широкая поддержка большей частью сторонников Гуманитарной инициативы продемонстрировали существование раскола в подходе к изменению разоруженческой повестки. По состоянию на май 2016 г. под документом подписались 127 государств. В то же время за резолюцию A/RES/70/48 с аналогичным названием и содержанием на сессии ГА ООН в декабре 2015 г. проголосовали 139 стран[59] — в их числе Швейцария, Швеция и Новая Зеландия, которые формально не присоединились к обязательству. Представитель Новой Зеландии даже заострил на этом внимание в разъяснении мотивов голосования[60]. Представители Швеции и Швейцарии отметили, что не признают существования *правовой лакуны*, хотя и считают, что для выполнения Статьи VI ДНЯО понадобится составить новые правовые документы[61].

Итак, гуманитарная риторика в настоящее время используется всеми возможными игроками и объединениями в рамках обзорного процесса ДНЯО и на других площадках, занимающихся разоружением. Одни государства активно выступают за ядерное разоружение и готовы начать обсуждение новых правовых документов для заполнения *правовой лакуны* без участия ядерных государств (примеры: Австрия, Ирландия). Другие, в том числе Швейцария, привнесшая в разговоры о разоружении гуманитарную риторику, а также Новая Зеландия и Швеция считают, что начинать обсуждение новых правовых инструментов без участия членов *ядерного клуба* бессмысленно, однако целиком согласны с буквой и духом *Совместных заявлений о гуманитарных последствиях ядерного оружия*. Третья группа государств и коалиций согласна с тем, что подход, при котором ЯОГ не участвуют в обсуждении вопроса о новых мерах для имплементации Статьи VI ДНЯО, непрактичен. Эти же страны приняли решение о выработке собственных гуманитарных заявлений, не содержащих формулировки о том, что ядерные вооружения никогда и ни при каких условиях не должны быть использованы вновь. К этой группе относятся страны — члены НАТО, Австралия и Япония. Большинство ядерных

государств не принимает участие в обсуждениях гуманитарных последствий ядерного оружия, однако на обзорной конференции ДНЯО 2015 г. представитель Великобритании в официальном выступлении согласился с тем, что ядерные вооружения «могут иметь разрушительные гуманитарные последствия»[62]. Таким образом, можно говорить о фрагментации или даже исчезновении одной из коалиций обзорного процесса ДНЯО — Группы шестнадцати — которая, по всей видимости, уже не будет координировать свои действия в обзорном процессе в таком составе и с такой повесткой дня, как это было в 2012–2015 гг.

ЗНАЧЕНИЕ ГУМАНИТАРНОЙ ИНИЦИАТИВЫ ДЛЯ ОБЗОРНОГО ПРОЦЕССА ДНЯО

В 2010–2015 гг. в обзорном цикле ДНЯО отчетливо выделились три группы стран, чьи подходы к разоружению существенно различаются: государства *ядерной пятерки*, страны под *ядерным зонтиком* (которые категорически настаивают на том, что их позиция не идентична позиции ядерных государств) и страны *гуманитарного лагеря*. Позиция первых заключается в том, что разоружение в настоящий момент происходит удовлетворительными темпами и форсировать этот процесс не только не нужно, но и вредно. Позиция государств, имеющих обязательства, налагаемые политикой расширенного сдерживания, разнится от страны к стране, но в целом заключается в том, что процесс разоружения застопорился и его необходимо оживить, однако принятие конвенции о ядерном оружии или другого подобного документа преждевременно и бессмысленно. Эти государства в основном придерживаются пошагового подхода, однако не всегда предлагаемые ими шаги совпадают с представлениями ЯОГ.

Гуманитарный лагерь, в свою очередь, очень неоднороден. Эти страны выступают за принятие юридически обязывающего инструмента, который способствовал бы выполнению Статьи VI ДНЯО. Кроме того, они пытаются продемонстрировать ядерным государствам новую философию разоружения, согласно которой мотивацией выступают не соображения стратегической стабильности, а стремление к скорейшему сокращению колоссальных рисков для всего человечества. И если в этом понимании сходятся все страны, обеспокоенные гуманитарными последствиями, то в отношении процесса принятия юридически обязывающего инструмента, делающего обладания ЯО незаконным, имеются разногласия. Некоторые государства, включая Австрию, Бразилию и Мексику, уверены, что документ может быть обсужден, согласован и принят без участия ядерных государств. Другие (например, Швейцария, Новая Зеландия), хотя и поддерживают идею создания такого инструмента, считают, что без участия ядерных государств документ не будет иметь смысла. Основное развитие Гуманитарная инициатива получила за рамками обзорного процесса — на организованных Норвегией, Мексикой и Австрией гуманитарных конференциях и на Генеральной Ассамблее ООН, в том числе в ее вспомогательном органе — Рабочей группе открытого состава по разоружению.

Здесь важно сделать оговорку относительно стран — участниц ОДКБ. Формально они находятся под российским *ядерным зонтиком,* но часть из них относится, скорее, к лагерю *гуманитарных* государств (в первую очередь, речь идет о Казахстане и Киргизии). Среди стран, находящихся под американским *ядерным зонтиком,* симпатию радикальной гуманитарной повестке высказывали Норвегия и Япония.

К ЧЕМУ ПРИВЕЛО ИСПОЛЬЗОВАНИЕ ГУМАНИТАРНОЙ РИТОРИКИ В ОБЗОРНОМ ПРОЦЕССЕ?

Произошла поляризация позиций *антиядерных активистов*. Обособилась группа наиболее радикально настроенных в отношении процесса разоружения государств, готовых принять специальные международные правовые документы, утверждающие незаконность ядерного оружия — речь идет, в первую очередь, об Австрии и Мексике. Они отделились от более широкой и по составу, и по взглядам Группы шестнадцати, другие участники которой, хотя и выступают за скорейшее разоружение, не готовы к столь радикальным мерам.

Вновь был поднят вопрос о законности обладания ядерным оружием[63], а на Обзорной конференции 2015 г. основные дебаты развернулись по вопросу о гуманитарных аспектах как стимуле скорейшего ядерного разоружения. НЯОГ через новую риторику призывали и продолжают призывать к ускорению процесса разоружения в наиболее радикальной манере, то есть через скорейшее принятие документов, запрещающих ядерное оружие.

Стало очевидным, что эрозия института *связывающих стран (bridging states),* возникшая, с одной стороны, из-за несоответствия желаемых НЯОГ темпов разоружения и практических предпринимаемых действий, а с другой стороны, под давлением антиядерных активистов, наносит значительный вред дипломатии, в том числе в рамках обзорного процесса ДНЯО. Критика *средней* позиции и ее стигматизация антиядерными активистами и НПО привели к ее размыванию и затруднению поиска точек соприкосновения. Страны, находящиеся под *ядерным зонтиком,* обратились к гуманитарной риторике, чтобы не остаться в стороне от идей, которые они в целом поддерживают, и, возможно, готовы взять на себя задачу по *наведению мостов*, однако это не вызвало одобрения антиядерных активистов и не заставило страны *ядерной пятерки* более терпимо относиться к идее о гуманитарных последствиях. Более того, стигматизация позиций ЯОГ привела к их нежеланию и невозможности начать диалог с антиядерными странами.

Обзорному процессу ДНЯО был нанесен ущерб, так как гуманитарные форумы воспринимались как альтернативная площадка для обсуждения вопросов и продвижения повестки разоружения. Едва ли будут проведены новые гуманитарные конференции, учитывая, что в настоящее время поднятые на них вопросы обсуждаются в Рабочей группе открытого состава, являющейся вспомогательным органом Генеральной Ассамблеи ООН. Эта группа была созвана именно благодаря призыву заполнить *правовую лакуну* в отношении запрещения и ликвидации ядерного оружия. Рабочая группа открытого состава также имеет перспективы стать некой альтернативой обзорному процессу. Важно, что поднятая Гуманитарной инициативой дискуссия, начавшись на консенсусной площадке обзорной конференции ДНЯО, сейчас проводится уже в соответствии с правилами ГА ООН — то есть решения принимаются простым большинством голосов (хотя они и носят не обязательный, а только рекомендательный характер).

Можно сказать, что страны, поддержавшие гуманитарную позицию, в целом добились своих целей: привнесли новую риторику и инициировали обсуждение в правительственных кругах и экспертном сообществе новой парадигмы, которая могла бы прийти на смену стратегической стабильности и ядерному сдерживанию.

Активисты вынесли на обсуждение в формате ООН вопрос о принятии юридически обязывающего документа, который позволил бы запретить ядерное оружие. 

Примечания

1 A/RES/70/33. Продвижение вперед процесса многосторонних переговоров по ядерному разоружению. Резолюция, принятая Генеральной Ассамблеей 7 декабря 2015 года, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/33 (последнее посещение — 24 мая 2016 г.)

2 A/AC.286/WP.17. A legally-binding instrument that will need to be concluded to attain and maintain a world without nuclear weapons: a prohibition on nuclear weapons. Item 5 of the agenda Taking forward multilateral nuclear disarmament negotiations. Submitted by Mexico. 12 April 2016, http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/OEWG/2016/Documents/WP17.pdf (последнее посещение — 24 мая 2016 г.)

3 A/AC.286/WP.36. The *Legal Gap*: Recommendations to the Open-ended Working Group on taking forward nuclear disarmament negotiations. Open-ended Working Group taking forward multilateral nuclear disarmament negotiations. Geneva, May 4, 2016, http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/OEWG/2016/Documents/WP36.pdf (последнее посещение — 24 мая 2016 г.)

4 Здесь и далее в отношении проблематики, поднимаемой гуманитарным движением стран, будут употребляться понятия *законность* и, несмотря на некоторую нелогичность термина в отношении международных отношений (так как в основе международного права, как известно, лежат договоры и обычаи, а не законы). Подписанты соответствующих англоязычных документов употребляют в них слово legality, который можно перевести как раз как *законность* или *легальность*.

5 A/C.1/70/L.37 Гуманитарные последствия применения ядерного оружия, http://www.un.org/ga/search/viewm_doc.asp?symbol=A/C.1/70/L.37 (последнее посещение — 24 мая 2016 г.)

6 Humanitarian Pledge. — International Campaign to abolish nuclear weapons. URL: http://www.icanw.org/pledge/

7 Далее первые будем для краткости называть Гуманитарной инициативой, вторые — странами Гуманитарного обязательства.

8 Конференция 2010 года участников Договора о нераспространении ядерного оружия по рассмотрению действия Договора. Заключительный документ (Часть I). Нью-Йорк, 2010. С. 22, http://www.un.org/ga/search/view_doc.asp?symbol=NPT/CONF.2010/50%20 (VOL.I)&referer=http://www.un.org/en/conf/npt/2010/confdocs.shtml&Lang=R (последнее посещение — 24 мая 2016 г.)

9 8th Review Conference of the States Parties to the Nuclear Non-Proliferation Treaty (NPT). General Debate Statement by Her Excellency Micheline Calmy-Rey, Head of the Federal Department of Foreign Affairs. New York, 4 May 2010, https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/sicherheitspolitik/NPT-RevCon-2010-Declaration-Debat-general-HLS-PJD_en.pdf (последнее посещение — 24 мая 2016 г.)

10 Støre Jonas Gahr, Disarmament — reframing the challenge. The Norwegian Atlantic Committee. The 45th Annual Conference. (Leangkollen Conference). Oslo, 1 February 2010, https://www.regjeringen.no/en/aktuelt/disarmament/id592550/(последнее посещение — 24 мая 2016 г.)

11 Для сравнения: название документа NPT/CONF.2015/PC. III/WP.35 на русском языке *Резюме Председателя второй Конференции по гуманитарным последствиям применения ядерного оружия Наярит, Мексика, 14 февраля 2014 года*, на английском — *Chair's summary: second Conference on the Humanitarian Impact of Nuclear Weapons Nayarit, Mexico, 14 February 2014*, http://www.un.org/Docs/journal/asp/ws.asp?m=NPT/CONF.2015/PC. III/WP.35 (последнее посещение — 24 мая 2016 г.)

12 Для сравнения: в документе КНО CCW/GGE/2011-III/3 во всех случаях impact переводится как *издержки* (на русском: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/634/91/PDF/G1163491.pdf?OpenElement, на английском: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/634/89/PDF/G1163489.pdf?OpenElement). В документе КНО CCW/MSP/2008/SR.1 во всех случаях impact переводится как *последствия* (на русском: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G08/644/81/PDF/G0864481.pdf?OpenElement, на английском: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G08/644/79/PDF/G0864479.pdf?OpenElement). В документе КНО CCW/AP.II/CONF.9/SR.1 в ряде случаев impact переводится как *издержки* (п. 60), а в ряде — как *последствия* (пп. 22, 33) (на русском: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G07/643/10/PDF/G0764310.pdf?OpenElement,наанглийском:https://documents-dds-ny.un.org/doc/UNDOC/GEN/G07/643/08/PDF/G0764308.pdf?OpenElement).

13 Meyer Paul. Nuclear disarmament: The hard slog to get beyond rhetoric — The Embassy, 15 November 2012,: http://www.embassynews.ca/opinion/2012/11/15/nuclear-disarmament-the-hard-slog-to-get-beyond-rhetoric/42842 (последнее посещение — 24 мая 2016 г.)

14 Løvold, Magnus. We'll get you in the end — *Twenty Tons of TNT*, 4 November 2011, http://in-spite-of-all.blogspot.ru/2011/11/well-get-you-in-end.html (последнее посещение — 24 мая 2016 г.)

15 A/C.1/66/L.21/Rev.1. Австрия, Мексика и Норвегия: пересмотренный проект резолюции Продвижение вперед процесса многосторонних переговоров по разоружению, 25 октября 2011 г., http://www.un.org/Docs/journal/asp/ws.asp?m=A/C.1/66/L.21/Rev.1 (последнее посещение — 24 мая 2016 г.)

16 Австрия, Ватикан, Дания, Египет, Индонезия, Ирландия, Коста-Рика, Малайзия, Мексика, Нигерия, Новая Зеландия, Норвегия, Филиппины, Чили, Швейцария, ЮАР

17 Joint Statement on the humanitarian dimension of nuclear disarmament. — First Session of the Preparatory Committee for the 2015 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, 2 May 2012, http://www.un.org/disarmament/WMD/Nuclear/NPT2015/PrepCom2012/statements/20120502/SwitzerlandOnBehalfOf.pdf (последнее посещение — 24 мая 2016 г.)

18 Joint Statement on the humanitarian dimension of nuclear disarmament — 67th session of the United Nations General Assembly First Committee, 22 October 2012, http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com12/statements/22Oct_Switzerland.pdf (последнее посещение — 24 мая 2016 г.)

19 Договор о коллективной безопасности. Ташкент, 15 мая 1992 г. Статья 4, (http://www.odkb.gov.ru/b/azb.htm), Концепция коллективной безопасности государств-участников Договора о коллективной безопасности от 15 мая 1992 г. Пункт II. (http://www.odkb.gov.ru/b/azc.htm), Военная доктрина Российской Федерации (в редакции от 2015 г.). Пункт 27 (http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/976907/pop_up?_101_INSTANCE_CptICkB6BZ29_viewMode=tv&_101_INSTANCE_CptICkB6BZ29_qrIndex=0)

20 Резюме председателя конференции, https://www.regjeringen.no/globalassets/upload/ud/vedlegg/hum/chair_russian.pdf (последнее посещение — 24 мая 2016 г.)

21 Там же

22 Joint Statement on the humanitarian impact of nuclear weapons — Second Session of the Preparatory Committee for the 2015 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, 24 April 2013, http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/prepcom13/statements/24April_SouthAfrica.pdf (последнее посещение — 24 мая 2016 г.)

23 UNGA 68: First Committee Joint Statement on the Humanitarian Consequences of Nuclear Weapons. Delivered by Ambassador Dell Higgle 21 October 2013, http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_21-Oct_CL-1_New_Zealand- (Joint_St)) (последнее посещение — 24 мая 2016 г.)

24 NPT/CONF.2015/PC. III/WP.35. Резюме Председателя второй Конференции по гуманитарным последствиям применения ядерного оружия Наярит, Мексика, 14 февраля 2014 г., http://www.un.org/Docs/journal/asp/ws.asp?m=NPT/CONF.2015/PC. III/WP.35 (последнее посещение — 24 мая 2016 г.)

25 Vienna Conference on the Humanitarian Impact of Nuclear Weapons, http://www.bmeia.gv.at/en/european-foreign-policy/disarmament/weapons-of-mass-destruction/nuclear-weapons-and-nuclear-terrorism/vienna-conference-on-the-humanitarian-impact-of-nuclear-weapons/(последнее посещение — 24 мая 2016 г.)

26 United States Will Attend the Vienna Conference on the Humanitarian Impact of Nuclear Weapons. Office of the Spokesperson of the U.S. Department of State. 7 November 2014, http://www.state.gov/r/pa/prs/ps/2014/11/233868.htm (последнее посещение — 24 мая 2016 г.)

27 UK intervention at the Vienna Conference on the Humanitarian Impact of Nuclear Weapons. UK Mission to the United Nations. 9 December 2014,://www.gov.uk/government/world-location-news/uk-intervention-at-the-vienna-conference-on-the-humanitarian-impact-of-nuclear-weapons (последнее посещение — 24 мая 2016 г.)

28 Chernyshova Daria. Chinese Official Attends Vienna Nuclear Conference Under Guise of Academic. Sputnik, Vienna, 9 December 2014, http://sputniknews.com/military/20141209/1015651824.html (последнее посещение — 24 мая 2016 г.)

29 Pledge presented at the Vienna Conference on the Humanitarian Impact of Nuclear Weapons by Austrian Deputy Foreign Minister Michael Linhart Vienna, December 2014, https://www.bmeia.gv.at/

fileadmin/user_upload/Zentrale/Aussenpolitik/Abruestung/HINW14/HINW14_Austrian_Pledge.pdf (последнее посещение — 24 мая 2016 г.)

30 Document Genf-V/POL/0027/2015, issued by Permanent Mission of Austria to the United Nations in Geneva, есть в распоряжении автора.

31 Электронная переписка с представителем постпредства Швейцарии при ООН в Женеве, февраль 2016 г.

32 Kmentt Alexander. Der pragmatische Realismus des Wahnsinns. Internationale Politik und Gesellschaft, 23.03.2015, http://www.ipg-journal.de/schwerpunkt-des-monats/neue-high-tech-kriege/artikel/detail/der-pragmatische-realismus-des-wahnsinns-851/(последнее посещение — 24 мая 2016 г.)

33 Nielsen Jenny, Hanson Marianne. The European Union and the Humanitarian Initiative In the 2015 Non-Proliferation Treaty Review Cycle. EU Non-Proliferation Consortium. Non-Proliferation Papers. No. 41 December 2014, P. 3, http://www.nonproliferation.eu/web/documents/nonproliferationpapers/jennyniel senmariannehanson54856428912ca.pdf (последнее посещение — 24 мая 2016 г.)

34 Средняя держава — политически и экономически значимое государство, добровольно отказавшееся от участия в ядерной гонке. Как правило, это состоятельные, стабильные, эгалитарные государства. (Определение на основе документа Creating the Conditions and Building the Framework for a Nuclear Weapons-Free World, (http://www.middlepowers.org/pubs/Building-a-Framework.pdf) и исследования The concept of a middle power in international relations: distinguishing between emerging and traditional middle powers, Jordaan E.; Politikon: South African Journal of Political Studies, Volume 30, Issue 1, 2003)

35 Рассекреченная переписка представителей МИД Австралии, с. 16. (DFAT — Declassified. File 13/19834. Copy issued under FOI Act 1982, https://dfat.gov.au/about-us/corporate/freedom-of-information/Documents/dfat-foi-1312-F722.pdf (последнее посещение — 24 мая 2016 г.)

36 Рассекреченная переписка представителей МИД Австралии, с. 16. (DFAT — Declassified. File 13/19834. Copy issued under FOI Act 1982, https://dfat.gov.au/about-us/corporate/freedom-of-information/Documents/dfat-foi-1312-F722.pdf (последнее посещение — 24 мая 2016 г.)

37 Интервью с сотрудником постоянного представительства Швейцарии в ООН и других международных организациях в Женеве. Февраль, 2016 г.

38 Интервью с сотрудником постоянного представительства Швейцарии в ООН и других международных организациях в Женеве. Февраль, 2016 г.

39 Совет делегатов, 2011: Резолюция 1. Содействуя уничтожению ядерного оружия. 26 ноября 2011 г., https://www.icrc.org/rus/resources/documents/resolution/council-delegates-resolution-1-2011.htm (последнее посещение — 24 мая 2016 г.)

40 За поддержку этого заявления Япония, по некоторым данным, получила выговор от США (рассекреченная переписка представителей МИД Австралии. С. 29).

41 Рассекреченная переписка представителей МИД Австралии. С. 46.

42 Joint Statement on the humanitarian consequences of nuclear weapons. Delivered by Ambassador Peter Woolcott Australian Permanent Representative to the United Nations, Geneva and Ambassador for Disarmament. UNGA68 First Committee. 21 October 2013, http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com13/statements/21Oct_Australia2.pdf (последнее посещение — 24 мая 2016 г.)

43 Рассекреченная переписка представителей МИД Австралии. С. 74.

44 Рассекреченная переписка представителей МИД Австралии. С. 83.

45 Так, австралийский дипломат во время обсуждения гуманитарного заявления на ГА ООН в 2013 г. в личной переписке даже согласился с мнением о том, что приведенная фраза была нарочно выработана Группой шестнадцати как «проклятие для государств, которые полагаются на расширенное ядерное сдерживание» (источник — рассекреченная переписка представителей МИД Австралии. С. 41

46 Mukhatzhanova Gaukhar's speech at the EU Non-Proliferation and Disarmament Conference 2015 First Plenary Session, http://www.iiss.org/en/Topics/eu-non-proliferation-and-disarmament-conference/mukhatzhanova-dfdb (последнее посещение — 24 мая 2016 г.)

47 Joint Statement on the Humanitarian Consequences of Nuclear Weapons delivered by H. E. Sebastian Kurz Federal Minister for Europe, Integration and Foreign Affairs of Austria 28 April 2015. 2015 Review

Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2015/statements/28April_AustriaHumanitarian.pdf (последнее посещение — 24 мая 2016 г.)

48 Mukhatzhanova Gaukhar, Notes From The Revcon III. Arms Control Wonk, 8 June 2015 http://www.armscontrolwonk.com/archive/207695/notes-from-the-revcon-iii/(последнее посещение — 24 мая 2016 г.)

49 Humanitarian Pledge, http://www.bmeia.gv.at/fileadmin/user_upload/Zentrale/Aussenpolitik/Abruestung/HINW14/HINW14vienna_Pledge_Document.pdf (последнее посещение — 24 мая 2016 г.)

50 NPT/conf.2015/MC.I/SB.1/CRP.1 (Subsidiary Body 1: Draft substantive elements) http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2015/documents/SBI–CRP1.pdf (последнее посещение — 24 мая 2016 г.)

51 SIPRI NPT-2015 daily reports, https://www.sipri.org/research/armaments-and-disarmament/nuclear-weapons/npt-review/2015/daily (последнее посещение — 1 июня 2016 г.)

52 NPT/CONF.2015/DEC.2. Decision on subsidiary bodies. 2015 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons. New York, 4 May 2015, http://www.un.org/en/conf/npt/2015/pdf/NPT-CONF2015-DEC.2.pdf (последнее посещение — 24 мая 2016 г.)

53 W. C. Potter. The Unfulfilled Promise of the 2015 NPT Review Conference. P. 157.

54 http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2015/documents/SBI-CRP1-Rev1.pdf

55 Например, совместное заявление Коалиции за новую повестку дня, 14 мая 2015 г. (http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2015/statements/14May_NAC_MCI.pdf)

56 SIPRI NPT-2015 daily reports. New York, 14 May 2015. (https://www.sipri.org/research/armaments-and-disarmament/nuclear-weapons/npt-review/2015/npt_report_day14)

57 2015 Review Conference of the Parties I to the Treaty on the Non-Proliferation of Nuclear Weapons. Draft Final Document. New York, 27 April–22 May 2015, http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2015/documents/DraftFinalDocument.pdf (последнее посещение — 24 мая 2016 г.)

58 Statements to the 2015 NPT Review Conference. Austria. 12 May 2015, http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2015/statements/12May_Austria_SBI.pdf (последнее посещение — 24 мая 2016 г.)

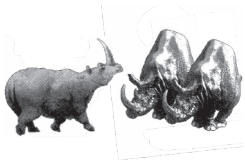
59 On Recommendation of First Committee, General Assembly Adopts More than 50 Drafts, Including New One on 'Ethical Imperatives' for Nuclear Disarmament. Seventieth Session, 67th Meeting (AM). General Assembly. Meetings Coverage. 7 December 2015 (http://www.un.org/press/en/2015/ga11735.doc.htm)

60 A/C.1/70/L.38. Explanation of vote by New Zealand, http://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com15/eov/L38_NZ.pdf (последнее посещение — 24 мая 2016 г.)

61 70ème Session de l'Assemblée générale Première Commission Point 97 Humanitarian Pledge New York, le xx novembre 2015 Explication de vote de la Suisse, http://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com15/eov/L38_Switzerland-Sweden.pdf (последнее посещение — 24 мая 2016 г.)

62 2015 Review Conference of the Treaty on Non-Proliferation of Nuclear Weapons: New York, 27 April — 22 May 2015. General Debate. Statement by the United Kingdom, http://reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2015/statements/27April_UK.pdf (последнее посещение — 24 мая 2016 г.)

63 В 1996 г. Международный Суд ООН рассматривал вопрос о законности угрозы применения или применения ядерного оружия и о применимости принципов и норм МГП в отношении ядерного оружия. Он постановил, что в целом применение или угроза применения ядерного оружия противоречили бы нормам международного гуманитарного права.



ВЫСОКОТЕХНОЛОГИЧНАЯ ПРЕСТУПНОСТЬ: НОВЫЕ ВЫЗОВЫ ДЛЯ ОБЩЕСТВА, ГОСУДАРСТВА И БИЗНЕСА

Экспоненциальное развитие и распространение интернет-технологий привело к возникновению нового феномена — высокотехнологичной преступности. В интернете совершаются как традиционные правонарушения — мошенничество, шантаж, кражи — так и преступления нового типа, противодействие которым зачастую выходит за рамки возможностей силовых структур. Интернет вещей, блокчейн, атрибуция — в лексикон полицейских и судей постепенно входят новые термины и понятия. Без тесного взаимодействия государства и общества, законодательной и исполнительной власти, а также скоординированных усилий всего мирового сообщества противодействовать новым вызовам вряд ли удастся.

Что такое высокотехнологичная преступность и как с ней бороться, обсуждалось на заседании круглого стола, проведенного Комитетом гражданских инициатив совместно с ПИР-Центром. Модератором дискуссии выступил председатель КГИ Алексей Кудрин. В мероприятии приняли участие члены Рабочей группы по международной информационной безопасности и глобальному управлению интернетом при Экспертном совете ПИР-Центра и эксперты КГИ: директор некоммерческого партнерства Информационная культура *Иван Бегтин, председатель Общественного Совета при МВД России Анатолий Кучерена, эксперт расширенной рабочей группы по реформированию МВД Елена Ларина, бизнес-консультант по информационной безопасности компании Cisco Алексей Лукацкий, советник министра внутренних дел Владимир Овчинский, генеральный директор компании Group-IB Илья Сачков, вице-президент по взаимодействию с заинтересованными сторонами в России, странах СНГ и Восточной Европы Корпорации Интернета по присвоению имен и номеров (ICANN) Михаил Якушев, руководитель стратегических проектов в России, странах Закавказья и Средней Азии* Лаборатории Касперского *Андрей Ярных и эксперт по вопросам управления бизнес-системами Алексей Яцына.*

АЛЕКСЕЙ КУДРИН: Наша сегодняшняя тема — *Высокотехнологичная преступность: новые вызовы для общества, государства и бизнеса*. Проблема преступлений с использованием высоких технологий, которую мы будем сегодня обсуждать, относительно нова, и государство не успевает на нее реагировать, правоохранительные органы и спецслужбы не готовы иметь дело с преступлениями

нового типа. Именно об этом и сегодня и поговорим. Наш первый докладчик — Илья Сачков, генеральный директор Group-IB, фирмы, занимающейся в том числе расследованием киберпреступлений, член Рабочей группы по международной информационной безопасности и глобальному управлению интернетом при Экспертном совете ПИР-Центра.

ИЛЬЯ САЧКОВ: Постараюсь очень кратко рассказать о трендах развития высокотехнологичной преступности, которые мы видим на территории Российской Федерации. Часть нашей работы — экспертно-криминалистическая деятельность по сопровождению особо сложных и резонансных уголовных дел против компьютерной преступности.

Самая большая проблема компьютерной преступности состоит в том, что общество в целом не совсем понимает, о чем идет речь, и не совсем верит в реальность высокотехнологичных правонарушений.

Есть потрясающий пример мошенничества против Московской биржи. В апреле мошенники от лица *Энергобанка* отправили на биржу заявку в размере 300 млн долл. и получили деньги. Банк обратился к нам за помощью, мы провели компьютерную криминалистическую экспертизу и нашли на компьютере, на котором находился брокерский терминал, вредоносное программное обеспечение. После этого мы получили запрос из Центрального банка России с требованием предоставить все материалы по делу, которые, между прочим, являются тайной следствия, что мы и ответили Центральному банку. В ответ получили штраф в 500 тыс. рублей за нарушение закона об инсайдерской деятельности. В итоге Центральный банк не верит в то, что заявку мог отправить вирус, в отношении *Энергобанка* ведется проверка, мы заплатили штраф 500 тыс. рублей, уголовное дело продолжается.

Когда мы говорим о компьютерной преступности, важно понимать, что общество знает лишь о верхушке айсберга. Возьмем пример *кардинга* — воровства денег с кредитных карточек — несложное и очень популярное преступление. Преступники пользуются специализированными интернет-магазинами, в которых продаются *дампы* кредитных карточек — копии магнитной полосы и PIN-коды, то есть то, что необходимо, чтобы снимать деньги с карточки. Набор дампов стоит порядка 10 долларов. В одном магазине продается около 5 млн валидных кредитных карточек. Принято думать, что теневой интернет — это что-то очень технически сложное, зеленые буквы на черном экране. Ничего подобного. У таких магазинов очень удобный интерфейс, они вообще мало чем (кроме товара) отличаются от обычных интернет-магазинов.

Когда правоохранительные органы видят подобные сайты в интернете, они пытаются их блокировать. Проблема в том, что, закрывая что-то в интернете без понимания, какие есть тенденции, с которыми надо бороться, правоохранители просто запускают гонку вооружений: поверьте, люди, которые создают кардинговые магазины, из-за того что закрыли один веб-сайт или ликвидировали домен, который стоит 20 долларов, не расстроятся и не скажут «пора, наверное, отходить от дел». Напротив, они станут умнее, хитрее, используют новые средства анонимного доступа.

Это, кстати, уже произошло с торговлей наркотикам. Изначально сайты, на которых их продавали, находились в обычных доменных зонах, и идентифицировать продавцов было достаточно легко. После принятия закона о блокировке их начали закрывать тысячами, а наркоторговцы ушли в теневой интернет. Но проблема никуда не делась, преступники стали изобретательнее, и теперь есть случаи (ФСКН, естественно, в курсе), когда наркотики заказывают с доставкой на дом через *Почту России*.

Сталкиваясь с преступлениями в интернете, очень важно анализировать всю цепочку. В случае с кардингом надо начинать с вопроса, каким образом похитили данные 5 миллионов карточек? В магазине, о котором я говорил, продавали дампы, полученные с зараженных терминалов в двух американских торговых сетях, *Target* и *Home Depot:* в одной похитили данные 70 млн карточек, в другой — 56 млн. Это очень важная информация, ведь если мы знаем точку компрометации, понятно, что делать дальше: любой человек, который был в этих торговых сетях в определенный промежуток времени, должен свою карточку заблокировать.

Также важно понимать, что владелец сайта, торгующего дампами, на комиссии с покупок заработал 6 млн долларов и в случае юридического преследования обеспечит себе первоклассную юридическую защиту. Кстати, появляется целый класс адвокатов, которые специализируются на защите компьютерных преступников, потому что это достаточно просто и очень прибыльно.

Что происходит сейчас на рынке компьютерной преступности, какие цели у злоумышленников? В первую очередь, деньги. Есть случаи, когда компьютерные преступники охотятся за информацией, но это сотые доли процента. Благодаря развитию платежных систем, интернет-банкинга для физических и юридических лиц процветает и воровство денег в платежных системах. Технически это относительно несложно, а если добавить в уравнение сверхприбыль и чувство безнаказанности, получается привлекательная картина. Надо иметь в виду, что компьютерный преступник не вызывает в обществе негативных эмоций — в отличие, например, от наркодилера.

Кроме того, законодательство не успевает за развитием высокотехнологичных преступлений, в нем много лакун. Компьютерные преступления можно за одну секунду совершить с территории одной страны через территорию другой страны в ста странах одновременно. Поэтому, несмотря на то что государство, общество, бизнес, люди тратят на информационную безопасность с каждым годом все больше, атак меньше не становится.

Отношение общества — это отдельный вопрос. Приведу старый, но показательный пример. Господин Аникин из Новосибирска в составе организованной преступной группы украл 9,5 млн долларов. В этот же год господин Блинников взломал щит на Садовом кольце и крутил там порнографию, а господин Гаврилов украл у своей соседки с дачного участка два куста роз и два куста лилий. Приговоры: Аникин — пять лет условно, Блинников — шесть лет колонии, Гаврилов — два года строгого режима.

В сознании людей кража электронных денег — это какая-то игра. В день оглашения приговора Аникину *Первый канал* выпустил новость про *талантливого моло-*

дого программиста, обхитрившего службу безопасности банка. Мы мониторим хакерские форумы, так вот, в этот день количество регистраций на них увеличилось на 400%.

Появляется целое поколение преступников, которые не обладают специальными знаниями, а используют готовые, понятные инструменты. Они, как правило, очень молоды, большинству нет 30 лет. Программы, которыми они пользуются, предельно просты и, что самое поразительное, имеют лицензионную политику, а создающие их злоумышленники тратят время на борьбу с пиратством и на защиту своей собственности. Эти сайты предлагают круглосуточную техподдержку на нескольких языках, которой могут позавидовать некоторые производители программного обеспечения. Работа с ними не требует никаких технических знаний. Есть, конечно, в составе преступных групп очень умные люди, но есть и те, у которых IQ в районе 40–60.

Члены преступной группы зачастую живут в разных регионах не только России, но и мира, что создает массу юридических проблем. Если преступная группа находится в трех — четырех странах, то о расследовании и кооперации правоохранительных органов можно забыть. Сейчас многие люди, которые в России подпадают под подозрение в совершении компьютерных преступлений, уезжают на Украину, а многие хакеры из Украины приезжают в Россию. Русские с территории Украины воруют деньги в российских банках, украинцы с территории России воруют деньги в украинских банках, и все остаются безнаказанными. Политика используется для того, чтобы скрывать компьютерные преступления. Есть и другие факторы. Кроме технической возможности заразить компьютеры, преступники ищут страны, где нет проблем с обналичкой. В России с этим все относительно просто, поэтому компьютерная преступность процветает. Решение вопроса с обналичкой нанесло бы очень эффективный удар по компьютерной преступности.

Мобильные устройства. Благодаря тому, что Android занял 80% мирового рынка устройств и телефоны на базе Android продаются за 20 долларов, идет огромное количество разработок вредоносного ПО под мобильные устройства. С телефоном можно сделать все, что угодно, начиная от кражи денежных средств и кончая прослушкой телефона, когда он просто лежит на столе. Стоимость заражения телефонов на черном рынке — приблизительно 100–200 долларов за тысячу аппаратов. Мы регулярно с 2006 г. выпускаем памятки по компьютерной гигиене, но есть ощущение, что их читают только наши сотрудники. В прошлом году мы выходили с инициативой в Министерство образования, предлагали часть часов ОБЖ выделять на правила компьютерной гигиены. К сожалению, не получилось. В то же время в США дети 6–8 лет изучают основы компьютерной грамотности. В 6–8 лет они знают, что такое фишинг, кардинг. Я считаю, что то же самое необходимо в России, потому что вчерашние школьники становятся сотрудниками предприятий и, не зная базовых вещей, становятся легкой мишенью для атак.

АЛЕКСЕЙ КУДРИН: А кроме вашей компании кто-то в России занимается похожей экспертизой?

ИЛЬЯ САЧКОВ: *Лаборатория Касперского* и мы.

АНДРЕЙ ЯРНЫХ: *Лаборатория Касперского* занимается подобными расследованиями, но в значительно меньшей степени, оперативно-разыскные мероприятия, в основном, проводятся правоохранительными органами.

Мы своей основной задачей видим выпуск программного обеспечения для защиты пользователей, а также стараемся максимально широко их информировать и повышать компьютерную грамотность. Несмотря на то, что все бесконечно повторяют, что интернет является агрессивной средой, пользователи зачастую проявляют беспечность и становятся жертвами злоумышленников.

Это несложно, даже в основе создания ботнет-сетей лежит обычное заражение компьютера троянской программой, после чего компьютеры объединяются в ботнет-сети, и уже под управлением злоумышленников происходят атаки на инфраструктуру, кражи денег, формирование финансовых баз украденных данных. То есть в основе проблемы — элементарная безграмотность пользователей.

АЛЕКСЕЙ КУДРИН: Какой вывод мы можем сделать? Нужно обучать детей в школах, создавать дополнительные системы защиты и выявления преступлений?

ИЛЬЯ САЧКОВ: Российские вузы не выпускают специалистов по цифровой криминалистике. У нас практически все самоучки. Мы проводили олимпиаду по компьютерной криминалистике, в ней участвовало 50 тысяч студентов, задания решили два человека. При этом по уровню сложности это был восьмой класс математической олимпиады.

Кроме того, надо развивать законодательство и обучать следователей и судей. Следователей, которые могут вести серьезные дела, в России можно пересчитать по пальцам. Серьезные сложности с судьями: человек, который выносит решение по компьютерному преступлению, должен понимать специфику.

Еще одна фундаментальная вещь. Интернет — глобальный феномен, требующий тесного взаимодействия между правоохранительными органами разных стран, а если законодательство не гармонизировано, общение между правоохранительными органами занимает не секунды, а часы, дни, а чаще всего месяцы и годы, при том что компьютерные преступники общаются в режиме реального времени, совершают преступления буквально за несколько секунд.

АЛЕКСЕЙ КУДРИН: Получается, нужна международная компьютерная разведка?

ИЛЬЯ САЧКОВ: Необходимо выработать единую конвенцию по борьбе с компьютерными преступлениями на базе ООН. Сейчас есть только Европейская конвенция, к которой Россия не присоединяется, потому что в ней есть статья, которая ущемляет наши национальные интересы. Это логично, но в результате уже много лет реального сотрудничества между нашими правоохранительными органами нет.

Кроме того, было бы полезно, чтобы в отделениях полиции были шаблоны заявлений по компьютерным преступлениям. Когда человек, ставший жертвой компьютерного преступления, приходит в районное отделение полиции и пытается

подать заявление, он встречает непонимание. У полиции нет единых баз данных по расследуемым преступлениям, поэтому бывает, что в разных регионах России ведется одно и то же уголовное дело и следователи не подозревают, что охотятся на одну и ту же преступную группу.

В правоохранительных органах работают очень серьезные профессионалы, но их категорически недостаточно. Сейчас они могут работать только против самых крупных организованных групп, но мелкими преступлениями, например кражами 300 рублей с мобильного телефона, никто не будет заниматься.

АЛЕКСЕЙ КУДРИН: Наш следующий докладчик — Иван Бегтин.

ИВАН БЕГТИН: На протяжении многих лет в России неэффективное использование бюджетных средств мешало государству внедрять давно разработанные информационные технологии. Теперь на помощь чиновникам могут прийти бизнес-круги, которые могут поделиться с ними своими наработками.

Однако государство должно активно стимулировать диалог с гражданами по вопросам информационной политики и формировать институты доверия. Граждане должны, например, иметь право требовать установки видеокамеры на перекрестке рядом со своим домом, где, по их сведениям, совершаются преступления, требовать от правоохранительных органов, чтобы те направляли патрульные машины в определенные районы, пользуясь необходимой информацией. Я давно говорю о том, как важно с правовой точки зрения обеспечить открытость данных, кроме разве что имеющих совсем личный характер. На мой взгляд, это должно быть внедрено в самые краткие сроки: от полугода до ближайших трех лет. Обратной стороной медали или фактором сдерживания распространения этих технологий является готовность российских органов внутренних дел вторгаться в личную жизнь граждан.

Современный уровень технологического развития позволяет хранить данные пользователей практически вечно. Когда в Германии пользователи Facebook на законных основаниях запрашивали свои персональные данные, им предоставляли все, что они когда-либо размещали, включая удаленный контент. Если люди старшего поколения прожили часть жизни без активного использования интернета и соцсетей, то все подробности жизни наших детей и внуков можно будет обнаружить и использовать в тех или иных целях.

В Великобритании и США, например, общественность начинает выражать недовольство тем, какой объем данных собирает полиция. В ближайшие 10–20 лет эта тенденция будет только усиливаться. Представьте себе, что у каждого полицейского будет при себе камера и данные, записанные с ее помощью, будут храниться вечно. Кроме того, камерами будут оснащены дроны самых разных типов. В итоге каждое преступление будет зафиксировано на видео, причем с нескольких ракурсов. Человек, совершивший преступление, будет находиться под постоянным наблюдением, причем с помощью не только камер, но и датчиков, закрепленных на его теле. С технологической точки зрения это осуществимо уже сейчас, просто в большинстве стран общество к такому не готово. Поэтому когда я слышу про неудачи внедрения автоматизации в МВД, я испытываю противоречивые чувства.

АЛЕКСЕЙ КУДРИН: Мне кажется, что США и другие страны с высоким уровнем развития компьютерных технологий в этом плане опережают нас лет на 15. Возможно, и вопросы использования и обработки этих данных, вмешательства в частную жизнь там продуманы более тщательно?

ИВАН БЕГТИН: По моим ощущениям, США в настоящее время — это гибрид тоталитарного и демократического государства. Просто, когда в распоряжении государства появляется эффективный инструмент, каким бы добрым, либеральным, демократичным оно ни было, ему очень трудно избежать соблазна им воспользоваться. А инструмент этот очень удобен для осуществления тотального контроля.

Количество информации в интернете не безгранично. В сутки человек способен создавать ограниченный объем контента, поэтому рано или поздно можно будет отследить действия каждого человека, что, собственно, и происходит. Именно поэтому АНБ стало подвергаться огромному давлению со стороны правозащитных организаций еще до того, как начало осуществлять массовую слежку. Можно даже вспомнить случай, когда американская правозащитная организация *Electronic Frontier Foundation* обнаружила, что некоторые модели принтеров оставляют специальную маркировку, позволяющую узнать, где был напечатан тот или иной документ.

АЛЕКСЕЙ КУДРИН: В Советском Союзе КГБ вел учет всех пишущих машинок, чтобы иметь возможность выяснить, на чем печатается запрещенная литература.

ИВАН БЕГТИН: Это разные традиции. У нас чаще всего прибегают к запретам, у них все разрешено, но находится под наблюдением. Мне трудно сказать, какой вариант хуже. Доподлинно известно, что большая часть операционных систем — Android, последние операционные системы от Microsoft — следят за пользователями. Появление систем в духе *Большого брата* тесно связано с вопросами компьютерной грамотности и культуры как рядовых граждан, так и государственных органов. Хотелось бы, чтобы при внедрении любой новой системы, которая затрагивает наши права и свободы, существовали какие-то площадки для диалога, где вырабатывалось бы взаимопонимание и создавались механизмы ограничения и контроля над теми людьми, которые этими системами управляют, потому что злоупотребления обязательно будут.

АЛЕКСЕЙ КУДРИН: А как бороться с *Большим братом*?

ИВАН БЕГТИН: В этой борьбе хорошо помогает коррупция в правоохранительных органах, но этого я советовать не стану. Поэтому, наверное, власти нужно повышать осведомленность граждан и вступать с ними в диалог.

АЛЕКСЕЙ КУДРИН: Следующий докладчик — Владимир Овчинский.

ВЛАДИМИР ОВЧИНСКИЙ: Сегодня мы говорим о полиции и преступности будущего. В нашем обществе обсуждение этих проблем с политической, социальной и криминологической точек зрения только начинается. Уже примерно пятнадцать лет правоохранительные органы ведут работу по предупреждению преступлений, по борьбе с компьютерной преступностью, с новыми типами преступлений,

возникающими на базе технологических инноваций. Но фактически обсуждения последствий внедрения новых технологий еще не было.

В этом году были опубликованы две очень интересные книги по этой теме — *Будущие преступления* М. Гудмана, бывшего старшего советника Интерпола, который сейчас консультирует один из проектов Google. Еще одна интересная работа — *Будущее насилия* Б. Уиттиса и Г. Блум, которая посвящена тем же вопросам. Так вот, в книге *Будущее насилия* приводятся результаты исследования Стюарта Бейкера, который до недавнего времени был руководителем Департамента политики министерства внутренней безопасности США. Этот ученый с помощью компьютерного анализа, в основу которого было положено два параметра — снижение цены коммерческого использования новой технологии и масштаб ее распространения — исследовал взаимосвязь применения новых технологий и изменения уровня преступности за последние 120 лет и сделал прогноз на ближайшее будущее. Он доказал, что в ближайшие годы мир захлестнет волна высокотехнологической преступности, с которой действующая государственная, банковская система и гражданское общество не смогут справляться. Многие либерально настроенные американские и европейские ученые приходят к неожиданному для них самих выводу о том, что, чтобы противостоять этой волне компьютерной преступности (и речь идет не просто о хищении банковских средств, но о терроризме и других формах насилия), надо будет отказаться от многих привычных ценностей, поступиться своими правами, даже в ряде случаев допустить правоохранительные органы в свою личную жизнь.

Вы знаете, что после атак 11 сентября на *башни-близнецы* в США был принят *Патриотический акт*, сейчас во Франции принят целый комплекс законодательных изменений, которые тоже касаются контроля за сетевым пространством, в Великобритании ужесточено законодательство и расширены права правоохранительных органов в этом плане. Мы должны быть готовы к тому, что придется чем-то поступиться. Ведь кибератака может закончиться и военным нападением, взрывом ядерной станции, взрывом энергосетей, выводом из строя всей технологической инфраструктуры.

Теперь о масштабах. Дело в том, что новая преступность, как раковая опухоль, уже успела пустить метастазы. Я приведу данные, которые были озвучены на 13-м Конгрессе ООН по предупреждению преступности и уголовному правосудию, который проходил в апреле этого года в Катаре. ООН провела исследования по виктимизации в 21 стране, и результаты такие, что если обычный уровень виктимизации, связанный с кражами, грабежами, разбоями, преступлениями против личностями — традиционной преступностью — равен от 1 до 5%, то виктимизация, связанная с киберпреступностью — мошенничеством с банковскими картами, похищением личных данных и прочим — составляет в этих странах до 17–18%.

То есть уже сейчас уровень виктимизации, число потерпевших почти в 4 раза выше, чем при традиционной преступности. При этом мы должны понимать, что традиционная преступность никуда не уйдет. Продолжаются кризисные явления в мировой экономике, продолжаются волны миграции беженцев. Любые потоки вынужденной миграции сами по себе всегда порождают преступность. Сейчас эти потоки идут и через Европу, и через евразийское пространство. Никуда

не уйдет обычное бытовое насилие, которое дает 80–90% всех убийств и нанесений тяжкого вреда здоровью. Правоохранительным органам придется с этим иметь дело. И при этом мир накрывает та волна, о которой я уже говорил, волна совершенно новой высокотехнологичной преступности.

Возникают новые формы преступности, а правоохранительная система, банковская система и общество в целом еще обращены в прошлое. Это проявляется во всем — в подготовке кадров, в выработке мер противодействия, в материально-техническом и кадровом обеспечении. На основании решения Совета Безопасности за последние три года МВД с огромным трудом на треть увеличило численность экспертов, которые занимаются киберпреступностью. Но этого совершенно не достаточно. На сегодняшний день эксперты загружены настолько, что расследования по киберпреступлениям длятся от одного года и дольше. Такая загруженность на 80–90% превышает установленные нормативы.

У государства никогда не будет достаточно средств для борьбы с новыми видами преступлений. Такие выводы делаются в последнем докладе Европола, опубликованном летом этого года. Европейцы прямо указывают, что государство будет вынуждено делегировать некоторые свои функции коммерческим структурам. Некоторые детективные функции, все, что касается экспертизы, защиты, предотвращения преступлений. При этом важно избежать коммерциализации правоохранительной деятельности.

Допустим, существует известное соглашение МВД с Ассоциацией российских банков 1995 г. Сейчас необходимо составить дополнительный протокол к этому соглашению, где должны быть четко регламентированы все действия банковского сообщества, скажем, по обмену информацией и созданию единого банка данных нападений, какие уже созданы в США, Китае, Великобритании. В Великобритании за него отвечают органы МВД. Может быть, возможно создание какого-то агентства, которое будет заниматься такими расследованиями и проведением экспертиз в рамках закона *О частной детективной и охранной деятельности*. Но на это нужны деньги. Банковское сообщество должно решить этот вопрос, потому что возлагать эти обязанности только на экспертные подразделения МВД и ФСБ нереально в условиях дефицита денег и той военно-политической ситуации, в которой мы находимся, и, думаю, что еще целый ряд лет будем находиться.

И, конечно, нужно укреплять международное сотрудничество. Я хотел бы немного поправить Илью Сачкова: ведется большая работа по международному сотрудничеству в рамках Интерпола. В этом году в Сингапуре был создан центр по борьбе с киберпреступностью, его открывали совместно Интерпол и Европол. Россия активно в этом участвует, идет обмен информацией в рамках Интерпола. Само участие в организации предполагает, что обмен оперативными данными должен происходить в режиме реального времени, без сложных согласований. Поэтому нужно расширять центральное бюро Интерпола в России, ведь там тоже произошло сокращение — вы знаете, недавно все структуры МВД были сокращены на 10–15%. Сейчас мы сталкиваемся с парадоксом, когда полиция сокращается, а объемы борьбы и с традиционной, и нетрадиционной, новой преступностью все время возрастают. Из такого положения надо выходить. Первый

путь — прекратить сокращения. Второй — делегировать часть функций коммерческим структурам.

АЛЕКСЕЙ КУДРИН: Но ведь в тех странах, которые вы ставите в пример, численность полиции на сто тысяч жителей значительно меньше, чем у нас.

ВЛАДИМИР ОВЧИНСКИЙ: Даже при имеющемся уровне учета преступлений число убийств на сто тысяч жителей в России где-то в 6–8 раз превосходит этот показатель в средней европейской стране. И тенденций к снижению не видно. Поэтому сокращать полицию никак нельзя.

АЛЕКСЕЙ КУДРИН: Какие структуры государственной власти занимаются этой проблемой концептуально?

ВЛАДИМИР ОВЧИНСКИЙ: При Совете Безопасности есть комиссия по информационной безопасности, и распоряжения об увеличении количества экспертов, приобретении новых аппаратных комплексов для экспертиз, получении новой техники для наших оперативных подразделений были приняты как раз на основе последних решений Совбеза.

АЛЕКСЕЙ КУДРИН: Спасибо. Слово Елене Лариной.

ЕЛЕНА ЛАРИНА: Хочу кратко обратиться к зарубежному опыту взаимодействия между государством (в данном случае полицией), обществом и бизнесом. Начну с опыта США. Как здесь уже правильно отмечали, их цифровое настоящее — это наше ближайшее будущее, поэтому, изучив то, что у них происходит сегодня, мы можем почерпнуть полезный опыт и в некоторых местах подстраховаться, чтобы избежать в будущем повторения их ошибок.

Сейчас в Америке и других технологически продвинутых странах практически нет различия между виртуальностью и реальностью. В наш обиход пришли такие термины, как *интернет вещей*, *интернет людей*, уже сейчас появились *интернет игрушек*, *интернет денег* и такой всеобъемлющий термин, как *интернет всего*. Это значит, что в самом ближайшем будущем практически все будет подключено к интернету, включая устройства и предметы, которые человек носит с собой и на себе. Возникнет единая цифровая среда.

Кроме того, существует проблема разрыва поколений. Современная молодежь с младенчества умеет обращаться с новыми технологиями, у них есть знания и опыт, который наращивается буквально с каждым днем. Людям старшего поколения, которые осваивали компьютеры уже в зрелом возрасте, сложнее адаптироваться в этом быстро меняющемся мире.

К чему все это ведет? По данным полиции крупных американских городов, раскрываемость компьютерных преступлений в настоящий момент в пять-шесть раз ниже, чем традиционных преступлений. Если при традиционных видах преступлений потерпевшие обращаются в органы правопорядка в 80–90% случаев, то при компьютерных преступлениях обращаются где-то в 15–20% случаев. Соответственно, пока показатели раскрываемости низкие, для киберпреступника соотношение потенциальной выгоды от преступления и риска быть пойманным и наказанным значительно меньше, чем при традиционной преступности. Скажу боль-

ше: мы все еще делим преступность на компьютерную и традиционную, в то время как в ближайшем будущем, учитывая, что интернет подключен ко всему, практически любой преступник, за исключением самых отпетых маргиналов, будет компьютерным преступником, и почти вся противозаконная деятельность перейдет именно в эту плоскость.

В условиях такого расцвета высокотехнологичной преступности большое число западных стран изменило свою стратегию и тактику борьбы с ней и ее профилактики. С принятием в США в 2015 г. Стратегии национальной безопасности, Стратегии кибербезопасности, а также с внесением некоторых изменений в законодательство ряда штатов подход к киберпреступности в Америке изменился.

Суть изменений в следующем. Предполагается гораздо более широкое участие общества и бизнеса в борьбе с киберпреступностью. На сегодняшний день федеральным органам власти, включая ФБР, разрешено создавать различные государственно-частные партнерства (ГЧП). То есть за государством остаются системообразующие функции, а все, что менее важно, отдается на откуп бизнесу. При этом такие партнерства создаются не только с крупными корпорациями, но и с более мелкими динамично развивающимися компаниями, иногда даже со стартапами.

В нашей стране на сегодняшний день тоже заложены законодательные основы подобных процессов. Я имею в виду закон ФЗ-224 от 13 июля 2015 г. *О государственно-частном и территориально-частном партнерстве*, который вступил в силу с 1 января 2016 г. К сожалению, пока действие этого закона распространяется только на материальные активы, то есть с помощью механизма ГЧП можно строить дороги, но нельзя оказывать услуги по обеспечению безопасности.

Отдельная тема — взаимодействие государства, бизнеса и общества. В Америке, например, в отдельных штатах на смену полицейским участкам приходят выборные шерифы. В Калифорнии власти могут привлекать к борьбе с преступностью своеобразные высокотехнологичные ЧОПы. Конечно, в России этот опыт сейчас неприменим, потому что у нас нет ни законодательной базы, ни соответствующих традиций, но интересно проследить, в каком направлении развиваются страны мира.

Австралийское правительство устанавливает налоговые вычеты для компаний, которые покупают мощное сертифицированное программное обеспечение для собственной информационной безопасности. Таким образом они побуждают предприятия бороться с киберпреступлениями и предотвращать их. Кроме того, власти Австралии компенсируют частным лицам половину затрат на покупку этих защитных программ.

Очень интересен опыт Голландии. Чтобы противодействовать киберпреступности, нужны современные инструменты и мощное техническое оснащение, приходится закупать ПО и оборудование. Более десяти лет назад в Нидерландах было принято решение о создании центра по расходованию бюджетных средств всех уровней. Комиссия, которая принимает от организаций заявки на участие в тендере, должна информировать общественность о его условиях и о компаниях,

которые подали заявки на участие. Эта информация публикуется в определенной базе, доступной для любого гражданина. В ней можно найти информацию о компании, которая участвует в тендере, о ее учредителях, о том, есть ли у нее какие-то проблемы с правоохранительными и судебными органами. Более того, там даже есть раздел, где каждый гражданин страны может разместить известные ему негативные сведения о той или иной компании. Не принимаются только анонимные сообщения, кроме того, каждый несет за предоставленные данные ответственность вплоть до уголовной.

Таким образом, компании, у которых есть какие-то проблемы с правоохранительными, судебными органами или даже общественными организациями, не могут стать победителями тендера. В результате, если раньше до трети тендеров выигрывалось компаниями, так или иначе связанными с криминалом, то сейчас абсолютно во всех сферах конкурсы проводятся совершенно прозрачно, и ни одна компания, к которой есть претензии даже у гражданского общества, не получила тендер. Использовать этот опыт в России было бы очень полезно.

АЛЕКСЕЙ КУДРИН: Наш следующий докладчик — Анатолий Кучерена.

АНАТОЛИЙ КУЧЕРЕНА: Тема, которую мы затронули, периодически возникает у нас в обществе, особенно в контексте вторжений в частную жизнь. Владимир Овчинский сказал о том, что мы вынуждены будем делиться информацией или предоставлять возможность вторжения в нашу личную жизнь. Я категорически с этим не согласен, потому что считаю, что сейчас давать возможность такого вторжения нельзя, нужно понимать, кому мы даем на это право и как этой информацией могут воспользоваться те или иные структуры.

Из общения с Эдвардом Сноуденом я понял, что мы должны обучать население, проводить информационно-просветительскую работу. Необходимо помнить, что, пользуясь любыми программами или устройствами, мы в первую очередь должны думать о том, как обезопасить себя.

Универсальной технологии, которая могла бы защитить нас с вами, не существует, и вряд ли она появится в ближайшее время. При всей осторожности полностью защитить нашу информацию, нашу частную жизнь на сегодняшний день невозможно.

Существуют специалисты, которые предлагают разные виды защиты, но все омрачает недоверие к правоохранительным органам в обществе и высокий уровень коррупции. Пример тому — *вбросы* закрытой информации по уголовным делам, которые происходят в интернете. Во многих случаях это делается для того, чтобы опорочить или оскорбить человека. Создать имидж сегодня проще простого, в том числе используя новые технологии и утечки информации, хищение данных, например из смартфонов. Поэтому позаботиться о том, как себя защитить, должны мы сами.

Кроме того, необходимо проводить работу среди молодежи. Было правильно сказано, что информация, которая появляется в интернете, остается там навечно. Сегодня она никому не нужна, а завтра может быть использована против человека, чтобы оказать на него давление.

Принципиально важно, чтобы каждый сотрудник полиции был профессионально пригоден к той работе, которой он занимается. Мы понимаем и знаем имеющиеся трудности. К сожалению, надо признать, что сегодня сотрудник полиции вынужден больше 50% своего рабочего времени заниматься отчетностью, ему не хватает времени на повышение профессиональной квалификации, а это необходимо, когда речь идет о борьбе с высокотехнологичными преступлениями.

АЛЕКСЕЙ КУДРИН: Следующий докладчик — Алексей Лукацкий.

АЛЕКСЕЙ ЛУКАЦКИЙ: Хотел бы сказать несколько слов по поводу культуры информационной безопасности. Два года назад при Совете Безопасности была сформирована рабочая группа по разработке документа под названием *Основы государственной политики в области формирования культуры информационной безопасности*. В проект этого документа было включено все то, о чем сегодня упоминали. Это и введение различных образовательных дисциплин, начиная с самого раннего возраста, и обучение преподавателей и воспитателей в детских садах, школах и вузах, и просвещение в вопросах информационной безопасности и грамотности. К сожалению, финальный вариант документа пока так и не увидел свет, и те важные вещи, о которых сегодня говорили, пока не нашли отражения в основополагающем документе, которым руководствовалось бы государство.

Все это время мы говорили о традиционных преступлениях, которые совершаются с помощью высоких технологий, таких как кража денег. Это неприятно, но не смертельно. А бывают киберпреступления, которые могут привести к смерти человека, например атаки на подключенные к интернету кардиостимуляторы, инсулиновые помпы, специальное медицинское оборудование для больных астмой, автомобили, которые практически все оснащены достаточно серьезной электроникой. Прецеденты уже были.

Необходимо предпринять серьезные усилия на уровне взаимодействия различных органов исполнительной и законодательной власти для того, чтобы при выпуске такой продукции на рынок она оценивалась не только с точки зрения медицинской или промышленной безопасности, но и с точки зрения безопасности информационной. Внимание этому сегодня не уделяется по вполне понятным причинам — это совершенно новые угрозы, с ними мало кто сталкивался, поэтому никто не закладывает их в будущие модели угроз и существующие нормативные документы. Через несколько лет эти технологии прочно войдут в нашу жизнь, и если сейчас, скажем, сантехника или бытовая техника, подключенная к интернету, — нечто из области фантастики, то в будущем все будет гораздо серьезнее, и если сейчас к этому не готовиться, то через несколько лет СМИ могут начать сообщать о киберпреступлениях, повлекших человеческие смерти или нанесение вреда здоровью людей.

АЛЕКСЕЙ КУДРИН: Слово Михаилу Якушеву.

МИХАИЛ ЯКУШЕВ: То, что я сейчас скажу, я говорю регулярно уже многие годы: ситуация медленно меняется к лучшему, но, к сожалению, преступность нас все равно обгоняет. Значит, проблема комплексная и отношение к ней должно быть именно комплексное. Мне не совсем понятно, почему тут упоминаются только МВД и полиция, как раз там медленно, но стабильно происходят изменения

к лучшему, в то время как в других правоохранительных органах проблема борьбы с киберпреступностью фактически не решается никак. Поэтому, если мы говорим об улучшении работы правоохранительных органов, то нельзя ограничиваться только МВД или Федеральной службой безопасности, где есть специалисты, адекватно понимающие ситуацию, — нужно брать шире.

Что касается законодательства, решение правовых вопросов очень важно — это первый компонент комплексного подхода к проблеме. На экспертном уровне вопросы, связанные с разработкой законодательства, не поднимаются, то есть опыт тех же Сачкова и Касперского, как мы видим, не сильно используется. В связи с этим, когда речь шла о международном опыте, упоминалась Будапештская конвенция. Госорганы поддерживают неучастие в ней России, эксперты занимают противоположную позицию. Действительно, Россия в этом плане изолирована, Интерпол, к сожалению, не способен решить все проблемы, и поэтому ситуация не исправляется. На международном уровне действительно нужно ставить вопросы о конкретных инициативах, о решении конкретных проблем, а не просто говорить о доминировании одной организации или одной страны.

Второй компонент проблемы — технологический. Почему-то считается, что чем больше запретить в интернете на уровне провайдеров, тем меньше будет проблем. На самом деле доказано, что чем ближе к устройству пользователя происходит фильтрация, тем эффективнее результат. В качестве примера можно привести так называемый *родительский контроль*. Возникает вопрос: где проекты продвижения программных, аппаратных средств, которые позволили бы такой контроль осуществлять? Что-то делают на коммерческой основе операторы мобильной связи или *Лаборатория Касперского*, но это организации коммерческие, их интересует уровень продаж. В то же время государство и общественность хотят, чтобы программные продукты были недорогими, но в то же время известными и надежными.

Третий момент — образовательный, про который тоже много говорили. В этом плане не происходит практически ничего. Давайте себе представим, что в детских садах и школах на вопрос ребенка, что там на улице горит красным и зеленым цветом, ему отвечали бы: «не обращай внимания, тебе нужно перейти дорогу — переходи». Нет, ему объясняют, что означают красный, желтый и зеленый цвета и так далее, это вкладывается человеку в голову *с младых ногтей*.

Последнее, о чем, как я понимаю, пока еще не говорили, — это проблема доверия. Доверия друг к другу и к правоохранительным органам. Это опять-таки часть общей, комплексной проблемы. Существует значительная разница между тем, что такое законность, эффективность и качество с точки зрения гражданина и с точки зрения того, от кого требуют отчетов по показателям раскрываемости, законности и эффективности. Или мы, как коллеги из ФСКН, считаем главной задачей закрыть как можно больше сайтов и тем самым лишить себя возможности поиска людей, которые занимаются торговлей наркотиками, или наша цель — поймать и наказать этих преступников. Еще один аспект в плане повышения доверия — так называемый *пиар*. Нужно рассказывать о конкретных случаях, когда благодаря деятельности правоохранительных органов, российских и зарубежных экспертов выявленные банды привлечены к ответственности, а те, кто занимались педо-

филией или продажей наркотиков, — наказаны. К сожалению, чаще можно услышать об обратных примерах.

Поэтому давайте друг другу доверять. Прозвучали правильные слова про государственно-частное партнерство: бизнес наш патриотичен, население обладает достаточно хорошими знаниями и гражданской позицией, и нужно работать сообща.

АЛЕКСЕЙ КУДРИН: Выступающие более-менее обрисовали состояние дел на сегодня. Но что нас ждет через 15–20 лет? Хотел бы попросить Алексея Яцыну, модератора проекта *Форсайт-флот,* кратко высказаться об этом.

АЛЕКСЕЙ ЯЦЫНА: *Форсайт-флот* этого года, как известно, был посвящен Национальной технологической инициативе, мы стояли у истоков ее проработки, сейчас это официальная государственная программа.

Надо понимать, что уже в следующем году на дороги общего пользования Российской Федерации выйдет первый беспилотный *КАМАЗ*. Это означает, что пройдет пять, семь, десять лет, и беспилотный транспорт будет ездить по нашим дорогам. Не в Америке, не в Англии — у нас. Это означает, что уже сегодня надо формировать дорожно-транспортное законодательство, рассчитанное на беспилотный транспорт. Кто будет виноват, если беспилотник собьет человека? Это к вопросу техноэтики ближайшего будущего, о чем пока думают мало, а думать пора. Завтра в воздух поднимутся тысячи, десятки тысяч дронов. Сегодня маленький дрон с фотовидеокамерой является самым популярным подарком ребенку на Новый год, он стоит уже две-три тысячи рублей, послезавтра эти устройства будут выполнять десятки, а то и тысячи задач. Каким образом они будут помогать полиции обеспечивать безопасность? Готовы ли полицейские работать по профессиональным стандартам не участкового, который обходит дома, а участкового-программиста, способного запрограммировать дронов на облет территории, контроль и вызов оперативной группы?

Был приведен пример того, что людей, имеющих достаточную квалификацию для анализа киберпреступности, крайне мало. В то же время в Лондоне в рамках чемпионата World Skills, где соревнуются представители различных профессий, криминалистика — одна из дисциплин. То есть туда приезжают не только сварщики, штукатуры, ландшафтные дизайнеры, CAD-инженеры, специалисты по 3D-моделированию, но и криминалисты. Известно, что в нашей стране развивается кружковое движение, мне кажется, что МВД и другие органы безопасности должны подключаться к этому процессу со своими задачами, и тогда сегодняшние 12–15-летние дети вырастут и захотят работать в области обеспечения безопасности и решать задачи, в том числе связанные с борьбой с киберпреступностью. Сегодня граждане иногда могут самостоятельно провести расследование быстрее, лучше, эффективнее, чем МВД. Наши граждане готовы в этом смысле сотрудничать с органами правопорядка. Запрос на безопасность есть, и он будет расти.

И последнее. Я уже говорил про снятие законодательных барьеров. Самый яркий пример — это технология блокчейн. Она связана с контролем и криптозащитой транзакций. На днях Герман Греф говорил в своем выступлении, что снимать

законодательные ограничения на блокчейн надо было год назад. В этом плане Российская Федерация отстает, а, значит, наши финансовые институты не имеют доступа к самым современным способам защиты.

Основные предложения, которые у меня сформировались, пока я слушал уважаемых докладчиков: снятие барьеров, формирование перспективного законодательства, проведение конкурсов для младшего поколения. Я считаю, что органы безопасности должны входить в группу *Национальная технологическая инициатива*, туда должны входить разнообразные кружки, и они должны вырабатывать совместную повестку дня.

Матвей Войтов

КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА В КОНТЕКСТЕ КИБЕРБЕЗОПАСНОСТИ

Вот уже несколько лет тема защиты критической инфраструктуры является крайне актуальной среди производителей защитных систем в сфере информационной безопасности — повышение спроса из-за участившихся кибератак на критически важные объекты рождает рост предложения, в данном случае — рынка продукции, защищающей от таких нападений[1]. Но в большинстве случаев под одной вывеской кроется множество различных направлений: сертифицированные решения для государственного сектора, использование средств информационной безопасности (ИБ) на промышленных объектах, защита национального сегмента интернета и многое другое.

В этот раз мы постараемся определить, что же, с точки зрения *Лаборатории Касперского,* представляет собой критическая инфраструктура в контексте кибербезопасности и от чего, а, главное, как ее надо защищать. Критичность объекта и, соответственно, его инфраструктуры во всем мире определяется на государственном уровне, критические для существования и функционирования государств предприятия и отрасли фиксируются в специальных перечнях. Естественно, государствообразующими являются самые различные секторы и отрасли — от финансовой и банковской системы до систем управления водо- и энергоснабжением.

Если говорить об отраслях, наиболее часто относимых к критической инфраструктуре и связанных не только с физической, но и с кибербезопасностью, то на основании усредненного мирового опыта можно составить следующий перечень, в определенной степени совпадающий у большинства государств:

- электроэнергетика (атомная энергетика часто выделяется отдельно);
- управление природными ресурсами (в частности, нефтегазовый сектор);
- управление водными ресурсами (включая водоочистку и управление сточными водами);
- транспорт;
- пищевая промышленность;

- здравоохранение;
- телекоммуникации;
- финансовая и банковская системы;
- органы государственной власти.

Данная выборка сделана на основе находящихся в открытом доступе перечней и трактовок критической инфраструктуры следующими организациями:

- министерство внутренней безопасности США[2];
- центр защиты национальной инфраструктуры Великобритании[3];
- федеральное управление по информационной безопасности Германии[4];
- правительство Австралии[5].

Естественно, каждая страна специфически трактует понятие критической инфраструктуры. Например, министерство внутренней безопасности США предоставляет более детальный перечень, включая в него в том числе военно-промышленный комплекс. Отдельного внимания заслуживают организации, открыто занимающиеся общими вопросами защиты критической инфраструктуры — от министерств и правительств до специализированных ведомств. Помимо государственных программ развиваются и международные инициативы. В качестве примера можно привести единую европейскую программу по защите критической инфраструктуры[6].

Если говорить об опыте Российской Федерации, то на данный момент единого публичного перечня элементов не существует, тем не менее имеется существенная нормативно-правовая база, состоящая из различных законов, постановлений и указов, выпущенных Правительством РФ, Советом Безопасности, ФСБ и Федеральной службой по техническому и экспортному контролю (ФСТЭК), в которых даются определения таким понятиям, как *критически важный объект* и *ключевая система информационной структуры*. Основополагающими документами в этой сфере являются *Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий* и *Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации*[7].

Имея представление о всем многообразии элементов критической инфраструктуры, невозможно говорить о едином подходе к кибербезопасности, так называемой *серебряной пуле*, для каждой из отраслей. Тем не менее, чтобы не усложнять задачу, можно классифицировать элементы критической инфраструктуры исходя из типологии информационных систем, лежащих в основе той или иной отрасли и существующих на сегодняшний день средств их защиты.

Если функционирование некоторой части отраслей, к примеру финансовой сферы или органов госуправления, основано на *классических* информационных систе-

мах, основной целью которых является управление информацией, то другие — энергетика, транспорт, добыча природных ресурсов и т. д. — работают на основе специализированных промышленных систем, созданных для управления технологическим процессом. В подавляющем большинстве случаев инциденты, которые могут произойти на подобных промышленных объектах, потенциально могут привести к гораздо худшим последствиям, чем потеря информации или денег: к угрозе жизни людей, загрязнению окружающей среды и прочим действительно опасным результатам.

Поэтому безопасность таких объектов, в том числе кибербезопасность их инфраструктур, во множестве стран регламентируется особо. Например, в Российской Федерации требования к кибербезопасности промышленных критически важных объектов определяются приказом ФСТЭК № 31[8] от 14 марта 2014 г. Кроме того, предпринимаются усилия по развитию отраслевых стандартов безопасности, в частности давно ведется разговор о внесении детализирующих поправок в ст. 11 ФЗ 256 от 21 июля 2011 г. *О безопасности объектов топливно-энергетического комплекса*[9]. Кстати, наиболее часто атакам подвергается именно энергетическая сфера, в которой стоит отдельно выделить нефтегазовый комплекс и транспортный сектор.

Естественно, защите критических отраслей, которые функционируют на базе широко распространенных информационных систем, например телекоммуникациям или здравоохранению, также должно уделяться значительное внимание, но, с нашей точки зрения, современные средства обеспечения информационной безопасности при грамотном их использовании способны значительно снизить риски, исходящие от самых различных угроз: начиная от обычных вредоносных программ и заканчивая сложными таргетированными атаками. В промышленных информационных системах эти методы просто неприменимы в силу множества причин, о которых мы расскажем ниже.

Проигнорировать же защиту вообще и положиться на распространенную в промышленных сетях физическую изоляцию значит рано или поздно оказаться под ударом. Как показал опыт последних лет, физическая изоляция не способна остановить не только целевые атаки (последний пример — атаки на энергетические объекты и критические сектора Украины с помощью программы BlackEnergy[10]) и промышленное кибероружие (весь мир до сих пор вспоминает Stuxnet[11], а совсем недавно был обнаружен его преемник — Irongate[12]), но и стандартное вредоносное ПО, которое регулярно обнаруживают на изолированных объектах. Векторов атаки достаточно — начиная от инженера, принесшего в изолированную сеть зараженное устройство, и заканчивая подрядчиком, осуществляющим работы на объекте. Ситуация усугубляется тем, что атаки на промышленные объекты теперь не только прерогатива кибертеррористов и государственных спецслужб, но и *обычных* хакеров[13]. Можно прогнозировать, что с широким распространением промышленного интернета вещей киберпреступники активизируются еще сильнее.

Помимо заражения вредоносным ПО и целевых атак промышленные организации сталкиваются с рядом других киберугроз и рисков, направленных против всех элементов инфраструктуры: людей, процессов и технологий. Вот лишь основные риски, которые могут привести к серьезным инцидентам:

- ошибки и сбои программно-аппаратных компонентов промышленных систем;
- случайные или намеренные ошибочные действия сотрудников или подрядчиков;
- мошеннические операции в автоматизированной системе управления технологическим процессом (АСУ ТП);
- неосведомленность о правилах расследования инцидентов, особенностях сбора достоверных данных о них.

Именно поэтому защита по-настоящему критической инфраструктуры требует специального подхода и понимания. В чем же должна заключаться специфика промышленной киберзащиты? АСУ ТП требуют совершенно иного подхода к обеспечению информационной безопасности (а точнее, кибербезопасности, так как речь идет не только о защите информации) по сравнению с классической *офисной* ИТ-инфраструктурой. В корпоративных средах основное внимание уделяется сохранности конфиденциальных данных, а бесперебойная работа не настолько важна, как для АСУ ТП, где цена минуты простоя, как и любой другой ошибки, очень велика. Поэтому в обеспечении безопасности технологических процессов действует противоположный подход, при котором основной задачей является поддержание их непрерывности и оперативное устранение любых сбоев. Не говоря уже о том, что промышленная инфраструктура содержит в себе крайне специализированные элементы, не встречающиеся в корпоративной сети: системы диспетчерского управления и сбора данных, человеко-машинные интерфейсы, программируемые логические контроллеры и многое другое, что просто не поддерживается традиционными средствами обеспечения информационной безопасности. Циклы обновления программного и аппаратного обеспечения в промышленных средах гораздо более протяженные — очень часто на промышленных объектах встречается ПО, которое уже давно не поддерживается и содержит множество уязвимостей. Такие условия также не позволяют традиционным средствам обеспечения информационной безопасности эффективно работать. Кроме того, инструменты промышленной кибербезопасности должны отвечать требованиям государственных и отраслевых регуляторов и проходить сертификацию у производителей АСУ ТП.

Дополнительной сложностью является размытость зоны ответственности за обеспечение промышленной кибербезопасности: очень часто промышленный уровень является доменом инженеров АСУ ТП, которые относятся к средствам обеспечения информационной безопасности как к помехе, способной негативно повлиять на технологический процесс.

При этом инструментов обеспечения ИБ, созданных специально для защиты промышленных объектов, до сих пор крайне мало. Этот рынок активно развивается[14], и в ближайшее время таких продуктов станет больше, однако при этом крайне важно, чтобы у производителей таких средств было глубокое понимание специфики АСУ ТП и угроз безопасности этих сред. К примеру, нашей компании на создание специализированного решения в этой области потребовалось 5 лет — после обнаружения Stuxnet в 2010 г. не осталось сомнений в том, что *традиционная* защита более не эффективна.

Важной особенностью обеспечения промышленной кибербезопасности является то, что каждый проект такого рода уникален — так же, как и каждая промышленная инфраструктура, в которую просто невозможно установить некие стандартизированные продукты. Подбор оптимальной конфигурации защитных технологий и набора сервисов осуществляется после полного обследования текущей системы безопасности промышленного объекта, а имплементация выбранных мер происходит только в специально отведенное технологическое окно, чтобы не повлиять на процесс работы системы.

Несмотря на трудоемкость подобного проекта, результатом правильной интеграции специализированного решения будет действующая концепция многоуровневой защиты: через сочетание различных методов превентивной защиты, мониторинга и прочих сервисов оператор критической инфраструктуры получает средство, позволяющее реагировать на киберинциденты на всех возможных стадиях — от прогнозирования потенциальных атак и непосредственной защиты от них до обнаружения комплексных угроз и снижения ущерба. Уже можно наблюдать, как операторы постепенно осознают, что использовать этот непростой, но действенный подход к защите промышленных объектов необходимо, не дожидаясь, пока они окажутся в сводках новостей.

Примечания

1 Critical Infrastructure Protection Market Expected to Reach 144.82 Billion USD by 2021. Market Watch, 13 June 2016, http://www.marketwatch.com/story/critical-infrastructure-protection-market-expected-to-reach-14482-billion-usd-by-2021-2016-06-13-92033051 (последнее посещение: 21.06.2016).

2 Critical Infrastructure Sectors. U.S. Department of Homeland Security, https://www.dhs.gov/critical-infrastructure-sectors (последнее посещение: 21.06.2016).

3 The national infrastructure. Centre for the Protection of National Infrastructure, http://www.cpni.gov.uk/about/cni/(последнее посещение: 21.06.2016).

4 Critical Infrastructures. Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance, http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html (последнее посещение: 21.06.2016).

5 Trusted Information Sharing Network for critical infrastructure resilience, http://www.tisn.gov.au/Pages/default.aspx (последнее посещение: 21.06.2016).

6 Communication from the Commission on a European Programme for Critical Infrastructure Protection. Commission of the European Communities, Brussels, 12 December 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786: FIN: EN: PDF (последнее посещение: 21.06.2016).

7 Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Совет безопасности Российской Федерации, http://www.scrf.gov.ru/documents/6/113.html (последнее посещение: 21.06.2016).

8 Приказ от 14 марта 2014 г. № 31 *Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды*. Федеральная служба по техническому и экспортному контролю, http://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (последнее посещение: 21.06.2016).

9 Федеральный закон от 21 июля 2011 г. № 256-ФЗ *О безопасности объектов топливно-энергетического комплекса*. *Российская Газета*. 2011, 26 июля, http://rg.ru/2011/07/26/tek-dok.html (последнее посещение: 21.06.2016).

10 Kaspersky Lab's Global Research & Analysis Team. При APT-атаках BlackEnergy на Украине применялся целевой фишинг с Word-документами. 28 января 2016, https://securelist.ru/blog/issledovaniya/27903/pri-apt-atakax-blackenergy-v-ukraine-primenyalsya-celevoj-fishing-s-ispolzovaniem-word-dokumentov/(последнее посещение: 21.06.2016).

11 Zero Days.The Internet Movie Database, http://www.imdb.com/title/tt5446858 (последнее посещение: 21.06.2016).

12 Spring Tom. Зловред, заточенный под АСУ ТП, украл идеи у Stuxnet. Threatpost, https://threatpost.ru/irongate-ics-malware-steals-from-stuxnet-playbook/16544 (последнее посещение: 21.06.2016).

13 Панасенко Александр. Хакеры нечаянно атаковали водоочистные сооружения. Anti-Malware, 24 марта 2016, https://www.anti-malware.ru/news/2016-03-24/18450 (последнее посещение: 21.06.2016).

14 Perkins Earl, Alaybeyi Saniye Burcu. Market Guide for Operational Technology Security. Gartner, 23 May 2016, https://www.gartner.com/doc/3327318/market-guide-operational-technology-security (последнее посещение: 21.06.2016).

Мария Ходынская-Голенищева. *На правильной стороне истории*. Сирийский кризис в контексте становления многополярного мироустройства. Олма Медиа Групп, 2015 г. 384 стр.

Политические трансформации, произошедшие в начале второго десятилетия XXI века в арабском мире, вызвали бурные споры о возможных последствиях этих событий не только для региона, но и для мирового сообщества. Сирийский кризис, ставший, пожалуй, самым затяжным эпизодом *арабской весны*, стал своего рода лакмусовой бумажкой современного мироустройства, дискуссии о котором на самых разных уровнях только разгораются. С этой точки зрения актуальность книги М. Ходынской-Голенищевой не вызывает сомнений. Работа вносит ценный вклад в изучение конфликта в Сирии через призму меняющейся конфигурации сил на политической карте мира.

В монографии отмечается, что во внешней политике США и их союзников наблюдается опасная тенденция к смещению *неугодных режимов* в отдельных странах, что является, по мнению автора, попыткой Запада *притормозить* переход к полицентричному миру. Для обоснования данного тезиса рассматривается эволюция позиции США и их союзников в отношении кризиса в Сирии. Анализируется деятельность сирийской оппозиции и радикальных исламистских формирований, которые своей *живучестью* обязаны американской политике. Кроме того, всесторонне изучена позиция России по этому вопросу и ее роль в урегулировании конфликта.

Книга представляет особую ценность ввиду того, что ее автор — не только исследователь, но и сотрудник Постоянного представительства России при ООН и других международных организаций в Женеве. М. Ходынская-Голенищева, кандидат исторических наук и автор многих публикаций по ближневосточной тематике, лично принимала участие в переговорных процессах по сирийской проблеме и накопила немалый опыт. Поэтому читатель имеет возможность ознакомиться не только с научным анализом происходящего в Сирии, но и *из первых рук* получить представление о ходе переговоров по урегулированию кризиса.

Основная мысль автора прослеживается уже в названии книги: есть группа стран, в числе которых Россия, не желающая допустить силового решения сирийского вопроса. Эти страны, в отличие от американского руководства, стоят на *правильной стороне истории*. С первых страниц монографии автор предлагает свое виде-

ние картины современного мироустройства, акцентируя внимание на внешнеполитической деятельности Соединенных Штатов после окончания холодной войны. По ее мнению, страны Запада, в первую очередь США, использовали антиправительственные выступления на Ближнем Востоке и в Северной Африке для дестабилизации региона. Такая политика обусловлена стремлением Америки сохранить доминирование и однополярную структуру мира. Исследователь настаивает на том, что причина затяжного характера сирийского кризиса кроется скорее в деструктивной роли США, нежели в неуступчивости режима Башара Асада.

Одна из глав книги посвящена анализу внутренних и внешних причин кризиса, где сирийский президент Б. Асад представлен как реформатор, которому не удалось в силу разных причин объединить политическую элиту страны. В той же главе анализируется деятельность Вашингтона, направленная на свержение правящего режима с использованием влияния региональных союзников: Турции и Саудовской Аравии. По мнению автора, Соединенным Штатам необходима *подконтрольная* Сирия для усиления влияния в регионе и противодействия Ирану. Для достижения такой цели Америка сделала ставку на вооруженную оппозицию, пытаясь обеспечить ее признание в качестве легитимной. Тут же подчеркивается, что так называемая *умеренная оппозиция* никогда не демонстрировала способность действовать самостоятельно и не смогла предложить свое видение посткризисного устройства Сирии.

Кроме того, автор описывает, каким образом радикальные исламисты *вышли на авансцену* и как они осуществляют свою деятельность, а также предлагает методы противодействия экстремистам. Политика двойных стандартов Запада, делящего террористов на *плохих* и *хороших,* представлена в работе как основная причина усиления и расширения сферы активности исламистов. По мнению исследователя, настроенность западных стран против Б. Асада вступает в противоречие с их антитеррористическими усилиями, так как борьба с джихадистами в Сирии без сотрудничества с действующим правительством страны невозможна, а после падения режима неизбежно разрастание террористической угрозы. Для эффективной борьбы с терроризмом нужно привлечь к этой деятельности как Сирию, так и Иран. Автор признает, что по мере того как зверства и убийства джихадистами мирного населения стали приобретать все больший масштаб, США и некоторым странам региона пришлось скорректировать свое отношение к происходящему.

В книге подробно проанализированы попытки урегулирования конфликта и роль ООН в этом процессе. Твердая и последовательная позиция России по сирийскому вопросу противопоставляется нелогичным и бессвязным действиям противников Б. Асада в ходе переговоров. При этом автор считает ключевым историческим событием принятие резолюции СБ ООН о ликвидации химического оружия в Сирии, что и привело к отказу от силового вмешательства со стороны западных стран.

В монографии утверждается, что *объективный* процесс преобразования мира в сторону полицентричности неизбежен. Конфликт в Сирии отчасти является *зеркалом* этого явления, демонстрирующим противостояние двух концепций: представления США о том, что они являются единственным центром силы, с одной стороны, и поддерживаемого Россией принципа решения международных проблем на коллективной основе — с другой.

Монография, бесспорно, открывает глаза на множество ранее неизвестных фактов и в то же время отличается последовательностью, аргументированностью и убедительностью. Раскрываемые в работе подробности переговорного про-

цесса, о которых не сообщают СМИ, являются ценной информацией для тех, кому небезразличен исход сирийского кризиса.

Вместе с тем следует заметить, что, говоря о многополярности, автор не упоминает других крупных субъектов мировой политики, кроме России. Кроме того, в книге практически не описан положительный вклад противников Б. Асада в урегулирование кризиса. Чувствуется некий негатив и предвзятость в отношении западных стран в контексте сирийской тематики. Это отчасти объясняется спецификой работы автора в должности дипломата в международной организации, где представление и защита интересов собственной страны является первостепенной задачей.

В целом, книга может представлять интерес как для дипломатов и политиков, чьи профессиональные обязанности так или иначе связаны с отстаиванием интересов России на международной арене в контексте сирийского вопроса, так и для более широкой аудитории, включая экспертов-международников и тех, кто интересуется Ближним Востоком.

Магомед Меджидов

Marc Goodman. Future Crimes: a journey to the dark side of technology — and how to survive it. Doubleday, New York, 2015. 464 pp.

По мере распространения современных технологий растут и возможности злоупотребления ими. Общедоступность интернета несет риски для всех, от отдельных пользователей до компаний и даже государств, а экспоненциальный характер технологического прогресса влечет за собой резкий рост уязвимости.

Книга *Будущие преступления* дает исчерпывающий обзор киберугроз настоящего и будущего. Марк Гудман, специалист в области правоприменения, работавший с Интерполом, ФБР, Целевой группой по осуществлению контртеррористических мероприятий ООН и полицией различных стран, считает, что современный мир совершенно не подготовлен к атакам преступников, террористов и враждебных режимов на автоматизированные системы, которые, по сути, управляют современной экономикой и обществом.

Значительная часть книги посвящена защищенности отдельных пользователей от цифровых технологий, таких как социальные сети, интернет-магазины и мобильные приложения. Несмотря на то что некоторые пользователи знают о том, что размещать в социальных сетях информацию может быть опасно, есть и те, кто будут удивлены, узнав, насколько подробным может быть досье, созданное на основе информации, собранной интернет-сервисами.

Целевая реклама является наиболее безобидным способом использования таких досье. Компаниям-производителям антивирусов и программного обеспечения систем безопасности очень сложно не отставать от хакеров, охотящихся за личными данными. Мошенничество с кредитными картами или кража идентификационной информации стали обычным делом, что и демонстрирует Гудман с помощью увлекательных практических примеров. Вопрос безопасности личных данных встает еще более остро из-за развития *интернета вещей* — сети физических объектов, которые обмениваются данными для улучшения функциональности — и развития бионики, ведь ни одна из этих технологий не является достаточно защищенной от злоупотреблений.

Кроме того, в книге *Будущие преступления* подробно описываются последствия распространения высоких технологий для экономики и безопасности в целом. По мере того как энергетические, транспортные системы и медицинская инфраструктура подключаются к интернету, их уязвимость с точки зрения атак террористов или враждебных государств резко возрастает. По словам Гудмана, системы защиты критически важной инфраструктуры содержат множество слабых мест, а правоохранительные органы плохо подготовлены к отражению нападений, что подвергает риску целые государства. Распространение интернета создает не только новые мишени для террористов, но и открывает им новые возможности поиска финансирования и координации. Гудман демонстрирует это на примере теневого интернета, используемого для торговли наркотиками и оружием.

Автор рисует безрадостную картину в сфере информационной безопасности, но лишь небольшая часть его книги посвящена рекомендациям по борьбе непосредственно с киберугрозами. Его рекомендации носят по большей части общий характер: увеличить корпоративное и правительственное финансирование программ безопасности, повысить осведомленность о киберугрозах среди населения с помощью обучения и внести поправки в законы, с тем чтобы компании — разработчики программного обеспечения и интернет-сервисы несли ответственность за нарушения правил обеспечения безопасности. Интересным идеям, таким как игрофикация или краудсорсинг в сфере безопасности, к сожалению, уделяется относительно мало внимания.

Тем не менее, *Будущие преступления* — исследование, хорошо описывающее текущее состояние кибербезопасности. Читатели, плохо знакомые с предметом, могут прийти в замешательство, узнав, насколько легко их частная информация может быть получена, продана или использована в преступных целях. Однако даже те, кто хорошо осведомлен об этих угрозах, могут почерпнуть из книги немало нового об опасностях, исходящих от технологий будущего.

Леа Гернеманн

Alan Dershowitz. The Case Against the Iran Deal: How Can We Now Stop Iran From Getting Nukes? Rosetta Books, 2015. 244 pp.

В книге *Аргумент против иранской сделки* Алан Дершовиц, профессор Гарвардской школы права и известный политический обозреватель, представляет критическую оценку Совместного всеобъемлющего плана действий (СВПД), также известного как Соглашение по ядерной программе Ирана, переговоров, предшествовавших его подписанию, политической обстановки, в которой велись переговоры, а также потенциальных последствий его реализации, которые, как утверждает автор, могут представлять угрозу глобальной безопасности.

Автор исследовал тему в течение десяти лет, в частности брал интервью у президента США Б. Обамы, беседовал с сотрудниками его администрации по вопросам безопасности, а также с премьер-министром Израиля Б. Нетаньяху и высокопоставленными должностными лицами израильских военных и разведывательных служб. В своих оценках американский исследователь делает особый упор на изменение позиции США в отношении иранского вопроса на протяжении двух президентских сроков Б. Обамы.

Подробно разбирая возможные опасности, которые может повлечь за собой соглашение, Дершовиц характеризует его как близорукое и наивно идеалистическое. Он указывает на то, что важные внешнеполитические решения относительно ядерного потенциала Ирана, страны, открыто враждебной по отношению к Израилю и США и имеющей сильные связи с террористическими группами, включая *Хезболлу*, не могут быть построены на вере, оптимизме и надежде на то, что в течение 10–15 лет под влиянием более умеренного и заслуживающего доверия режима Иран будет выполнять СВПД и не начнет вновь работать над созданием ядерного арсенала после отмены санкций.

Хотя Дершовиц критически оценивает соглашение и придерживается невысокого мнения об искусстве Б. Обамы вести переговоры, он подчеркивает, что было бы неосторожным демонизировать СВПД и полностью отказываться от него, так как отказ Конгресса США освободил бы Иран от большинства санкций и лишил бы его стимула соблюдать условия сделки по вопросу об остановке развития ядерной программы. По его мнению, соглашение — меньшее из двух зол, поскольку отказ от этого плана привел бы к более тяжелым последствиям. Тем не менее автор замечает, что если бы Б. Обама с самого начала занял на переговорах более решительную позицию и настоял бы на угрозе военных действий со стороны США, Иран охотнее шел бы на компромиссы и уступки. По мнению профессора, отказ от силового сценария сильно ослабил переговорную позицию США.

Несмотря на то, что Дершовиц описывает СВПД в мрачных тонах и предрекает его катастрофические последствия, автор все же сохраняет прагматизм и не демонизирует ни само соглашение, ни Б. Обаму. Понятным языком он освещает слабые стороны соглашения, а также предлагает выход из положения. По мнению автора, конгресс США может сделать условия, прописанные в плане, более выгодными не посредством изменения формулировок, а через принятие резолюции, которая в будущем позволила бы президенту страны применять силу в случае необходимости, чтобы помешать Ирану приобрести ядерное оружие.

Дершовиц доходчиво разъясняет свои выводы и приводит сильные аргументы, что делает книгу доступной для всех читателей вне зависимости от их осведомленности в вопросах международной безопасности и иранской ядерной программы. Книга составлена из статей, написанных во время ключевых событий, приведших к соглашению по Ирану и произошедших во время первого и второго президентских сроков Б. Обамы. К сожалению, в текстах много повторов, из-за чего книга может показаться громоздкой и утомительной. Кроме того, нужно понимать, что автор представляет свои аргументы с позиции американца и неизбежно отражает прозападный взгляд на рассматриваемую проблему. Тем не менее, книга *Аргумент против иранской сделки* стоит прочтения. Тщательный анализ, четко сформулированные аргументы и убедительный прагматизм работы во многом перевешивают ее недостатки.

Кейси Норман

Павел Шариков. Проблемы информационной безопасности в полицентричном мире. Весь Мир, Москва, 2015 г. 319 стр.

С развитием информационных технологий все большую значимость для любого государства приобретает проблема обеспечения информационной безопасности.

Влияние информационных факторов на конфликты продолжает расти, а эффективность международно-правовых институтов перед новыми информационными вызовами остается низкой. Кроме того, на международном уровне существуют значительные противоречия в отношении регулирования информационных ресурсов. Для обеспечения национальной и глобальной безопасности необходимо углубленно исследовать ее информационную составляющую. Именно поэтому книга П. Шарикова, руководителя Центра прикладных исследований Института США и Канады РАН, представляет актуальность. Его работа — фундаментальный труд, в котором автор сделал попытку привести выводы исследователей этой проблемы к общему знаменателю.

В книге объясняются базовые понятия, связанные с информационной безопасностью, проиллюстрированные примерами из мировой политической практики. Особое внимание уделяется информационной политике США и событиям 2013–2014 гг. — разоблачениям Э. Сноудена и масштабной информационной войне вокруг кризиса на Украине.

Рассматривая проблемы информационного общества, П. Шариков анализирует такое явление, как информационная революция. Автор приводит различные точки зрения на предмет и делает вывод о том, что развитие информационных технологий оказывает огромное влияние на все аспекты жизни общества. Он обращает внимание на то, что методы противодействия традиционным угрозам национальной безопасности не работают в отношении асимметричных вызовов безопасности информационной.

Автор приводит убедительные доказательства формирования в XXI веке нескольких центров силы, не обладающих возможностью полного контроля над информационными ресурсами — важнейшим фактором могущества стран в текущем столетии. Сделан акцент на значительную роль США в глобальном управлении информационными ресурсами. Важным выводом является необходимость выработки единых стандартов использования информационных технологий в рамках глобального регулирования информационного пространства. По мнению П. Шарикова, стратегическая стабильность в XXI веке зависит от процессов глобализации и хода информационной революции.

Кроме того, автор говорит об изменении характера военных конфликтов и опасности кибероружия, доступ к которому могут получить негосударственные субъекты. П. Шариков делает вывод о начале нового этапа гонки вооружений в киберпространстве и, как следствие, о необходимости превращения России в один из центров силы, который будет способен обеспечить свою информационную безопасность в условиях вероятного глобального противостояния. При этом приводятся статистика и факты, подтверждающие выдвинутые автором тезисы, что представляет особый интерес и важность для читателя.

Книга, несомненно, будет интересна и полезна всем, кто интересуется политикой в сфере информационной безопасности, правовым регулированием использования информационных ресурсов и современными тенденциями международных отношений.

Инна Яникеева

Thomas J. Christensen. The China Challenge: Shaping the Choices of a Rising Power. W. W. Norton & Company, 2015, 392 pp.

Растущие мощь и влияние Китая еще с конца прошлого века начали вызывать беспокойство у США и ряда других стран мира. Тот факт, что даже после всемирного экономического кризиса 2007–2008 гг., подкосившего западные страны, китайская экономика продолжила демонстрировать впечатляющие показатели роста, только укрепил подобные настроения. Распространилось мнение, что Китай хочет бросить США вызов и сместить Америку с пьедестала мирового лидера. Многие представители политической элиты в Китае, России и других государствах полагают, что в ответ США пытаются *окружить* Китай и не допустить его доминирования ни в мире, ни даже в Азиатско-Тихоокеанском регионе. Всерьез обсуждается возможность военного столкновения между двумя гигантами, при этом отмечается, что Китай уже догоняет США по эффективности военного потенциала. Эти и другие мифы и просто неточности развенчиваются в книге Томаса Кристенсена *Китайский вызов: как скорректировать курс восходящей державы.*

К очевидным положительным сторонам работы можно отнести то, что ее автор — одновременно ученый и государственный деятель. Будучи профессором Принстонского университета, с 2006 по 2008 г. он занимал пост заместителя государственного секретаря США по вопросам Азиатско-Тихоокеанского региона. Помимо этого, Т. Кристенсен владеет китайским языком, часто путешествует в КНР, где общается со многими авторитетными представителями академических кругов, о чем подробно рассказывает в книге. Автор также рассказывает о своем участии в ряде важных переговоров, оказавших решающее влияние на китайско-американские отношения, в их числе установление Стратегического и экономического диалога и шестисторонние переговоры по ядерной программе КНДР.

В книге подробно разбираются причины и особенности китайского экономического роста. Критикуя некоторые аспекты, автор в целом положительно отзывается о проведенных Пекином реформах и делится своими впечатлениями о том, как менялась жизнь в стране в течение последних трех десятилетий. По мнению автора, США заинтересованы в экономическом росте Поднебесной точно так же, как Китай заинтересован в стабильности положения США. Т. Кристенсен описывает существующую систему международных отношений как взаимосвязанный мир, в котором Китай является неотъемлемым структурным элементом. Довольно много говорится о том, какие представления об Америке, угрозах и возможностях сотрудничества с ней существуют у китайского руководства и простых граждан. Во многом они определяются уязвимостью национального самосознания Китая, на протяжении прошедших веков претерпевшего множество унижений со стороны западных стран. Описывается решающая роль коммунистической партии во внутренней и внешней политике Китая: стоящая у власти элита изо всех сил стремится сохранить свою власть и больше всего опасается внутренней нестабильности и протестов любого рода. По мнению автора, США (по крайней мере на определенном этапе) выгодно укрепление регулирующих механизмов со стороны китайского руководства. Прежде всего это касается контроля над соблюдением стандартов качества, защиты прав интеллектуальной собственности и повышения уровня социального обеспечения с тем, чтобы повысить покупательную способность китайских граждан.

Т. Кристенсен не обходит вниманием и тот факт, что в настоящее время и в ближайшем будущем Китай не сможет составить США серьезную конкуренцию на мировой арене. Автор показывает, что КНР значительно уступает США по таким параметрам, как экономическая мощь, финансовый потенциал, уровень ВВП на душу населения, дипломатический и научно-технический потенциал, а также военная сила. Говоря о последнем аспекте, Т. Кристенсен останавливается на таких популярных концепциях американской стратегической мысли, как Air-Sea Battle, Anti-Access/Area Denial и C4SIR. Помимо этого, развенчиваются представления пессимистов о снижении американской мощи и дается подробный анализ стратегии *разворота США в Азию*. Тем не менее, отмечает автор, Китай может представлять для США ряд вызовов. Прежде всего это касается программы военной модернизации НОАК и деятельности КНР в рамках ООН.

Ученый подробно рассматривает историю взаимоотношений между Китаем и США со времен администрации Дж. Буша-старшего по наши дни, а также — уже не столь детально — отношения КНР со странами региона. Говорится об основных проблемах в отношениях двух стран, главная из которых — союзнические связи между Тайванем и США и активное сотрудничество между ними в военной сфере. Автор недвусмысленно выступает против восприятия внешней политики в качестве *игры с нулевой суммой*, осуждает радикальный политический реализм и неоконсерватизм.

В то же время он признает целесообразность использования в отношениях с Китаем *силовой дипломатии*, отмечая, что ее объект должен не только осознать реальность применения силы, но и быть уверенным, что уступка в спорном вопросе принесет ему выгоду. Необходимо также предоставить Китаю гарантии того, что США не несут угрозы его стратегическим интересам. В качестве позитивного примера Т. Кристенсен приводит взаимодействие с Пекином по вопросу урегулирования кризиса в Судане. Этот эпизод он сравнивает с развитием событий в Ливии, когда Китай, согласившийся сотрудничать, был жестоко разочарован тем, что миссия ООН по защите жителей города Бенгази переросла в полномасштабные военные действия с участием войск НАТО, завершившиеся кровавой сменой режима. Именно этим Т. Кристенсен объясняет неуступчивость Китая и России в сирийском вопросе.

В заключение автор констатирует, что в сдерживании КНР, в строгом смысле этого слова, нет необходимости. Вместо этого нужно направить национальные амбиции Пекина в нужное Вашингтону русло. На практике это означает, что следует активнее вовлекать Китай в процессы глобального управления, отговорить его от агрессивного поведения, укрепить позиции США и их союзников в АТР, а также способствовать стабилизации обстановки в регионе.

Говоря о впечатлении от книги, стоит заметить, что в ней представлен весьма интересный и всесторонний анализ, она может послужить отличным справочным материалом для всех, кто изучает американо-китайские отношения или интересуется межгосударственной политикой в АТР. Работа написана простым понятным языком, так что большой объем информации легко усваивается читателем. Книгу *Китайский вызов* можно справедливо назвать одной из самых информативных на сегодняшний день работ по проблематике американо-китайских отношений.

Алексей Степанов

An Analysis of the Russian-American Games from the Perspective of Their Domestic Politics. Ed. By Li Xing, Liu Jun. Shi-shi Press, Beijing, 2011. 444 pp.

Коллективная монография *Анализ российско-американских отношений в контексте внутриполитических факторов*, изданная издательским домом Ши-ши в декабре 2011 г. при поддержке Фонда общественных наук Исследовательской базы Министерства образования КНР, представляет собой первую в китайском научном сообществе работу, рассматривающую современные российско-американские отношения с точки зрения внутренней политики этих стран.

В состав авторов входят эксперт Департамента международных связей Центрального Комитета Компартии Китая, декан факультета международных отношений Пекинского педагогического университета, старший научный сотрудник Центра российских исследований Пекинского педагогического университета при Министерстве образования КНР доктор Ли Син и старший научный сотрудник Центра по изучению России Восточно-китайского педагогического университета, доктор Лю Цзюй.

Данная монография отличается логичным построением материала и выдержана в научном стиле. В первой части работы авторы рассматривают различные внутриполитические факторы, влияющие на внешнюю политику страны, а также вводят некоторые теоретические понятия. Вторая часть посвящена роли внутриполитических факторов в современных российско-американских отношениях. В третьей части обсуждается влияние внешнеполитических факторов на ряд актуальных вопросов, присущих нынешнему этапу российско-американских отношений. В качестве примеров могут быть названы расширение НАТО на восток, энергетическая политика, борьба с терроризмом, разоружение, ядерное нераспространение и др. В четвертой части рассматриваются позиции России и США в отношении их зарубежных партнеров (таких как ЕС, Китай, СНГ, страны Центральной и Восточной Европы) с внутриполитической точки зрения. В заключительной части авторы рассуждают о перспективах российско-американских отношений, основываясь на своих теоретических и прикладных исследованиях.

Смысловому наполнению книги присущи несколько значимых особенностей. Во-первых, авторы предложили собственное видение вопросов внутренней политики, которое, бесспорно, представляет научную новизну этой работы. По их мнению, мировая политика базируется на трех уровнях: международной системе (международный уровень), межгосударственных отношениях (национальный уровень) и внутренних факторах (внутриполитический уровень). Центральным звеном в этой системе авторы называют национальный уровень, так как именно в его рамках внутриполитические факторы могут оказывать влияние на мировую политику. Авторы подчеркивают, что внутренняя политика также осуществляется на трех уровнях (правительство, общество и личность) и выражается в трех формах (материальная, институциональная и идеологическая). На этом уровне действуют не только государства, но и иные, негосударственные субъекты. К таковым относятся НПО, ТНК, индивиды, вступающие в межнациональные браки, участвующие в международных конференциях и других подобных мероприятиях, а также субъекты так называемой *народной дипломатии*. Как отмечают авторы, взаимосвязи трех уровней мировой политики, а также трех уровней и трех форм внутренней политики и составляют сущность мирополитической системы в современных условиях. В традиционном смысле внутренняя политика определяет направление

внешней политики, а внешняя политика представляет собой продолжение внутриполитических процессов. Однако в реальности внешняя политика часто является относительно независимой и самостоятельной и нередко оказывает существенное влияние на внутриполитическую конъюнктуру. На сегодняшний день внешняя политика и внутриполитические процессы взаимодействуют и дополняют друг друга, существенная разница между ними отсутствует. Именно такой концептуальный подход лег в основу теоретического и прикладного аспектов этой работы.

Во-вторых, с точки зрения авторов, внутренняя и внешняя политика тесно взаимодействуют, особенно в нынешнем глобализирующемся мире. Россия и США — мировые державы, чьи взаимосвязи между внутренней и внешней политикой, несомненно, оказывают значительное влияние на содержание и общую картину двусторонних отношений. Основываясь на этих представлениях, авторы проводят детальный анализ прошлого и настоящего российско-американских отношений и делают прогнозы на будущее. В связи с этим авторы уделяют внимание содержанию, специфике и тенденциям развития отношений двух держав после окончания холодной войны. Следует отметить, что в китайском научном сообществе редко можно встретить труды, посвященные российско-американским отношениям, в которых одновременно анализировались бы внутренняя и внешняя политика этих стран. На сегодняшний день китайские исследователи не уделяют значительного внимания теоретической разработке и систематизации знаний по российско-американским отношениям. Можно сказать, что данная монография заполнила эти пробелы.

Рассматриваемая монография значительно отличается от других работ по современным российско-американским отношениям. Во-первых, авторы книги, будучи ведущими китайскими экспертами по международным отношениям, предоставляют зарубежной аудитории *третий взгляд* — взгляд Китая на актуальные проблемы в отношениях между Россией и США. Во-вторых, работа вносит значительный вклад в теоретическую разработку представления о связи между внешней политикой и внутриполитическими процессами, используемого при изучении современных межгосударственных отношений.

Ван Чэньсин

МЕРЫ ДОВЕРИЯ И БЕЗОПАСНОСТИ В СФЕРЕ ИКТ И ВОПРОСЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Обсуждение в ОБСЕ мер доверия и безопасности в киберпространстве началось с создания при организации в 2009 г. по решению № 1039 профильной Неформальной рабочей группы открытого характера[1]. Эта группа была, как считается, создана по инициативе представителя США при ОБСЕ посла Иэна Келли. Выработка новых мер доверия идет как раз в рамках, а точнее, *под эгидой* этой неофициальной группы, поскольку фактически работа на каждый момент ведется не более чем в пяти-шести столицах. И хотя решения этой группы не являются обязывающими, их реализацию нельзя не учитывать при оценке уровня информационной безопасности государств — членов Организации.

Говоря о мерах укрепления доверия и безопасности, в первую очередь стоит определиться, о чем идет речь.

Впервые как международно-правовой инструмент меры доверия появились в Соглашении между СССР и США о мерах по уменьшению опасности возникновения ядерной войны 1971 г.[2]. В последующем эта форма межгосударственного сотрудничества была закреплена в Соглашении о предотвращении ядерной войны 1973 г.[3].

Реально работающим механизмом меры доверия стали после подписания Заключительного акта Совещания по безопасности и сотрудничеству в Европе 1975 г.[4] и включения его в практику работы СБСЕ, а затем и ОБСЕ. Хельсинкский акт предусматривал, в частности, предварительное уведомление о крупных военных учениях, обмен наблюдателями на военных учениях и предварительное уведомление о крупных передвижениях войск.

Меры доверия, зафиксированные в Заключительном акте, были усовершенствованы документом Стокгольмской конференции 1986 г. по мерам укрепления доверия и безопасности и разоружению в Европе[5]. Этот документ с однозначностью показал, что страны — участницы конференции видят меры доверия и безопасности не только как конкретные действия, но и относят их не иначе как к военной сфере.

Таким образом, надо четко осознавать, что есть меры доверия, которые относятся, в основном, к сфере культуры, гуманитарному измерению, а есть меры доверия и безопасности — именно в такой формулировке — которые относятся к военной и только к военной сфере и нацелены на снижение уровня военного проти-

востояния государств. Их нельзя смешивать, хотя не следует и противопоставлять. Именно в дополнении мер доверия и безопасности мерами доверия можно найти комплексное решения проблемы обеспечения мирного сосуществования. Как подчеркивается в Документе Стокгольмской конференции, первостепенную важность имеет соблюдение десяти обозначенных в Хельсинкском Заключительном акте принципов, которыми государства-участники будут руководствоваться во взаимных отношениях. Такой подход, кстати, мог бы послужить хорошей базой для международной конвенции по обеспечению международной информационной безопасности, особенно если дополнить указанные принципы правилами поведения в информационной сфере.

Россия всегда в своей политике контроля над вооружениями приветствовала принятие мер доверия и безопасности как важного механизма обеспечения международного мира и снижения уровня военных угроз.

Этот подход в целом распространяется и на сферу международной информационной безопасности. В частности, в представленной на Встрече высоких представителей, курирующих вопросы безопасности (Екатеринбург, 21–22 сентября 2011 г.), концепции Конвенции об обеспечении международной информационной безопасности прямо указано на то, что каждое государство-участник должно стремиться к укреплению мер доверия и безопасности в области военного использования информационного пространства, к которым относятся:

1) обмен национальными концепциями обеспечения безопасности в информационном пространстве;

2) оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах в отношении их урегулирования и нейтрализации;

3) консультации по вопросам деятельности в информационном пространстве, которая может вызывать озабоченность государств-участников, и сотрудничество в отношении урегулирования конфликтных ситуаций военного характера[6].

Однако такой принципиальный подход не означает, что Россия, как и любая другая страна, должна в любых ситуациях соглашаться на принятие на себя обязательств по любым мерам доверия безотносительно их соответствия национальным интересам и интересам безопасности, в том числе с учетом наших внешнеполитических обязательств и интересов наших партнеров.

Аналогичный подход исповедуется и в США. Анализ документов и выступлений американских и натовских экспертов показывает, что те выделяют три группы мероприятий, которые могли бы быть отнесены к мерам доверия:

- меры транспарентности, которые позволяют сделать взаимодействие более предсказуемым;
- межгосударственные консультации, которые направлены на совместное обсуждение угроз и выработку рекомендаций по борьбе с ними;
- меры добровольного ограничения деятельности, то есть добровольное принятие странами на себя конкретных обязательств относительно отказа от тех или иных действий, которые могут рассматриваться как недружественные или даже опасные.

Вместе с тем существует и другой подход к принятию мер доверия и безопасности как формы международных отношений государств в сфере безопасности. Многие эксперты считают, что принятие подобных мер эффективно, только когда такое решение принимается на уровне ООН и распространяется на все страны. В противном случае вступает в дело юридический принцип всеобщности, делающий соглашение, реализующее эти меры, недействительным в отношениях с третьими странами, а следовательно, сохраняющий для заключивших соглашение стран угрозы, против которых направлены принятые меры, а значит, и уровень их обороноспособности, что, в свою очередь, требует наращивания военного потенциала. Кроме того, установление доверительных отношений между потенциальными противниками невозможно в принципе, а обязательные при заключении соответствующего соглашения даже незначительные уступки могут повлечь за собой в дальнейшем отход от принципиальных позиций. Меры доверия и безопасности, в том числе и в информационной сфере, по своей природе затрагивают весьма чувствительные вопросы, требующие всестороннего рассмотрения в контексте государственной и общественной безопасности.

Формально существующие международные документы не ограничивают список вооружений, к действиям с применением которых могут быть отнесены меры доверия и безопасности. Поэтому появление в начале нынешнего десятилетия в ОБСЕ идеи распространить этот механизм на информационное оружие, в качестве которого могут рассматриваться информационно-коммуникационные технологии, нельзя считать неестественным шагом[7].

Все, что происходит в рамках ОБСЕ в вопросах международной информационной безопасности, относится к сфере мер доверия и безопасности, т. е. все это по определению следует относить к военной сфере. Однако этот факт почему-то часто упускают из виду. А зря. Из сказанного следует фактическое признание государствами ОБСЕ наличия в современных международных отношениях войн в информационном пространстве (с использованием информационных средств воздействия[8]) и желания вести их как бы более гуманно, *доверяя* друг другу.

В упомянутом выше документе Стокгольмской конференции для реализации мер доверия и безопасности в качестве обязательного предусмотрен механизм верификации. Это означает, что он должен быть прописан и в соответствующем соглашении, распространяющем меры доверия и безопасности на другие, не предусмотренные Итоговым документом, сферы. Если обратиться к мерам доверия, пакет которых был принят Постоянным советом ОБСЕ в 2013 г.[9], то в Решении № 1106 таковых вроде бы нет. Можно сослаться на то, что во введенном решением перечне неоднократно подчеркивается добровольный характер принятых мер. Однако следует внимательнее рассмотреть следующий за перечнем мер раздел Решения № 1106 Постоянного совета (PC. БЕС/1106 3 декабря 2013 г.) ОБСЕ под названием *Практические соображения*. В соответствии с ним «государству-участнику, желающему получить разъяснения по поводу того или иного индивидуального сообщения, предлагается делать это на заседаниях Комитета по безопасности и его неофициальной рабочей группы, учрежденной Решением № 1039 Постоянного совета[10], либо путем вступления в прямой диалог с представившим его государством с использованием устоявшихся механизмов для контактов, включая список адресов электронной почты и дискуссионный форум POLIS».

По сути это основа механизма контроля исполнения означенных в Перечне мер, то есть механизма верификации, пусть и находящегося в зачаточном состоянии.

Что может означать на практике это положение, ведь, как говорят сторонники принятых мер, они все равно остаются добровольными и государство вправе само решать, что отвечать и отвечать ли на эти вопросы? Представим себе, что представителя государства *поднимут* на Комитете по безопасности, в зале, полном по этому случаю журналистов, и спросят: «Почему данную информацию ваша страна представила так, а не по-другому? Ведь говорят, что есть другая информация, отличная от этой. Объясните, пожалуйста, этот факт». Действительно ли добровольным является представление информации, если представителю государства предложат публично ответить? А может ли он *добровольно* не отвечать на этот вопрос в присутствии представителей прессы? Или, скорее, эта добровольность относительная? И будет ли при освещении этого диалога учитываться политический фактор? Ведь до сих пор при отсутствии каких-либо доказательств Россию обвиняют в информационных атаках на Эстонию, имевших (или нет — доказательств не представлено) место в 2007 г. Какие вопросы были бы заданы Постоянному представителю России при ОБСЕ, если бы к тому времени уже были бы приняты решения, аналогичные документу № 1106? И принял ли бы кто-нибудь его объяснения и подтверждающие их аргументы? Известно, что нельзя доказать отсутствие чего-либо, всегда остается предположение, что-де *слишком хорошо спрятали*. Даже при отсутствии презумпции невиновности, что мы нередко вынуждены бываем отмечать в практике международных отношений.

В итоговом докладе четвертой группы правительственных экспертов (ГПЭ) ООН по международной информационной безопасности, работавшей в 2014–2015 г. на основании резолюции 68 сессии ГА ООН *Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности*[11], также содержится перечень мер доверия, по своему содержанию во многом пересекающийся с венскими. Вместе с тем их изложение, особенно в пунктах 17 и 18, содержит модальности, позволяющие ставить вопрос о декларировании Группой необходимости механизма контроля исполнения. Поэтому вся дискуссия, в основном, проходит не вокруг того, что включать в меры доверия, нужны они или не нужны, а вокруг того, как реализовывать эти меры и где заканчивается доверие и начинается верификация.

Последний пакет мер укрепления доверия в сфере ИКТ, одобренный в феврале этого года в рамках ОБСЕ[12], затрагивает, вероятно, самый скользкий момент — критическую инфраструктуру. Что означает обмен информацией об инцидентах на объектах критической инфраструктуры? В моем понимании, это предоставление сведений о средствах, которыми была осуществлена акция, о мерах, которые были приняты для защиты объекта, о результате применения средств защиты на объекте, о последствиях атаки для функционирования объекта. Однако как ответы на эти вопросы, крайне чувствительные для национальной безопасности, соотносятся с интересами безопасности государств, на территории которых находятся или которым принадлежат упомянутые инфраструктуры? Потенциальные противники, спецслужбы и военные структуры были бы готовы дорого заплатить за такую информацию. Гораздо больше она заинтересовала бы террористические организации. Представьте, что было бы, если бы террористы получили доступ

к информации о том, как защищены критические инфраструктуры и какие средства нападения наиболее *успешны*.

Аналогичные предложения (создать единый или распределенный банк данных, систему свободного обмена информацией и т. п.) не раз звучали (почему-то, в основном, от американцев) и на других переговорных площадках в рамках нераспространенческой и антитеррористической тематик. Однако они практически никогда не находили поддержки экспертов. Им, в отличие от политиков, изначально было понятно, что решение вопросов ограничения доступа к подобным сведениям и предотвращения их *нецелевого* использования будет куда сложнее, чем поддержание традиционных форм сотрудничества.

Вопрос о включении пункта о критических инфраструктурах в пакеты мер доверия — один из самых сложных, и подходить к нему нужно осмотрительно, разобравшись, в первую очередь, с проблемами национальной безопасности.

Подводя итог, хочу еще раз обратить внимание на то, что меры доверия и безопасности в любой области предотвращения конфликтов и обеспечения мирного сосуществования государств не могут быть мерами принуждения и должны основываться на учете национальных интересов, суверенитета и равноправия всех государств.

Александр Федоров,
член Экспертного совета ПИР-Центра

Примечания

1 В практике ОБСЕ *открытый характер* означает отсутствие фиксации состава группы и проведение ее заседаний вне зависимости от наличия кворума. Решение теоретически может быть принято и одним председателем, хотя это, конечно, вырожденный случай.

2 Соглашение о мерах по уменьшению опасности возникновения ядерной войны между Союзом Советских Социалистических Республик и Соединенными Штатами Америки. Вашингтон, 30 сентября 1971 г., http://old.nasledie.ru/politvne/18_9/article.php?art=26 (последнее посещение — 1 июня 2016 г.)

3 Соглашение между Союзом Советских Социалистических Республик и Соединенными Штатами Америки о предотвращении ядерной войны. Вашингтон, 22 июня 1973 г., http://old.nasledie.ru/politvne/18_24/18_24_1/article.php?art=8 (последнее посещение — 1 июня 2016 г.)

4 Совещание по безопасности и сотрудничеству в Европе. Заключительный акт. Хельсинки, 1 августа 1975 г., https://www.osce.org/ru/mc/39505?download=true (последнее посещение — 1 июня 2016 г.)

5 Документ Стокгольмской конференции по мерам укрепления доверия и безопасности и разоружению в Европе, созванной согласно соответствующим положениям Итогового документа Мадридской встречи Совещания по безопасности и сотрудничеству в Европе. Стокгольм, 1986 г., http://www.osce.org/ru/fsc/41242?download=true (последнее посещение — 1 июня 2016 г.).

6 Конвенция об обеспечении международной информационной безопасности (концепция), http://www.scrf.gov.ru/documents/6/112.html (последнее посещение — 1 июня 2016 г.).

7 Вопрос возможности применения информационно-коммуникационных технологий в качестве оружия, конечно, спорный, как минимум в лингвистическом смысле, но в политических кругах такая трактовка признается правомерной. Хотя какой ущерб может нанести технология как таковая, понять и объяснить непросто. Лично мне встречать рациональное объяснение или хотя бы конкретные примеры такого не приходилось.

8 Поскольку понятие *оружие* не определено, видимо, предпочтительным следует признать использование этого термина вместо получившего распространения термина *информационное оружие*.

Что под ним понимать, можно найти в выпущенной ПИР-Центром под моей и В. Н. Цыгичко редакцией еще в 2001 г. монографии *Информационные вызовы международной и национальной безопасности*, http://www.pircenter.org/media/content/files/9/13464042510.pdf (последнее посещение — 1 июня 2016 г.).

9 PC. DEC/1106. Решение № 1106. Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий. Организация по безопасности и сотрудничеству в Европе, Постоянный совет, 975-е пленарное заседание. 3 декабря 2013 г. PC Journal No.975, пункт 1 повестки дня, http://www.osce.org/ru/pc/109648?download=true (последнее посещение — 1 июня 2016 г.).

10 PC. DEC/1039. Решение № 1039. Разработка мер укрепления доверия с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий. Организация по безопасности и сотрудничеству в Европе, Постоянный совет, 909-е пленарное заседание. 26 апреля 2012 г. PC Journal No.909, пункт 2 повестки дня, http://www.osce.org/ru/pc/90634?download=true (последнее посещение — 1 июня 2016 г.).

11 A/70/174. Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Записка Генерального секретаря. 22 июля 2015 г., http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (последнее посещение — 1 июня 2016 г.).

12 PC. DEC/1202. Решение № 1202. Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий. Организация по безопасности и сотрудничеству в Европе, Постоянный совет, 1092-е пленарное заседание. 10 марта 2016 г. PC Journal No.1092, пункт 1 повестки дня, http://www.osce.org/ru/pc/228521?download=true (последнее посещение — 1 июня 2016 г.).

КОММЕНТАРИИ ОТНОСИТЕЛЬНО РЕКОМЕНДАЦИЙ ПИР-ЦЕНТРА ПО УКРЕПЛЕНИЮ РЕЖИМА ЯДЕРНОГО НЕРАСПРОСТРАНЕНИЯ В 2016—2020 гг.

Пять из девяти конференций по рассмотрению действия ДНЯО, прошедших с момента вступления Договора в силу, завершились без достижения консенсуса по итоговому документу. Такая ситуация не должна рассматриваться как особенно тревожная или необычная. Это естественное и неизбежное следствие тех условий, в которых Договор обсуждался в 1966 и 1967 гг. и был представлен на подпись и ратификацию государствам-членам в 1968 г. Договор, в первую очередь, отвечал интересам двух крупнейших обладателей ядерного оружия и их союзников, которые были настроены заблокировать доступ других государств к этому средству массового уничтожения.

С момента вступления ДНЯО в силу ряд государств, изначально выступавших против Договора, согласились к нему присоединиться. Исключением стали три страны, которые впоследствии разработали ядерное оружие. Позже покинула Договор и создала собственный ядерный арсенал четвертая страна. Поскольку, согласно положениям ДНЯО, количество стран, официально являющихся *государствами, обладающими ядерным оружием*, не может быть увеличено, это навсегда (если только не рассчитывать на внесение поправок в текст Договора) закрыло двери ДНЯО перед странами, испытавшими ядерное оружие после 1 января 1968 г. Присоединяться к нему в качестве *государств, не обладающих ядерным оружием*, эти страны явно не собираются. Поэтому в нынешних условиях универсализация Договора не стоит на повестке дня. Эта проблема, в первую очередь, создана самими сторонниками ДНЯО. Им придется жить с этим.

Тем временем реализация положений Договора, касающихся нераспространения, оказалась достаточно эффективной. С момента вступления ДНЯО в силу больше никто из его участников, не обладающих ядерным оружием, не приобрел атомную бомбу. Сюжеты предполагаемого нарушения странами своих обязательств разрешались за счет сочетания политического и экономического давления, в том числе при помощи санкционного механизма Совета Безопасности ООН. Совместный всеобъемлющий план действий по иранской ядерной программе служит здесь хорошим примером. Эта деятельность велась вне рамок ДНЯО.

Если где и существуют расхождения между обязательствами и их воплощением в жизнь, то это область ядерного разоружения, в частности реализация статьи VI

ДНЯО. Серьезных и последовательных усилий к тому, чтобы «в духе доброй воли вести переговоры… [по] ядерному разоружению, а также о договоре о всеобщем и полном разоружении под строгим и эффективным международным контролем», не прилагалось. Государства, обладающие ядерным оружием, несут особую ответственность по выполнению обязательств, записанных в этой статье. Конструктивное взаимодействие в рамках многосторонних механизмов — лучший путь для достижения прогресса в этой области.

Что касается стратегической стабильности, то это выражение является, по сути, эвфемизмом для описания конкретных отношений между США и Россией в ядерной сфере, основанных на доктрине ядерного сдерживания. Пока обе страны продолжают рассматривать друг друга в качестве ключевых соперников и выстраивать отношения, основанные на вражде, здесь нельзя ожидать никакого реального прогресса. Международное сообщество мало что может сделать, чтобы улучшить отношения между Вашингтоном и Москвой и обеспечить настоящую стабильность, основанную на безопасности, достигаемой через сотрудничество, которая учитывает интересы подавляющего большинства государств.

Россия и США должны воздерживаться от нагнетания напряженности в двухсторонних отношениях и в то же время начать переговоры по продолжению процесса сокращения стратегических наступательных вооружений. В рамках этого процесса нужно завершить этап сокращений ради самого факта сокращений и сфокусироваться на цели полностью уничтожить ядерное оружие. Обе страны должны взять на себя четкие и юридические обязывающие обязательства по достижению данной цели.

Предложение ПИР-Центра по предоставлению отчетности о своих арсеналах всеми ядерными государствами представляется полезным, похожее предложение выдвинул в 2008 г. Генеральный секретарь ООН в своем плане из пяти пунктов. Отчеты, однако, должны строиться по модели, выработанной ООН, как это происходит в случае с обычными вооружениями.

Что касается различий между ядерными и неядерными державами в рамках ДНЯО, то оно вырастает из дискриминационного характера договора, разделившего мир на две категории государств: обладатели ядерного оружия и все остальные. Бессрочное продление ДНЯО, казалось, закрепило это разделение навечно. Это и стало причиной поляризации. Неготовность пяти ядерных государств установить четкий график процесса разоружения интерпретируется многими неядерными государствами как отсутствие желания достичь прогресса. Невозможно *ускорить* темп того, что еще не началось.

Относительно предложений ПИР-Центра по разблокированию работы Конференции по разоружению (КР) хочу сказать следующее: многие государства считают, что структура, созданная в 1978 г. на первой Специальной сессии по разоружению ГА ООН, изжила себя и, чтобы активизировать ее, необходима реорганизация. Лучший способ добиться этого — как можно скорее провести четвертую Специальную сессию по разоружению. Что касается упорства ряда ядерных государств и их союзников, настаивающих на разработке на КР Договора о запрещении производства расщепляющихся материалов (ДЗПРМ), то оно только тормозит процесс и отвлекает внимание от необходимости прогресса в области разоружения. Государствам — членам ДНЯО, не обладающим ядерным оружием, уже запрещено производство ядерных материалов для оружейных целей. При этом в рамках предлагаемого

ДЗПРМ странам, обладающим ядерным оружием, будет разрешено сохранить свои огромные запасы делящихся материалов, что позволит им продолжать наращивать и модернизировать свои арсеналы. Государства вне ДНЯО не будут заинтересованы в присоединении к такому договору. Поэтому в текущем виде ДЗПРМ является излишним в области нераспространения и беззубым в области разоружения.

Выработка договора, запрещающего размещение оружия в космосе, который бы дополнил Договор по космосу 1967 г., была бы полезной с точки зрения нераспространения. Работа над ним должна вестись параллельно с рассмотрением вопроса о заключении Договора о запрещении применения ядерного оружия.

Я поддерживаю предложения ПИР-Центра, касающиеся образования в области нераспространения и разоружения, следует призвать все государства осуществить рекомендации, содержащиеся в докладе Генерального секретаря по вопросу о просвещении в области разоружения.

Наконец, резолюция о создании зоны, свободной от оружия массового уничтожения на Ближнем Востоке, принятая в 1995 г. на Конференции по рассмотрению действия ДНЯО, была ключевым элементом для достижения соглашения о бессрочном продлении Договора. Но как только ДНЯО был продлен, государства, обладающие ядерным оружием, казалось, потеряли интерес к выполнению резолюции. Также сложилось впечатление, что они потеряли интерес к принятию юридически обязывающих обязательств по полной ликвидации своих ядерных арсеналов.

Рекомендации ПИР-Центра по передаче переговоров по ЗСОМУ под эгиду аппарата Генерального секретаря ООН, по обязательству стран региона воздерживаться от атак (включая кибератаки) на все задекларированные ядерные объекты друг друга и по разработке *дорожной карты* по постановке ядерной инфраструктуры региона под гарантии МАГАТЭ полезны и должны быть приняты. Ратификация ДВЗЯИ двумя ближневосточными государствами (Израиль и Египет) сильно запаздывает, Договор должен быть ратифицирован без промедления.

Что касается предложения ПИР-Центра о ратификации всеми ближневосточными странами Дополнительного протокола к Соглашению о гарантиях МАГАТЭ, здесь у меня есть замечание. Принятие дополнительного протокола является добровольной мерой в области нераспространения, которая повышает контроль над неядерными государствами. При принятии решения в этой области государствам, не обладающим ядерным оружием, стоит учитывать прогресс в переговорах по разоружению.

Сержио Дуарте,

Высокий представитель Генерального секретаря ООН
по вопросам разоружения (2007–2012)

Примечание

Данный комментарий является частным мнением автора и не отражает официальную государственную позицию.

FROM THE EDITOR

PIR CENTER ANALYTICS

INTERVIEW

A N A L Y S I S

ОБ АВТОРАХ

Баклицкий Андрей Александрович — директор программы ПИР-Центра «Россия и Ядерное нераспространение». Научный сотрудник Центра глобальных проблем и международных организаций Дипломатической академии МИД России. Редактор бюллетеня Ядерный Контроль. Выпускник факультета международных отношений Уральского федерального университета. Специалист в области регионоведения. В 2008–2009 гг. проходил обучение в Университете Севильи (Испания). Выпускник Международной Летней школы по проблемам безопасности 2011. В 2011–2013 гг. — Руководитель Интернет-проекта ПИР-Центра, с 2013 — Директор информационных проектов ПИР-Центра. Участник сессий подготовительного комитета к Обзорной конференции ДНЯО 2013–2014 гг. и Обзорной конференции ДНЯО 2015 г. Редактор Белой Книги ПИР-Центра «Десять шагов к зоне, свободной от оружия массового уничтожения, на Ближнем Востоке», редактор доклада «Иран в региональном и глобальном контексте». Сфера научных интересов: международная безопасность, большой Ближний Восток, ядерная энергетика и ядерное нераспространение.

Бегтин Иван Викторович — директор, учредитель АНО Информационная культура. Один из ведущих российских экспертов в области от крытых данных (Open Data) и открытого государства (Open Government). Автор общественных проектов: ГосЗатраты, Школа открытых данных, Школа информационной культуры, Хаб открытых данных, Открытая полиция, Понятный русский язык, Цифровое сохранение. Состоит в ряде Экспертном совета при Правительств е Российской Федерации, Общественном совете при Федеральном Казначействе, Общественном совете при Росстате, Общественном совете при Минкомсвязи России, Совете по Открытым данным при Правительственной комиссии по координации деятельности Открытого правительства, Экспертном совете по контрактным отношениям при Минэкономразвития России. Комитете гражданских инициатив. Представитель международной организации Clarity International в России. Посол Open Knowledge Foundation в России. В 2011 г. стал лауреатом премии в области общественно-политической журналистики Власть N 4. В 2012 г. — лауреатом премии press Звание в номинации Зона особого внимания. Автор многочисленных публикаций в области открытого государства, государственных и муниципальных расходов и открытых государственных данных.

Войтов Матвей Леонидович — руководитель отдела продуктового маркетинга в департаменте защиты критических инфраструктур Лаборатории Касперского. До этого там же в позиции менеджера по продукту руководил запуском линейки корпоративных решений по ИБ. Более 10 лет продуктового опыта в различных российских IT компаниях, включая Яндекс, а также в ряде стартапов. В 2006 году закончил экономический факультет МГУ им. М.В. Ломоносова. В 2008 году получил степень магистра по направлению «Менеджмент» в Высшей Школе Бизнеса МГУ им. М.В. Ломоносова.

Гасымов Кямал Тофик-оглы — эксперт Центра стратегических исследований при президенте Азербайджанской Республики. Выпуск ник факультета востоковедения Бакинского государственного университета. В 2007–2008 гг. обучался в Кувейтском университете. С 2013 г. эксперт Центра стратегических исследований при президенте Азербайджанской Республики. Участник международных конференций по вопросам исламоведения и востоковедения. Выпускник Международной Летней Школы ПИР-Центра по проблемам глобальной безопасности (2013). Автор научных статей по ближневосточной проблематике и переводов книг современных мусульманских мыслителей. Сфера научных интересов: история и историография классического ислама, исламские политико-правовые концепции, теория и методология исламского права, исламские общественно-политические движения.

Дуарте Сержио — Высокий представитель Генерального секретаря ООН по вопросам разоружения (2007–2012). Карьерный дипломат, с июля 2007 по февраль 2012 гг. — высокий представитель Генерального секретаря по вопросам разоружения Организации Объединенных Наций (ООН). На протяжении сорока восьми лет служил в Министерстве внешних связей Бразилии. За время работы являлся послом Бразилии в Австралии, Хорватии, Словакии, Словении, Китае, Никарагуа, Канаде, Швейцарии, США, Аргентине, Италии. С 1999 по 2000 гг. был председателем Совета Управляющих МАГАТЭ. Представлял Бразилию во многих международных организациях по вопросам разоружения. Член Международной экспертной группы ПИР-Центра с 2012 года.

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. Является автором ряда научных публикаций об инновационной экосистеме России и соавтором отчета Сколковского института науки и новых технологий по новым производственным технологиям. С 1994 по 2011 год работал в средних и крупных российских телекоммуникационных компаниях — «Аэроком», «Equant» и Группа Мобильные телесистемы (МТС). В МТС отвечал за разработку и исполнение ИТ-стратегии и взаимодействие с бизнесом. 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 рабо-

тал 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 Робоцентр является организатором и идейным вдохновителем всех активностей в Фонде «Сколково», название которых начинается с «Робо…».

Зербо Лассина — исполнительный секретарь Подготовительной комиссии Организации договора о всеобъемлющем запрещении ядерных испытаний. Получил докторскую степень в области геофизики в Университете Париж-Дофин в 1993 г. Начал свою карьеру в компании BHP Minerals International. В 1995 г. занимал позицию главного геофизика Африканского отдела в компании Anglo-American Exploration. В 2004-2013 гг. служил директором Международного Центра Данных Подготовительной комиссии ОДВЗЯИ. Исполнительный секретарь ПК ОДВЗЯИ с августа 2013 г. Сопредседатель совета глобальной повестки в области ядерной безопасности Всемирного Экономического Форума и член различных исследовательских центров в сфере энергетики, наук, технологий, развития, мира и безопасности в Африке.

Козюлин Вадим Борисович — старший научный сотрудник ПИР-Центра. Кандидат политических наук, профессор Академии военных наук. В 1990 г. окончил МГИМО МИД СССР. Работал сначала в системе МИД СССР/РФ, затем в отделе эксклюзивной информации газеты Московские новости, был представителем РГП Казспецэкспорт в России. В 2000–2002 гг. обучался во Всероссийской академии внешней торговли по программе «Менеджмент в сфере военно-технического сотрудничества». Тесно сотрудничает с компаниями — спецэкспортерами стран СНГ и дальнего зарубежья. Защитил диссертацию «Совершенствование политических механизмов влияния военно-технического сотрудничества на региональную безопасность в Центрально-Азиатском регионе». Адрес электронной почты: kozyulin@pircenter.org.

Кучерена Анатолий Григорьевич — член Общественной палаты Российской Федерации, председатель Общественного совета при МВД РФ. Адвокат, доктор юридических наук, профессор. В 1991 г. завершил обучение в Московском Юридическом Институте (нынешней Московской Государственной Юридической Академии). В настоящее время возглавляет кафедру адвокатуры и нотариата Московской Государственной Юридической Академии. В 1999 г. защитил кандидатскую диссертацию на тему «Административная юстиция в механизме защиты прав и свобод человека и гражданина в Российской Федерации». В 2003 г. защитил докторскую диссертацию на тему «Роль адвокатуры в становлении гражданского общества в России» в МГЮА. С 2001 г. по настоящее время возглавляет кафедру адвокатуры и нотариата Московской Государственной Юридической Академии имени О.Е. Кутафина (с декабря 2001 года). С 1993 г. по настоящее время — адвокат, председатель коллегии адвокатов «Кучерена и Партнеры», член Московской городской коллегии адвокатов. В 1995 г. организовал и возглавил одно из первых адвокатских бюро в рамках Московской городской коллегии адвокатов — «Аргумент» (в 2003 г. было преобразовано в Коллегию адвокатов «Кучерена и Партнеры»). С 2006 г. — Председатель Комиссии Общественной

Палаты Российской Федерации по общественному контролю за деятельностью правоохранительных органов, силовых структур и реформированием судебно-правовой системы.

Ларина Елена Сергеевна — Генеральный директор компании «Персоналинвест». Преподаватель Института экономических стратегий РАН и Академии информационных систем. Ведущий аналитик Института системно-стратегического анализа. Член Сообщества практиков конкурентной разведки. Член Сретенского клуба. Окончила экономический факультет Российского экономического университета имени Г.В. Плеханова и юридический факультет Института международного права и экономики им. А.С. Грибоедова. Работала в государственных органах, с 2002 года — в частном бизнесе. Автор книг «Кибервойны XXI века. О чем умолчал Сноуден» (книга издана на русском, английском и болгарском языках), «Мировойна. Все против всех. Новейшие концепции боевых действий англосаксов», «Роботы-убийцы против человечества. Кибер-апокалипсис сегодня», многочисленных статей в научных журналах, докладов для федеральных органов власти, РСМД, Изборского клуба и т.п. Сфера научных интересов: нечеткие конфликты, информационная безопасность, Третья (Четвертая) производственная революция.

Лукацкий Алексей Викторович — бизнес-консультант по информационной безопасности Cisco Systems. В 1996 году окончил Московский институт радиотехники, электроники и автоматики (МИРЭА) по специальности «Прикладная математика» (специализация — «Защита информации»). Входит в рабочую группу ЦБ по разработке требований по безопасности Национальной платежной системы (382-П). Участвует в экспертизе нормативно-правовых актов, в области информационной безопасности и персональных данных. Является участником Подкомитета № 1 «Защита информации в кредитно-финансовой сфере» Технического Комитета № 1 22 «Стандартизация финансовых услуг» Федерального агентства по техническому регулированию и метрологии. Является участником Подкомитета № 1 27 «Методы и средства обеспечения безопасности ИТ» Технического комитета № 2 2 «Информационные технологии» Федерального агентства по техническому регулированию и метрологии. Является участником Технического комитета № 3 62 «Защита информации» Федерального агентства по техническому регулированию и метрологии и ФСТЭК. Член Консультативного совета при Роскомнадзоре по защите прав субъектов персональных данных. Член Рабочей группы при ЭКС Пир-Центра по международной информационной безопасности и глобальному управлению Интернетом с 2012 года. С 2014 года — член Экспертного совета ПИР-Центра.

Малов Андрей Юрьевич — старший советник Постоянного представительства Российской Федерации при Отделении ООН и других международных организациях в Женеве. Канд. истор. наук. Окончил переводческий факультет Московский государственный педагогический институт иностранных языков им. М. Тореза. Работал в Комитете молодежных организаций СССР. С 1991–1994 гг. занимался исследовательской и преподавательской деятельностью в Институте экономических стратегий РАН (Москва). В 1992 г. работал приглашенным преподавателем в Западном Международном Университете США (Финикс, Аризона). С 1994 г. — сотрудник МИД РФ. Работал в «горячих точках» по линии ОБСЕ: в Нагорном Карабахе (1994–1996 гг.), а также в Боснии и Герцеговине (1996–1998 гг.). С 1998 г. зани-

мается в МИД РФ вопросами контроля над вооружениями, нераспространения и разоружения. Участник переговоров в области многостороннего разоружения.

Махукова Алена Владимировна — научный сотрудник и координатор проектов ПИР-Центра. Окончила Национальный исследовательский ядерный университет (МИФИ) по специальности «Международные отношения». В 2011-2013 гг. работала на телеканале Мир 24. В 2013-2015 гг. занималась внутренним аудитом информационного агентства ТАСС, участвовала в реформировании агентства. Выпускница Международной Летней школы по проблемам безопасности 2013 года. Стажер ПИР-Центра в августе-декабре 2015 г. Сфера научных интересов: информационная безопасность, управление интернетом, новые вызовы и угрозы, атомная энергетика, ядерное нераспространение.

Михайлова Ольга Игоревна — консультант в области физической ядерной безопасности. Окончила Томский политехнический университет по направлению «Безопасность и нераспространение ядерных материалов» (2010), специализация на учете и контроле ядерных материалов. Проходила практику в Петербургском институте ядерной физики, на Ростовской АЭС и в Национальной лаборатории Ок-Ридж (США). В 2010–2012 гг. работала инженером в отделе ядерной безопасности Ростовской АЭС. В 2010–2014 гг. работала в компании Booz Allen Hamilton, осуществляя поддержку российско-американского сотрудничества по физической ядерной безопасности. В настоящее время продолжает работу в это области в качестве независимого консультанта. Основное направление деятельности — экспертиза проектов нормативных документов и рекомендаций, разрабатываемых органами власти в области сохранности ядерных материалов.

Мостинская Ольга Сергеевна — главный редактор Индекса Безопасности. В 2003 г. окончила Московский государственный лингвистический университет, изучала лингвистику и межкультурную коммуникацию. В 1999–2000 гг. была вольным слушателем факультета социологии и антропологии Universite Libre de Bruxelles (Бельгия). В 2005–2015 гг. работала в Министерстве иностранных дел России, завершила службу в должности советника Департамента лингвистического обеспечения.

Овчинский Владимир Семенович — советник министра внутренних дел РФ. Криминолог, генерал-майор милиции в отставке, доктор юридических наук. Заслуженный юрист Российской Федерации (2008). В 1976 г. окончил Омскую высшую школу милиции МВД СССР. С 1976 по 1986 гг. работал в ГУВД Московской области. С 1986 по1992 гг. работал во ВНИИ МВД СССР/России. В 1992–1995 гг. — помощник первого заместителя министра внутренних дел России. В 1995–1997 — помощник министра внутренних дел России. С 1997 по1999 гг. — начальник Российского бюро Интерпола. С 1999 по 2001 гг. — обозреватель по правовым вопросам еженедельника «Московские новости» В 2001–2002 гг. — вице-президент ОАО «Сибирско-Уральская алюминиевая компания». С 2004 по март 2011 г. — Советник Председателя Конституционного суда РФ. С 2004 г. по настоящее время — член Экспертного совета Комиссии ГД ФС РФ по противодействию коррупции. С 2012 года — советник министра внутренних дел РФ, ответственный секретарь Расширенной рабочей группы по реформированию органов внутренних дел России.

Орлов Владимир Андреевич — кандидат политических наук. Является основателем (в 1994 г.) и советником ПИР-Центра. С 1994 по 2015 г. — директор, прези-

дент ПИР-Центра, а также член Совета ПИР-Центра. С 1994 по 2015 г. — главный редактор журнала Индекс Безопасности (до 2007 г. выходил под названием Ядерный Контроль). С 2014 г. — заведующий Центром глобальных проблем и международных организаций Дипломатической академии МИД РФ. Член Консультативного совета по вопросам разоружения при генеральном секретаре ООН (с 2015 г.). Член Совета по формированию глобальной повестки дня Всемирного экономического форума (с 2014 г.). Основатель (в 1993 г.), а ныне член Международного клуба Триалог. Возглавляет (с 2006 г.) научно-исследовательскую ассоциацию Centre russe d'etudes politiques со штаб-квартирой в Женеве (Швейцария). Член Экспертного совета Правительства Российской Федерации (с 2014 г.). Член Экспертного совета по противодействию коррупции при Управлении Президента РФ по вопросам противодействия коррупции (с 2014 г.). Член Научного совета при Национальном комитете по исследованию БРИКС. Советник делегации Российской Федерации на Обзорной конференции ДНЯО (2010 г., сессии Подготовительного комитета 2012–2014 гг.). Член Совета по внешней и оборонной политике (СВОП). Член Международной академии по ядерной энергии (INEA). Член Российского Пагуошского комитета при президиуме РАН. Член редакционной коллегии журнала The Washington Quarterly . Занимается активной научной, просветительской и преподавательской деятельностью в России и за рубежом. Преподает в МГИМО МИД РФ. Автор (соавтор) более 10 книг и монографий, около 300 научных работ и публицистических статей. Адрес электронной почты: orlov@pircenter.org. Твиттер: Orlov_pircenter. Фейсбук: VladimirAOrloff.

Сачков Илья Константинович — генеральный директор компании Group-IB. Окончил МГТУ имени Н. Э. Баумана, факультет информатики и систем управления, кафедра информационной безопасности. Основатель Group-IB, российского лидера рынка расследования компьютерных преступлений и инцидентов. Возглавляет компанию с 2003 года. Является членом следующих международных ассоциаций: Ассоциация компьютерной криминалистики информационных систем (IISFA), Ассоциация сертифицированных специалистов по борьбе с мошенничеством (ACFE), Международного проекта Honeynet Project. Член экспертного совета премии ЗУБР, Ассоциации профессионалов в области информационной безопасности RISSPA и Комитета по киберпреступности РАЭК. Член экспертных комитетов Государственной думы РФ, Совета Европы и ОБСЕ в области киберпреступности. В 2010 году стал первым российским лауреатом премии международной конференции Digital Crimes Consortium за вклад в международный обмен опытом в области компьютерной криминалистики. Член Рабочей группы при Экспертно-консультативном совете ПИР-Центра по международной информационной безопасности и глобальному управлению Интернетом с 2012 года. Член Экспертного совета ПИР-Центра с 2014 года.

Стальмахов Константин Александрович — ведущий специалист Департамента правовой и корпоративной работы Государственной корпорации по атомной энергии «Росатом». В 2012 году окончил юридический факультет МГУ им. М.Ю. Ломоносова по специализации «Предпринимательское право». С 2012 года по настоящее время работает в отделе аналитической работы Департамента правовой и корпоративной работы Государственной корпорации по атомной энергии «Росатом».

Федоров Александр Валентинович — член экспертного совета ПИР-Центра. Кандидат физико-математических наук. После окончания учебы в Московском государственном университете им. М.В. Ломоносова работал в учреждениях государственного аппарата. Занимался проблемами разоружения и нераспространения ОМУ. В последнее время ведет активную научную и практическую деятельность в сфере международной и информационной безопасности, а также борьбы с международным терроризмом. Редактор и соавтор монографий *Информационные вызовы национальной и международной безопасности и Супертерроризм: новый вызов нового века*. Член Экспертного совета ПИР-Центра с 2001 года. Член Рабочей группы при ЭС Пир-Центра по международной информационной безопасности и глобальному управлению Интернетом с 2012 года.

Шкарбанов Андрей Александрович — Советник Департамента правовой корпоративной работы Государственной корпорации по атомной энергии «Росатом». В 2005 г. окончил юридический факультет Самарского государственного университета и факультет Зарубежной военной информации Военного университета МО РФ. В 2007–2011 гг. — начальник проектного отдела, старший руководитель направления Департамента корпоративной и правовой работы АО «Техснабэкспорт», с 2011 года по настоящее время — советник по международно-правовым вопросам Департамента правовой и корпоративной работы Государственной корпорации по атомной энергии «Росатом» (Госкорпорации «Росатом»), член международной группы экспертов по вопросам гражданской ответственности за ядерный ущерб при генеральном директоре МАГАТЭ, представитель РФ в комитете по ядерному праву Агентства по ядерной энергии ОЭСР, член Международной ассоциации ядерного права (INLA).

Якушев Михаил Владимирович — вице-президент по взаимодействию с заинтересованными сторонами в Восточной Европе и Центральной Азии Корпорации Интернета по присвоению имен и номеров (ICANN). Опытный юрист, специалист в области информационной безопасности. Директор службы информационной безопасности PayPal, ранее — Вице-президент Mail.ru Group, председателель Совета Координационного центра национального домена сети интернет, управляющий директор DST Advisors. Занимается вопросами информационного права, в том числе вопросами доступа к информации. Соавтор большинства законопроектов в области использования информационных технологий. Работал в российском представительстве компании Microsoft и отвечал за взаимодействие корпорации с органами власти в Российской Федерации и других странах СНГ. Представлял Российскую Федерацию в рабочей группе по юридическим вопросам Большой Восьмерки. В 2004 г. — член рабочей группы по управлению Интернетом при Генеральном Секретаре ООН. Являлся Председателем рабочей группы ПИР-Центра при Экспертном Совете по международной информационной безопасности и глобальному управлению интернетом с 2012-2014 г.

Ярных Андрей Юрьевич — Руководитель стратегических проектов в России, странах Закавказья и Средней Азии Лаборатории Касперского. Опытный специалист в области информационной безопасности. С 1996 года работает в сфере связи и массовых коммуникаций, с 2001 года — в Лаборатории Касперского. Входит в правление Региональной Общественной Организации «Центр Интернет-технологий», является экспертом по вирусной безопасности в проектах Горячая линия «Дружественный Рунет» и «Центра безопасного интернета в России». Явля-

ется также Председателем Комиссии по информационной безопасности и киберпреступности Российской Ассоциации электронных коммуникаций (РАЭК). Член Экспертного Совета ПИР-Центра с 2015 г.

Яцына Алексей Юрьевич — эксперт по вопросам управления бизнес-системами. Консультант по вопросам управления, бизнес-тренер, со-руководитель Клуба «Менеджмент», соавтор методик управления «Теория фазовых трансформаций бизнеса», «Универсальная 9-ти процессная модель», «Методика аутсорсинга в условиях ограниченной конкуренции», «Куб метастратегий». Автор книг «Умный консалтинг» и «Умный консалтинг 2.0». Окончил Российскую экономическую академию им. Г.В. Плеханова. Изучал стратегию и контроллинг в Wissenschaftliche Hochschule fuer Unternehmensfuehrung (Кобленц, Германия).

ПИР-ЦЕНТР

(по состоянию на 30 июня 2016 г.)

Екатерина И. **Бабенко**, стажер

Андрей А. **Баклицкий**, директор программы *Россия и ядерное нераспространение*

Евгений П. **Бужинский**, к.в.н., генерал-лейтенант, председатель Совета

Леа **Гернеманн**, стажер

Олег В. **Демидов**, консультант

Дмитрий Г. **Евстафьев**, к.п.н., член Совета

Вячеслав А. **Зайцев**, главный бухгалтер

Альберт Ф. **Зульхарнеев**, директор

Галия Р. **Ибрагимова**, к.п.н., консультант

Наталья И. **Калинина**, д.м.н., член Совета

Вадим Б. **Козюлин**, к.п.н., старший научный сотрудник, член Совета

Александра В. **Куликова**, консультант

Марина С. **Кучеренко**, стажер

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

Алена В. **Махукова**, координатор проектов

Магомед Л. **Меджидов**, стажер

Ольга С. **Мостинская**, главный редактор журнала *Индекс Безопасности*

Кейси **Норман**, стажер

Владимир А. **Орлов**, к.п.н., советник, член Совета

Майя А. **Печенова**, стажер

Дмитрий В. **Поликанов**, к.п.н., член Совета

Галина Д. **Рассказова**, бухгалтер

Глеб М. **Самойлов**, стажер

Юлия В. **Свешникова**, консультант

Алексей С. **Степанов**, помощник главного редактора журнала *Индекс Безопасности*

Екатерина А. **Степанова**, д.п.н., член Совета

Денис И. **Токарев**, стажер

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*

Александра В. **Чепелева**, координатор базы данных, секретарь международного клуба *Триалог*

Елена В. **Черненко**, к.и.н., член Совета

Олег И. **Шакиров**, консультант

Инна О. **Яникеева**, стажер

ЭКСПЕРТНЫЙ СОВЕТ ПИР-ЦЕНТРА

(по состоянию на 30 июня 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 госсекретаря США по вопросам проверки и соблюдения соглашений по контролю над вооружениями, Вашингтон, США (с 1994 г.)

Данилов Дмитрий Александрович, к.э.н., профессор, ведущий научный сотрудник, заведующий отделом европейской безопасности, Институт Европы РАН, Москва, Россия (с 2011 г.)

Дворкин Владимир Зиновьевич, д.т.н., генерал-майор (в отставке), главный научный сотрудник, ИМЭМО РАН, Москва, Россия (с 2003 г.)

Демидов Олег Викторович, консультант, ПИР-Центр, Москва, Россия (с 2015 г.)

Джонсон Ребекка, д-р, директор, Институт *Акроним*, Лондон, Великобритания (с 1994 г.)

Дханапала Джаянта, 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, член Экспертного совета, ПИР-Центр, 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., член-корр. РАН, научный руководитель, Институт востоковедения РАН, Москва, Россия (с 2014 г.)

Никитин Александр Иванович, д.п.н., проф., директор, Центр политических и международных исследований, Москва, Россия (с 1994 г.)

Пархалина Татьяна Глебовна, к.и.н., заместитель директора 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., заведующий отделом стратегических исследований, Центр международной безопасности, ИМЭМО РАН, Москва, Россия (с 2002 г.)

Сатановский Евгений Янович, к.э.н., проф., президент, Институт Ближнего Востока, Москва, Россия (с 2004 г.)

Сафранчук Иван Алексеевич, доцент, кафедра мировых политических процессов, МГИМО (У) МИД РФ, Москва, Россия (с 2015 г.)

Сачков Илья Константинович, генеральный директор, *Group-IB*, Москва, Россия (с 2014 г.)

Синайский Александр Сергеевич, д.п.н., проф., 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., Москва, Россия (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 июня 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 июня 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, директор, Академия ОБСЕ в Бишкеке, Будапешт, Венгрия (с 2010 г.)

Злобин Николай Васильевич, президент, Центр глобальных интересов, Вашингтон, США (с 2014 г.)

Каравели Халил, руководитель проекта по Турции, Институт по изучению Центральной Азии и Кавказа при университете Джона Хопкинса, Анкара, Турция (с 2010 г.)

Кортунов Андрей Вадимович, к.и.н., генеральный директор, Российский совет по международным делам, Москва, Россия (с 2006 г.)

Макгетланенг Сехларе, д-р, директор, Программа государственного управления и демократии, Южноафриканский институт африканских исследований, Претория, ЮАР (с 2012 г.)

Сагер Абдулазиз, основатель и председатель, Исследовательский центр Залива, президент, Sager Group Holding, Джидда, Саудовская Аравия (с 2012 г.)

Санаи Мехди, доктор политологии, Чрезвычайный 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.)