РОССИЙСКИЙ СОВЕТ ПО МЕЖДУНАРОДНЫМ ДЕЛАМ

RUSI
www.rusi.org

ДОКЛАД

РОССИЙСКО-БРИТАНСКИЙ ДИАЛОГ ПО ПРОБЛЕМАМ БЕЗОПАСНОСТИ: ПЕРСПЕКТИВЫ ДВУСТОРОННЕГО СОТРУДНИЧЕСТВА. ЧАСТЬ 2

№ 38 / 2018

РОССИЙСКИЙ СОВЕТ ПО МЕЖДУНАРОДНЫМ ДЕЛАМ

КОРОЛЕВСКИЙ ОБЪЕДИНЕННЫЙ ИНСТИТУТ ОБОРОННЫХ ИССЛЕДОВАНИЙ

МОСКВА 2018

УДК 327.56(470:410)

ББК 66.4(2Рос),9(4Вел),30

Р76

Российский совет по международным делам
Королевский объединенный институт оборонных исследований

Главный редактор:
докт. ист. наук, член-корр. РАН **И.С. Иванов**

Авторы:
канд. ист. наук **А.В. Кортунов**; **М. Чалмерз**; **С. Лэйн**; **М.В. Смекалова**

Выпускающие редакторы:
канд. полит. наук **Т.С. Богдасарова**; **М.В. Смекалова**

Р76 Российско-британский диалог по проблемам безопасности: перспективы двустороннего сотрудничества. Часть 2. Совместный доклад Российского совета по международным делам (РСМД) и Королевского объединенного института оборонных исследований (RUSI). Доклад No 38/2018 / [А.В. Кортунов; М. Чалмерс; С. Лэйн; М.В. Смекалова]; [гл. ред. И.С. Иванов]; Российский совет по международным делам (РСМД). – М.: НП РСМД, 2018. – 40 с. – Авт. и ред. указаны на обороте тит. л

ISBN 978-5-6040387-6-5

В настоящее время российско-британские отношения находятся в глубоком кризисе. Удастся ли странам восстановить регулярный и системный диалог на высшем уровне? Каковы перспективы сотрудничества России и Великобритании по военной линии, в сфере контроля над ядерными вооружениями и обеспечения информационной безопасности? Какие механизмы необходимо выработать для укрепления мер доверия и развития сотрудничества в борьбе с киберпреступностью? Эти и другие вопросы, связанные с прошлым, настоящим и будущим российско-британских отношений в области безопасности рассматриваются в совместном докладе Российского совета по международным делам (РСМД) и Королевского объединенного института оборонных исследований (RUSI).

Полный текст доклада опубликован на интернет-портале РСМД. Вы можете его скачать и оставить свой комментарий к материалу по прямой ссылке – **russiancouncil.ru/report38**

© Коллектив авторов, 2018

© Составление, оформление, перевод, дизайн обложки. НП РСМД, 2018

Содержание

Введение и краткое содержание

В настоящем докладе изложены результаты второго раунда двустороннего российско-британского диалога по безопасности, проведенного Российским советом по международным делам (РСМД) и Королевским объединенным институтом оборонных исследований *(RUSI)* в рамках дипломатии "второго трека". В обсуждении возможных путей улучшения двусторонних отношений в сфере безопасности, проходившем в период с апреля по декабрь 2017 г., приняли участие эксперты и бывшие правительственные чиновники обеих стран.

Первоначально двусторонний диалог экспертов Соединенного Королевства и Российской Федерации развивался на фоне умеренно-позитивного тренда в двусторонних отношениях между Москвой и Лондоном. Эта общая тенденция сохранялась до марта 2018 г., когда отношения двух стран резко ухудшились из-за отравления на территории Великобритании бывшего российского двойного агента Сергея Скрипаля и его дочери веществом нервно-паралитического действия. Лондон возложил ответственность за это событие на Москву, после чего правительства обоих государств последовательно объявили о введении режима санкций относительно друг друга. Наши обсуждения в рамках второго раунда двустороннего диалога были завершены до начала этих событий, и поэтому их анализ не вошел в настоящий доклад. Тем не менее, как нам представляется, содержание двустороннего доклада остается актуальным для отношений между двумя странами. Более того, в настоящее время вопрос о продолжении диалога между экспертами неправительственных организаций приобретает особую значимость с учетом того, что российско-британские политические отношения остаются напряженными, а возможности для официального диалога на высоком уровне становятся все более ограниченными.

В ходе первого раунда диалога[1] нами был рассмотрен целый ряд вопросов безопасности и геополитики с целью выявить направления, которые сегодня представляются наиболее перспективными для сотрудничества. Во втором раунде основное внимание было уделено более детальному рассмотрению трех наиболее перспективных направлений, определенных в ходе первого раунда: взаимодействию по военной линии и снижению рисков военного столкновения в Европе; контролю над ядерными вооружениями и ядерными угрозами на конкретном примере Северной Кореи; снижению общих для двух стран киберугроз.

Хотя все эти темы связаны со сложными проблемами и не обещают быстрых решений, ценность платформы диалога «второго трека» (на уровне неправительственных организаций и независимых экспертов) заключа-

[1] Его результаты представлены 28 марта 2017 г. в совместном докладе А. Кортунова и С. Лэйн «Российско-британский диалог по проблемам безопасности: перспективы двустороннего сотрудничества».

ется в том, что эти вопросы можно обсудить совместно в неофициальном режиме, не подверженном чрезмерному влиянию текущей политики. Стремясь избежать нереалистичных предложений или оторванных от практики дискуссий, РСМД и *RUSI* предварили проведение трех семинаров частными консультациями с авторитетными специалистами в Москве и Лондоне и постарались привлечь как можно больше экспертов, обладающих опытом государственной службы. Это позволило сбалансировать креативность выдвигаемых идей предложениями, которые отталкиваются от существующей политической реальности.

Российско-британские контакты по военной линии были прерваны после разразившегося в 2014 г. кризиса на Украине. Стороны согласились в том, что этот разрыв повышает риски неверного восприятия действий друг друга. Хотя в нынешних политических условиях восстановление диалога между военными до прежнего уровня маловероятно, реальные возможности для его поддержания в том или ином виде все же имеются. По мнению британской стороны, они включают предложения по установлению специальной линии прямой связи («горячей линии») для урегулирования кризисных ситуаций; развитие контактов высокого уровня после состоявшегося визита в Москву заместителя начальника штаба обороны вооруженных сил Великобритании генерала Гордона Мессенджера; и использование готовности Великобритании проявить большую транспарентность в отношении целей и роли подразделений ее вооруженных сил, размещенных в Эстонии и Польше в рамках программы НАТО «Расширенное передовое присутствие». Кроме того, сближению могло бы содействовать и расширение контактов военных атташе обеих стран в Москве и Лондоне, а также согласие предоставлять больше информации о предстоящих военных учениях. Российские эксперты поддержали идею российско-британской «горячей линии», которая может оказаться полезной при решении вопросов взаимодействия по военной линии и кибербезопасности. Особое внимание следует уделять сотрудничеству между государственными и частными структурами в обеих странах («государственно-частное партнерство»), а также укреплению контактов между представителями бизнеса России и Великобритании. Учитывая, что британских компаний в России, как и российских в Великобритании, работает немало, эту возможность необходимо использовать.

Что касается контроля над ядерными вооружениями, то стороны согласились в том, что возрастающая вероятность одного или обоих участников от Договора о ликвидации ракет средней и меньшей дальности (Договор о РСМД) и Договора СНВ-3, будет иметь негативные последствия для обеих стран. Некоторые британские эксперты отметили, что существующие соглашения, даже если удастся их сохранить, могут потерять актуальность по мере развития военных технологий и эволюции военных доктрин ядерных держав. Вот почему повышенное внимание следует уделить растущему потенциалу неядерных военных технологий (включая космические, противоракетные и кибер-возможности), которые способны оказать влияние на баланс ядерных сил. Следует изучить возможность придания дискуссиям

по этому вопросу многостороннего характера, например, в рамках диалога между членами ядерной «пятерки».

Что касается кибербезопасности, то участники из обеих стран отметили заинтересованность коммерческих структур Великобритании и России в совместной борьбе с киберпреступностью и готовность к ней подключиться. Поскольку в нынешнем политическом климате на прямые контакты между российскими и британскими правоохранительными структурами рассчитывать трудно, совместная борьба с киберпреступностью на государственном уровне представляется весьма проблематичной. Однако поддерживать контакты можно по другим каналам или через третьи страны, в том числе в рамках многосторонних усилий. Операция, которая привела к разгрому преступной кибергруппировки *Avalanche* («Лавина»), показывает, насколько эффективно может действовать межюрисдикционное, частно-государственное некоммерческое сотрудничество. Однако и России, и Великобритании необходимо обеспечить наличие адекватной законодательной базы, которая позволит им участвовать в этой работе. Вместе с тем, необходимо укреплять доверие и заинтересованность акторов частного сектора в обмене информацией для борьбы с преступностью, а также укреплять доверие между государственным и частным сектором. Перспективы двустороннего сотрудничества между государственным и частным сектором воспринимается неоднозначно, поскольку в Великобритании существует мнение, что частные российские фирмы по компьютерной безопасности связаны со спецслужбами и делятся с ними информацией. Но даже если такое мнение и соответствует действительности, то это отнюдь не исключает возможности диалога с заинтересованными сторонами частного сектора.

В целом, следует иметь в виду, что все надежды на двустороннее сотрудничество в этих крайне чувствительных с точки зрения национальной безопасности областях должны учитывать нынешнее состояние отношений между Россией и Западом, которое является итогом их длительной эволюции в период после окончания холодной войны. По основным вопросам отношения с Россией Запад занимает коллективную позицию, выработанную в рамках НАТО, ЕС или в рамках особых отношений между США и Великобританией. Например, некоторые российские эксперты указывали на то, что развертывание Великобританией своих военных подразделений в странах Балтии является частью более общего проекта НАТО, и поэтому никакой отдельной двусторонней российско-британской договоренности о предотвращении инцидентов в воздухе в духе предложенной Финляндией летом 2016 г. инициативы (см. сноску 11 ниже), достигнуто быть не может. Понятно, что политическая конфигурация в этих областях будет задаваться в том числе и политикой президента США Дональда Трампа, изложенной его администрацией в Стратегии национальной безопасности, Стратегии национальной обороны и Обзоре состава и количества ядерных сил, которые были приняты в период с декабря 2017 г. по февраль 2018 г.

Британские участники выразили озабоченность тем, что набирающая обороты российская «информационная война», в том числе предполагаемые

хорошо организованные попытки российских организаций вмешаться в политические процессы на Западе, подрывают взаимное доверие и не способствуют его укреплению в других областях. Российские же участники, напротив, считают, что политизация информации, распространение дезинформации многочисленными источниками, а также примат домыслов над фактами еще больше подрывают доверие между Россией и Западом и лишь осложняют сотрудничество по вопросам, представляющим взаимный интерес. Участники обеих стран согласились с необходимостью приложить все усилия, чтобы эти проблемы не приводили к дальнейшему обострению отношений между Россией и Западом на межгосударственном и общественном уровнях.

Взаимодействие по военной линии

Первый раунд диалога по безопасности в рамках дипломатии второго трека был проведен РСМД и RUSI в Лондоне в октябре 2017 г. На нем рассматривался вопрос, целесообразность обсуждения которого была выявлена в ходе предварительных дискуссий. На них эксперты отмечали, что прекращение взаимодействия между военными двух стран чревато осложнением эффективного двустороннего управления рисками и повышает риски неверного восприятия действий друг друга. В ходе этого обсуждения основное внимание уделялось определению мер, принятие которых могло бы содействовать усилению российско-британского взаимодействия между военными и в сфере обеспечения безопасности.

Рекомендации

- Представляется, что существенного укрепления взаимодействия в военных вопросах можно достичь небольшими шагами в деле повышения прозрачности, сокращения рисков и развития контактов. Именно эти меры, а не решение масштабных проблем, таких как заключение новых соглашений о доверии или создание новой системы европейской безопасности, должны стать ближайшими задачами в российско-британских отношениях. Коллективный поиск возможных шагов по устранению главных препятствий на пути контроля над вооружениями, укрепления доверия и формирования основ новой системы безопасности сохраняет свою актуальность, поскольку он может облегчить принятие конкретных практических мер и улучшить взаимопонимание. Вместе с тем, в силу существующего низкого уровня доверия, такой «мозговой штурм» будет, скорее всего, достаточно продолжительным процессом, практические результаты которого проявятся нескоро.
- Следует добиваться большей транспарентности в вопросе проведения крупномасштабных учений. Предоставление значимой информации поможет обеим сторонам показать, что за этими учениями не скрывается никаких тайных планов. Было отмечено, что Великобритания, проявив бóльшую, чем раньше, открытость в отношении своей деятельности в рамках программы НАТО «Расширенное передовое присутствие», была разочарована тем, что Россия воздержалась от проявления такой же прозрачности относительно своих военных учений «Запад–2017».
- России и Соединенному Королевству надлежит расширять взаимодействие между военными в областях, которые не являются политически мотивированными, но, скорее, связаны с безопасностью и гуманитарными вопросами, в частности, в поиске и спасании подводных лодок и ликвидации последствий природных и техногенных катастроф.
- Было высказано мнение о том, что успешность Соглашения о предотвращении инцидентов в открытом море (*INCSEA*) может быть использована

для выработки аналогичного соглашения о предотвращении инцидентов в воздухе, чтобы предотвратить опасное маневрирование боевых самолетов двух стран.

- Необходимо придать новый импульс институциональному опыту в области укрепления доверия и контроля над обычными и ядерными вооружениями. Участники выразили обеспокоенность тем, что опыт в этой сфере утрачивается, прежде всего, представителями нового поколения экспертов-международников.

Трудности укрепления доверия

Реалистичные попытки реанимировать диалог между военными потребуют на начальном этапе относительно небольших, осторожных шагов, направленных на достижение конкретных целей, таких как снижение рисков эскалации или обмен информацией. Учитывая существующий низкий уровень доверия, рассчитывать на успех крупных инициатив по «укреплению доверия», не говоря уже о выработке новых официальных соглашений, например, о контроле над обычными вооружениями, в настоящее время не приходится. Вот почему центром внимания двусторонних дискуссий по вопросам обороны и безопасности должно стать предотвращение кризисов. Как выразился один британский участник, обеим сторонам присуще «взаимное гарантированное ложное представление». Но какими бы ни были текущие политические разногласия, двусторонние отношения необходимо налаживать.

Любая формальная зацепка в существующих договорах об обычных и даже ядерных вооружениях, таких как Венский документ 1990 г. (впоследствии обновленный)[2], Договор РСМД 1987 г. между СССР и США[3] или Договор по открытому небу, вступивший в силу в 2002 г.[4], используется сторонами для извлечения односторонней политической выгоды, что подрывает саму идею существования мер по укреплению доверия. Так, Россия объявила, что в учениях «Запад-2017», проходивших в Беларуси в сентябре 2017 г., участвовало 12,7 тыс. военнослужащих, что ниже установленного Венским документом порога в 13 тысяч, после которого необходимо приглашение наблюдателей. Однако одновременно с этими учениями в самой России проводилось много других официальных учений, которые не были обозначены как часть «Запада-2017». Российские эксперты разъяснили, что именно в это время года большие учения обычно проводятся в каждом военном округе. Однако, по мнению НАТО, разграничение не было убедительным, и учения «Запад-2017» вполне можно расценить как проведенные в гораздо большем масштабе.

При всей необходимости принятия поправок к существующим соглашениям, в нынешних условиях их вряд ли удастся согласовать. Сама эта тема

---

[2] OSCE, 'Vienna Document 2011 on Confidence and Security-Building Measures', 30 ноября 2011 г.

[3] Arms Control Association, 'The Intermediate-Range Nuclear Forces (INF) Treaty at a Glance', 22 декабря 2017 г.

[4] OSCE, 'Open Skies Consultative Commission', <http://www.osce.org/oscc>, accessed 18 February 2018. В настоящее время участниками Договора по открытому небу являются 34 государства – члена ОБСЕ.

на данный момент является камнем преткновения. Россия заявляет, что она уже предлагала реформировать и обновить, к примеру, Венский документ, однако Запад не проявил встречной заинтересованности. Теперь Запад выражает готовность рассмотреть этот вопрос, но настала очередь России говорить «нет».

Отчасти сложность проблемы заключается в том, что положения существующих соглашений, даже когда имеется доверие, необходимое для претворения их в жизнь согласно духу и букве договоренности, с течением времени теряют свою актуальность и устаревают. Нынешняя динамика военной модернизации и эволюция военных доктрин связана не столько с количеством оружия, сколько с его мобильностью, огневой мощью, точностью и другими качественными параметрами. Более того, современными мощными военными державами становятся государства, деятельность которых не ограничена ранее заключенными соглашениями. Многие страны все чаще осознают конкурентные преимущества, которое они получают благодаря неучастию в соглашениях о контроле над обычными вооружениями или о мерах по укреплению доверия.

Глядя в будущее, участники выразили обеспокоенность тем, что международно-правовые, морально-этические или технические ограничители развития новых технологий и их потенциального использования в вооруженных силах (например, дроны различных типов или системы, построенные с использованием искусственного интеллекта) разрабатываются недостаточно быстро. В нынешних политических условиях крайне трудно выработать и принять соглашение об ограничениях или правилах в отношении новых технологий. Участники выразили надежду на то, что общие принципы и побуждения, которыми руководствовались стороны при выработке прежних мер по укреплению доверия, заставят их задуматься о растущих рисках, связанных с неготовностью учитывать фактор быстрого развития новых военных технологий при прогнозировании динамики отношений двух стран в сфере безопасности.

При обсуждении мер по укреплению доверия и контролю над обычными и ядерными вооружениями, экспертами высказывалась особая озабоченность по поводу постепенной утраты сторонами столь необходимых для дальнейшего продвижения вперед уже накопленных институциональных знаний. Поскольку представители нового поколения экспертов не слишком стремятся изучать подобные проблемы, сохранение и развитие «институциональной культуры» в сфере безопасности следует всячески поощрять как Москве, так и Лондону.

Взаимодействие по военной линии

Стороны согласились с тем, что напряженность в отношениях России и Великобритании существовала задолго до событий на Украине. Это не означает, однако, что сотрудничество в сфере обороны и безопасности не развивалось. Например, в январе 2014 г. Министерство обороны Великобритании (МО) и Федеральная служба по военно-техническому сотрудничеству России пла-

нировали подписать уже согласованное Соглашение о военном техническом сотрудничестве[5]. Однако события на Украине, особенно в Крыму в марте 2014 г., привели к новому витку ухудшения отношений и положили конец большинству направлений двустороннего сотрудничества в военной сфере.

В результате кризиса сотрудничество между военными и взаимодействие между ними было прекращено. В нынешних условиях восстановление сотрудничества в полном объеме не представляется возможным. Вместе с тем отмечалось, что обе стороны заинтересованы во взаимодействии по отдельным направлениям с целью получить конкретные, пусть и ограниченные результаты. Особенно значимым является сотрудничество в сфере снижения рисков эскалации кризисов и повышения прозрачности военной деятельности сторон.

Несмотря на усиление напряженности в отношениях, отдельные двусторонние инициативы удается успешно поддерживать до настоящего времени. Эксперты обеих сторон согласились с тем, что двустороннее Соглашение о предотвращении инцидентов в открытом море *(INCSEA)* с обновлениями, согласованными в 2017 г., выполняется достаточно успешно. Было предложено использовать накопленный позитивный опыт *INCSEA* при выработке аналогичного соглашения о предотвращении инцидентов в воздухе, чтобы снять проблему опасного маневрирования. В 2017 г. в Санкт-Петербурге состоялась первая за десять лет встреча российских и британских гидрографов. При этом отмечалось, что при всей значимости этих инициатив, их недостаточно для устранения рисков неверного восприятия действий друг друга, существующих в отношениях между двумя странами.

Участники с обеих сторон подчеркивали, что прямое двустороннее взаимодействие необходимо укреплять, даже если оно сводится лишь к поддержанию каналов коммуникации. За последние полтора года Великобритания активизировала усилия по взаимодействию с российскими военными. Например, после визита в Москву в декабре 2015 г. главного маршала британской авиации Стюарта Пича, занимавшего пост заместителя начальника генштаба[6], была установлена «горячая линия» между Министерством обороны Великобритании и Национальным центром управления обороной Российской Федерации для разрешения инцидентов и кризисных ситуаций. После этого визита в феврале 2017 г. произошла встреча в Москве нового заместителя начальника штаба обороны вооруженных сил Великобритании генерала Гордона Мессенджера с занимающим аналогичный пост в российской армии генерал-полковником Александром Журавлевым. Питер Уоткинс, начальник Главного управления политики безопасности и военных операций Министерства обороны Великобритании, встретился с заместителем министра обороны России Александром Фоминым на полях конференции по безопасности в Азии «Шангри-Ла Диалог». В работе этого межправительственного форума по проблемам безопасности в рамках первого трека, ежегодно проводимого Лондонским международным институтом

[5] Matthew Holehouse, 'Comrades in Arms: Britain and Russia to Sign Defence Deal', The Telegraph, 26 января 2014 г.

[6] Интервью с представителями Министерства обороны Великобритании, Лондон, июль 2017 г.

стратегических исследований, приняли участие министры обороны, постоянные заместители министров обороны и военачальники 28 государств азиатско-тихоокеанского региона[7].

Во время визита в Москву в феврале 2017 г. британского заместителя начальника штаба обороны вооруженных сил Великобритания рассчитывала на большую открытость России, сообщив ей новые сведения о своей деятельности в рамках программы НАТО «Расширенное передовое присутствие» в Восточной Европе. Хотя Россия также представила информацию об учениях «Запад-2017», эти сведения, по мнению британских участников, носили слишком общий характер. Увеличение прозрачности крупномасштабных учений представляет собой хорошую возможность для двустороннего взаимодействия в будущем.

Поэтому один из британских экспертов посчитал не соответствующим действительности утверждение предыдущего доклада РСМД-*RUSI*, что по мерам укрепления доверия Великобритания «плетется в хвосте» других западных стран. В Лондоне складывалось ощущение, что Великобритания пытается добиться прогресса, но не сможет продвинуться вперед, если Россия не ответит взаимностью. Ниже приводятся возможные объяснения такого восприятия.

В качестве жеста доброй воли Россия могла бы предоставить более подробную информацию об учениях «Запад-2017», особенно учитывая, что аналогичное развитие событий предшествовало российским кампаниям в Грузии и на Украине. Один из российских экспертов высказал мнение, что России следовало довести количество задействованных в учениях «Запад-2017» военнослужащих до определенного Венским документом порога в 13 тысяч и пригласить наблюдателей, чтобы доказать, что ей нечего скрывать. Хотя это может сегодня и не понравиться российскому руководству, но такие идеи полезны для определения алгоритма действий, необходимых для восстановления мер по укреплению доверия, если на то появится политическая воля. При этом важно, чтобы при подготовке к предстоящим военным учениям в Европе, НАТО продолжало выполнять взятые на себя обязательства по Венскому документу.

Что касается контактов между военными, то было бы очень полезно поддерживать существующее российско-британское взаимодействие независимо от кадровых перестановок на той или другой стороне. Генерал Александр Журавлев теперь назначен командующим войсками Восточного военного округа, и пока не ясно, кто его заменит. Для продолжения диалога между российскими и британскими военными очень важно, кто сменит А. Журавлева на посту заместителя начальника Генерального штаба Вооруженных сил России. Один из британских экспертов предположил, что взаимодействие между военными может быть усилено на оперативном уровне, например, между британским начальником Объединенных операций и командующим Западным военным округом России.

[7] Интервью с представителями Министерства обороны Великобритании, Лондон, июль 2017 г.

Отмечалось, что поддержание личных контактов как продолжающих службу генералов и старших офицеров, связанных с оборонной тематикой и безопасностью, так и непосредственно министров обороны России и Великобритании, является исключительной редкостью. Даже в условиях высокой политической напряженности налаживание взаимопонимания и расширение подобных контактов представляется весьма полезным. Однако проведение только специальных совещаний недостаточно, контакты следует развивать в формате устоявшихся мировых практик. Оптимальным решением было бы подключение к диалогу в сфере безопасности Министерства иностранных дел и по делам Содружества Великобритании и Министерства иностранных дел России, о чем свидетельствуют итоги визита в Москву в декабре 2017 г. министра иностранных дел Великобритании Бориса Джонсона.

Обеим странам необходимо извлечь уроки из практики введения санкций и их влияния на развитие отношений. Один из британских экспертов подчеркнул, что контакты между военными, которые имели решающее значение в разгар украинского кризиса, пострадали из-за «тактических ошибок», заключавшихся во включении в санкционный список некоторых военных руководителей России. Например, в то время Стюарт Пич имел хорошие рабочие отношения с первым заместителем министра обороны Аркадием Бахиным. Этот полезный канал связи был перекрыт включением Бахина в санкционный список.

По-прежнему существуют сферы, сотрудничество в которых уже было успешным и вряд ли может вызывать возражения. Среди них поиск и спасание терпящих бедствие подводных лодок. Возможности расширения взаимодействия в таких сферах следует изучать. В 2005 г. Великобритания направила спасательную команду для оказания помощи экипажу российского батискафа АС-28, терпевшего бедствие в Тихом океане. Президент Владимир Путин впоследствии наградил британских спасателей «Орденом Дружбы»[8]. Оказание помощи при массовых бедствиях – еще одна область, в которой диалог может быть конструктивным и приносить пусть скромные, но конкретные результаты.

Форматы для дальнейшего взаимодействия

Помимо взаимодействия на двустороннем уровне участники дискуссии рассмотрели возможные форматы сотрудничества на многостороннем уровне. По мнению многих экспертов, возможности многосторонних институтов в урегулировании кризисов сильно преувеличены. Совет Россия–НАТО (СРН) подвергся критике за неспособность добиться деэскалации ситуации на Украине на ранней стадии конфликта. При этом, по мнению участников обсуждения, роль СРН нельзя преувеличивать. Хотя на начальном этапе его вмешательство могло бы сыграть положительную роль, окончательно разрешить конфликт помешала непримиримость позиций по вопросам безопасности, которые отстаивают Россия и НАТО. С одной стороны, расшире-

[8] 'Putin Honours Submarine Rescue Team', The Guardian, 5 октября 2005 г.

ние НАТО на Восток вызывает озабоченность у России, а с другой стороны, в НАТО не готовы отказаться от политики открытых дверей ради того, чтобы успокоить Россию. Москва считает программу НАТО «Расширенное передовое присутствие» провокацией, но для Североатлантического альянса эта программа – прямой ответ на действия России на Украине.

Это не означает, что СРН является бесполезной платформой, однако в настоящее время ему следует пересмотреть свои задачи из-за растущего расхождения в подходах к безопасности. Достижению этой цели могло бы содействовать реформирование и оживление деятельности рабочих групп СРН. Отношения между Россией и НАТО представляют собой очень сложную проблему, решить которую не удастся без налаживания контактов. Возможным вариантом является диалог между НАТО и Организацией Договора о коллективной безопасности (ОДКБ). Несмотря на традиционное нежелание НАТО участвовать в этом диалоге, для модификации зашедшего в тупик нынешнего формата необходимо искать новые творческие подходы.

Как было отмечено экспертами с обеих сторон, глубокое недоверие между Россией и государствами-членами НАТО препятствует достижению прогресса в развитии отношений уже на этапе выдвижения первоначальных инициатив. Например, в августе 2016 г. Россия предложила странам Балтии, Польше, Швеции и Финляндии обсудить меры безопасности в воздухе[9]. Литва и Эстония отклонили это предложение под предлогом того, что его истинной целью является раскол единства НАТО. Россия впоследствии ссылалась на этот факт как на пример отказа стран НАТО от реального сотрудничества по проблемам безопасности. Такой проблематичный подход и отклонение членами НАТО любой российской инициативы без дальнейшего обсуждения сегодня является обычной практикой при рассмотрении вопросов европейской безопасности.

Россию совершенно не устраивает нынешняя архитектура европейской безопасности, в которой доминирует НАТО при исключении России. Ранее России и НАТО удавалось наладить конструктивные двусторонние отношения, когда Россия в 1991 г. присоединилась к Совету североатлантического сотрудничества и в 1994 г. – к программе «Партнерство во имя мира», но этих мер в итоге оказалось недостаточно. Ключевая проблема заключается в том, что Россия и большинство европейских государств по-разному видят архитектуру региональной безопасности. В контексте последних событий становится понятным, что принимать во внимание интересы России в вопросах региональной безопасности западным партнёрам представляется затруднительным из-за политики Москвы в отношении таких стран как Грузия и Украина.

Тем не менее, по мнению российских экспертов, окончательное разрешение украинского кризиса остается малореальным без решения более общих вопросов формирования новой, всеобъемлющей и неделимой архитектуры европейской безопасности. Фактически, по их мнению, речь должна идти о

[9] Justyna Gotkowska and Piotr Szymański, 'Russia's "Niinistö Plan"', The Centre for Eastern Studies, 25 августа 2016 г.

пересмотре существующих на Западе с начала 1990-х гг. подходов, предполагавших укрепление безопасности в Европе преимущественно за счет географического расширения НАТО. Такие подходы должны быть заменены другими решениями, способными окончательно преодолеть раскол Европы и подвести черту под эпохой холодной войны.

Некоторые российские эксперты подчеркивали, что в современных условиях отсутствия единой архитектуры европейской безопасности, устраивающей как Россию, так и НАТО, основным институтом для ведения диалога по вопросам безопасности могла бы стать ОБСЕ. Однако эта организация так и не превратилась в такой региональный орган безопасности, о котором говорится в Главе VIII Устава ООН. Хотя структурированный диалог и картографирование военных учений в рамках ОБСЕ крайне важны для активизации дебатов по структуре и содержанию мер укрепления доверия, ее влияние и реализация любого конкретного достигнутого в рамках ОБСЕ соглашения, будут, скорее всего, носить весьма ограниченный характер. Деятельность ОБСЕ ограничена ее мандатом и может быть затруднена противоположными интересами ее членов. С этим сталкивается любая многосторонняя организация. Тем не менее ОБСЕ по-прежнему представляет собой серьезную платформу для диалога, но у этой организации есть определенные ограничения, которые следует признать.

В отсутствии перспективы заключения в краткосрочной перспективе формального соглашения об архитектуре европейской безопасности, на двустороннем уровне Россией и Великобританией могут быть предприняты определенные конкретные шаги и выдвинуты практические предложения. Продолжение диалога по вопросам европейской безопасности на широких многосторонних площадках, таких как ОБСЕ и Совет Россия–НАТО, попрежнему жизненно необходимо. Вместе с тем необходимы креативные реформы этих организаций, и двусторонние инициативы, если о таковых удастся договориться, могут придать импульс этому процессу.

Контроль над ядерными вооружениями

В ноябре 2017 г. в Москве в рамках двустороннего диалога РСМД–RUSI по вопросам безопасности состоялся второй семинар, на котором эксперты обсудили проблемы ядерных угроз и будущее контроля над ядерными вооружениями. Пример Северной Кореи рассматривался как геополитический вызов, затрагивающий в том числе и двусторонние российско-британские отношения. Хотя контроль над ядерными вооружениями является вопросом двустороннего российско-американского диалога, последствия возможного отказа от него затрагивают как Великобританию, так и Европу в целом. Более того, Россия рассматривает возможности США, дополненные потенциалом НАТО, и территорию государств-членов Североатлантического союза как стратегической плацдарм США, используемый в качестве «сильной передней позиции». Учитывая, что Великобритания входит в ядерную пятерку государств и НАТО, рассмотрение данного вопроса в двустороннем формате представляется весьма актуальным[10].

Рекомендации

- Контроль над вооружениями традиционно считался предметом переговоров между Россией и США. Необходимо обновление формата переговоров. Представляется целесообразным привлечь к обсуждению проблемы нераспространения ядерного оружия государства ядерной «пятерки». Хотя идея многостороннего контроля над вооружениями пока не находит широкой поддержки, необходимы усилия по расширению диалога по этому вопросу.
- Хотя размышления о роли технологий будущего и их влиянии на контроль над вооружениями являются непростой и зачастую неблагодарной задачей, они могут стать основой для рассмотрения возможных последствий технического прогресса для существующей системы контроля над ядерными вооружениями.
- Уже появились новые арены возможного ведения военных действий, связанные с использованием ядерного оружия, в частности, космос; новые виды оружия, в том числе гиперзвуковое, воздушные и подводные дроны; а также новые средства ведения войны, включая кибероружие. Все это расширяет эскалационные возможности сторон, что в итоге может привести к снижению ядерного порога и повысить угрозу войны.
- С появлением новых технологий меняются основополагающие параметры стратегической стабильности. Принимая во внимание существующие риски отказа от договоров по ядерным вооружениям, анализ политического мышления на Западе и на Востоке относительно перспектив сохранения

[10] The White House, 'National Security Strategy of the United States of America', декабрь 2017 г.

стратегической стабильности приобретает особую актуальность, включая разработку краткосрочных мер по снижения риска возникновения конфликтов.

- Ядерная угроза, исходящая от Северной Кореи, является общей проблемой для России и Великобритании. Однако пока не ясно, каким образом можно согласовать политические подходы двух стран к решению этой проблемы.

Великобритания признает, что Китай обладает наибольшим влиянием в ситуации с Северной Кореей, однако у России есть длительный опыт развития отношений с КНДР, и Россия может быть важным участником международных усилий по разрешению этой проблемы. Первым шагом в этом отношении может стать расширение обмена экспертными знаниями и информацией между Россией и ее международными партнерами относительно состояния и перспектив северокорейских ядерных и баллистических программ.

При обсуждении вопросов контроля над вооружениями было отмечено, что Договор о РСМД и Договор СНВ-3 находятся на грани срыва. Если одна из сторон откажется от Договора о РСМД, то переговоры о продлении срока действия Договора СНВ-3, срок действия которого истекает в феврале 2021 г., не будут продолжены. Крах этих договоров, помимо всего прочего, будет иметь негативные последствия для Конференции по рассмотрению действия Договора о нераспространении ядерного оружия (ДНЯО) в 2020 г.

Напряженность в связи с Договором о РСМД возникла из-за взаимных обвинений сторон в его нарушении. США выразили обеспокоенность развертыванием Россией крылатой ракеты наземного базирования (Новатор 9М729) с радиусом действия от 500 до 5500 км в нарушение положений Договора о РСМД. Это давняя проблема, поскольку испытания этой ракеты начались еще в 2008 г[11]. В ноябре 2016 г. обеспокоенность нарушением была озвучена на совещании Специальной комиссии по проверке, однако никакого прогресса в разрешении конфликта достигнуто не было[12].

Россия обвинила США в развертывании установки вертикального пуска Mk 41 *(Mark 41)* – компонента системы противоракетной обороны, которая, по мнению России, может использоваться для запуска наступательных крылатых ракет. Это произошло в нарушении Договора о РСМД. Россия также утверждает, что некоторые американские беспилотные летательные аппараты с летальным вооружением на борту являются по сути запрещенными Договором крылатыми ракетами, и что Америка продолжает нарушать Договор, используя ракеты средней дальности в качестве мишеней во время испытаний систем противоракетной обороны на европейском театре[13].

[11] Amy F Woolf, 'Russian Compliance with the Intermediate Range Nuclear Forces (INF) Treaty: Background and Issues for Congress', Congressional Research Service, 6 декабря 2017 г.

[12] Там же

[13] Ankit Panda, 'The Uncertain Future of the INF Treaty', Council on Foreign Relations, 21 декабря 2017 г.

Российские и британские эксперты обсудили вопрос о том, будет ли продуктивно вводить схему проверок двух ключевых вещей контроля над ядерными вооружениями, а именно – крылатой ракеты наземного базирования 9М729, разработанной и испытанной Россией, и американской системы вертикального пуска *Mark 41* для *Aegis Ashore*, в настоящее время развернутой в Польше и Румынии. Еще одной областью контроля над вооружениями, которая требует особого обсуждения, является тактическое ядерное оружие. Однако уровень доверия между странами сейчас настолько низок, что возможность выработки соглашения по этому вопросу на данный момент представляется весьма призрачной.

Москва и Вашингтон расходятся в способах выражения претензий и недовольства. По словам одного российского эксперта, Москва хотела бы действовать в рамках существующих каналов контроля над вооружениями, в то время как США, по мнению России, предпочитают действовать за их рамками. Эксперт пояснил, что в отношении Договора о РСМД проблемы следовало вынести на обсуждение в соответствующую Специальную контрольную комиссию, а не делать достоянием общественности претензии США по поводу возможных нарушении Россией положений Договора.

Позиция нового руководства США и его политическая риторика усиливают неопределенность в отношении приверженности США контролю над ядерными вооружениями. Хотя модернизация ядерного арсенала США была предложена еще администрацией Б. Обамы, Д. Трамп пообещал сделать потенциал ядерного сдерживания «намного сильнее и мощнее, чем когда-либо прежде»[14]. В недавно опубликованном «Обзоре ядерной политики США»[15] при освещении ряда вопросов содержатся прямые упоминания о России. В нем говорится о намерении создать тактические ядерные вооружения малой мощности для усиления сдерживания; разработать в ответ на разработку российской ракеты, нарушающую Договор о РСМД, крылатую ракету морского базирования, «не нарушающую обязательств по Договору»; а также рассмотреть возможность использования ядерного ответа на серьезный неядерный удар по, например, инфраструктуре США[16]. Законопроект по оборонной политике США от ноября 2017 г. предусматривает выделение 58 млн долл. в ответ на нарушение Россией Договора о РСМД, включая НИОКР по созданию собственной ракеты средней дальности[17].

Президент В. Путин, со своей стороны, подтвердил приверженность Москвы обязательствам по Договору о РСМД, но предупредил об ответе России, если США из него выйдут, практически заранее обвинив США в прекращении его действия. В своей речи на Валдайском форуме в октябре 2017 г. В. Путин упомянул Договор о РСМД: «Если кому-то он [Договор о РСМД]

[14] Gregory Hellman, 'Trillion-Dollar Nuclear Arms Plan Sets up Budget Brawl', Politico, 31 октября 2017 г.

[15] US Department of Defense, 'Nuclear Posture Review', февраль 2018 г.

[16] Aaron Mehta, 'Nuclear Posture Review Draft Leaks; New Weapons Coming Amid Strategic Shift', Defense News, 12 января 2018 г.

[17] Steven Pifer, 'Order from Chaos: U.S. Response to Russian Treaty Violation Plays into Moscow's Hands', Brookings Institution, 15 ноября 2017 г.

не нравится, и у кого-то есть желание выйти из договора вообще, с нашей стороны ответ будет мгновенным. Хочу об этом сказать и предупредить. Мгновенным и зеркальным»[18].

Помимо политической риторики и проводимой политики, которая все больше выглядит как де-факто отказ от контроля над вооружениями, проблема двусторонних соглашений о контроле над ядерными вооружениями времен холодной войны осложняется тем, что поддерживать налагаемые на двустороннем уровне ограничения становится все труднее в условиях, когда другие страны развивают свой собственный ядерный потенциал. Звучали предложения о заключении многосторонних соглашений, однако есть серьезные сомнения относительно политической готовности таких стран, как Китай, согласиться на сокращения или даже на контроль в отношении собственного ядерного потенциала. Даже заключение самых общих двусторонних соглашений между ядерными державами, помимо России и США, оказалось крайне трудной задачей. Тем не менее, это еще один вопрос, заслуживающий мозгового штурма на уровне дипломатии «второго трека», и последующего внесения его в формат обсуждений ядерной пятерки государств.

Как и при рассмотрении проблематики контроля над обычными вооружениями, обе стороны выразили озабоченность в связи с разрушением институциональных знаний о контроле над ядерными вооружениями. Потенциальной отправной точкой для исправления этой ситуации могло бы стать проведение совместных российско-британских исследований по экологическому и климатическому воздействию применения ядерного оружия для Европы на основе теории «ядерной зимы».

Новые технологии

Новые технологии меняют потенциал обычного, ядерного и альтернативного оружия, что не может не затрагивать соглашения о контроле над ядерными вооружениями. Новые технологии выносят на повестку дня вопрос о возможности намеренного или даже «непреднамеренного ядерного удара» в Европе, в частности, как вариант асимметричного ответа на действия потенциального противника, о чем говорится в ставшем достоянием общественности «Обзоре ядерной политики США». В ходе обсуждения было отмечено, что при коллективном обсуждении способов борьбы с текущими угрозами целесообразно рассмотреть отдельные сценарии развития кризисных ситуаций с целью определения механизмов сдерживания новых общих угроз.

Появляющиеся новые инструменты влияют на безопасность систем доставки ядерных боеприпасов. Потенциальная возможность, например, для террористов, с помощью кибервозможностей получить доступ к контролю над системами доставки ядерного оружия, означает, что вопрос контроля над ядерными вооружениями не только по-прежнему сохраняет актуальность,

[18] Выступление Президента России на заседании Международного дискуссионного клуба «Валдай», 19 октября 2017 г.

но и сталкивается с новыми угрозами, которые затрагивают все ядерные державы. Все большее беспокойство вызывает опасность взлома систем управления ядерными объектами государства другими странами.

Говоря о космосе, один британский эксперт отметил, что в развитии новых технологий имеется, по крайней мере, один положительный аспект, а именно – появление более широкого спектра методов проверки. Так, если бы Индия, к примеру, провела ядерные испытания, то их вряд ли удалось бы это скрыть, учитывая, «как много в космосе глаз». Участники дискуссии выразили мнение, что принципы соглашений о контроле над вооружениями времен холодной войны, которые выглядят в наши дни все более «анахроничными», тем не менее по-прежнему могут использоваться в качестве образца при обсуждении правил и методов проверки для новых технологий с тем, чтобы успешно противостоять новым вызовам.

В 2014 г. Россия и Китай представили обновленный проект своего Договора о предотвращении размещения оружия в космическом пространстве. США отвергли его по многим причинам, прежде всего из-за отсутствия надлежащих, по их мнению, механизмов проверки, а также из-за отсутствия ограничений на разработку противоспутникового оружия на земле[19]. Как отметил один участник из Великобритании, спектр технических особенностей слишком широк, чтобы найти адекватное отражение в проекте, но данная инициатива, в случае ее принятия, знаменовала бы собой начало нового диалога по предотвращению конфликтов. Хотя в нынешней политической реальности рассчитывать на заключение соответствующего юридически обязывающего соглашения вряд ли возможно, но для предотвращения конфликта обсуждение этих проблем на экспертном уровне необходимо.

Британские и российские эксперты обсудили наметившиеся тенденции к пересмотру основ традиционной концепции стратегической стабильности. Учитывая риски отказа от договоров по сокращению ядерных вооружений, требуется дополнительный анализ факторов, влияющих на формирование политических подходов сторон в сфере стратегической стабильности в краткосрочной перспективе, что могло бы стать одной из тем для дальнейшего российско-британского экспертного обсуждения.

Северная Корея

В ходе групповой дискуссии участники обсудили проблему ядерной угрозы со стороны Северной Кореи, и то, как Россия и Великобритания могли бы найти точки соприкосновения для решения этой проблемы, Северная Корея, обладающая ядерным оружием, является предметом озабоченности и России, и Великобритании. Однако сложность заключается в определении того, в какой степени и в каких направлениях обе стороны готовы действовать сообща для разрешения этой проблемы. Совет Безопасности ООН одобрил санкции в отношении КНДР, однако британской стороной отмечалось, что в России есть лица и компании, которые эти санкции

[19] Jeff Foust, 'U.S. Dismisses Space Weapons Treaty Proposal as "Fundamentally Flawed"', Space News, 11 сентября 2014 г.

нарушают. В силу особенностей политической конъюнктуры и специфики опыта двусторонних отношений с Пхеньяном, реакции России и Великобритании на политику Северной Кореи не совпадают. Вместе с тем имеются конкретные проблемы, решение которых могло бы лечь в основу диалога. В частности, к ним относится предотвращение утечки ядерных и баллистических технологий и компонентов ядерного оружия Северной Кореи в другие страны.

В ходе обсуждения проблематики Северной Кореи у некоторых участников диалога складывалось ощущение, что некоторые предложения или соглашения используются, скорее, для обострения ситуации, чем для того, чтобы действительно найти конструктивный путь решения проблемы. Так, выдвинутая Россией и Китаем идея «двойной заморозки» представляется Великобритании «неискренней». Прекращение американо-южнокорейских учений или сворачивание их масштабов не является решением проблемы, и Россия, по мнению Запада, должна это понимать. Российские эксперты, со своей стороны, отмечали, что у Северной Кореи есть объективные причины для опасений в отношении своей безопасности, и что любое решение ядерной проблемы должно рассматриваться в более широком контексте обеспечения стабильной, предсказуемой и всеобъемлющей системы безопасности на Корейском полуострове. С российской стороны была также высказана точка зрения, что решение ядерной проблемы Северной Кореи должно рассматриваться не как ближайшая, а как долгосрочная задача, а ближайшей задачей следует считать снижение напряженности на Корейском полуострове. Российские и британские эксперты согласились с тем, что переговоры с Пхеньяном необходимо продолжить хотя бы потому, что других предложений по достижению общей цели сделать Корейский полуостров безъядерным просто нет.

Большинство экспертов согласилось с тем, что добиться от Северной Кореи разоружения в ближайшей перспективе не удастся, учитывая, насколько далеко Пхеньян продвинулся в развитии своей ядерной программы. Таким образом, придется взаимодействовать с Пхеньяном как с де-факто ядерным государством. Ключевая опасность заключается в ограниченном опыте взаимодействия Северной Кореи с государствами мира и недостаточных знаниях международного сообщества об этой стране. По словам одного российского эксперта, Пхеньян имеет весьма смутное представление о том, как в США принимаются политические решения. С другой стороны, международные оценки положения дел в самой Северной Корее также оставляют желать лучшего. Это потенциально увеличивает риск просчетов.

Хотя главным партнером Пхеньяна считается Пекин, эксперты отметили, что Москва обладает серьезным политическим весом в Северной Корее. По словам одного британского эксперта, Великобритания, в отличие от США, это признает. Кроме того, Великобритания является одной из немногих стран, имеющих дипломатическое присутствие в Пхеньяне. Общая заинтересованность в побуждении Пхеньяна к началу переговоров могла бы стать основой

для обмена существующим опытом во взаимодействии с северокорейским руководством.

Это не означает, что Россия или Великобритания могут существенно воздействовать на позицию Северной Кореи, поскольку главной иностранной державой, обладающей рычагами влияния на КНДР, является Китай. Однако и Россия, и Великобритания заинтересованы в стабилизации положения на Корейском полуострове. Россия заинтересована в реализации своих экономических и энергетических проектов, в частности в прокладке запланированного газопровода через Северную Корею. Более того, другим странам тоже надлежит использовать имеющиеся у них возможности для активизации своей работы с Северной Кореей, поскольку есть большие сомнения, что Китай помимо выполнения решения о международных санкциях будет делать что-то еще, чтобы не допустить выхода ситуации из-под контроля. Северная Корея, в свою очередь, стремится проводить более независимую от Китая политику, о чем свидетельствует изменение Ким Чен Ыном стиля своего руководства и прошедшая чистка высших эшелонов северокорейского руководства от проводников китайского влияния.

Кибербезопасность: сфера общих интересов?

Ввиду того, что кибер-/информационная безопасность становится одним из приоритетов для государственного и частного сектора, страны стремятся занять проактивную позицию и бороться с кибератаками. Как и в других актуальных для российско-британских отношений вопросах безопасности, взаимодействие в киберсфере определяется политическими факторами. В 2017 г. причиной антагонизма в этой области стали обвинения в адрес России в том, что она использовала кибер-прокси для вмешательства в выборы в США и странах Европы. Хотя в условиях возникшей политической напряженности заключение любого соглашения о правилах поведения в киберпространстве представляется маловероятным, данная тематика придает новый импульс участию экспертов в широких дискуссиях по решению ключевых проблем, связанных с киберпространством. К ним относятся восприятие угроз, атрибуция кибератак, а также юридические и технические барьеры на пути сотрудничества по представляющим общий интерес проблемам, например, по путям противодействия киберпреступности.

В настоящее время на политическом уровне наблюдается кризис доверия. Тем не менее в работе третьего семинара, проведенного РСМД и RUSI в рамках двустороннего российско-британского диалога по безопасности, приняли участие эксперты из частного сектора и академических кругов, а также бывшие сотрудники профильных ведомств обеих стран. Участники семинара поделились своими взглядами на киберугрозы и обсудили варианты налаживания более конструктивного взаимодействия для противодействия таким угрозам, особенно в частном секторе.

Рекомендации

- Хотя на сегодняшний день дискуссии по нормам в киберпространстве увенчались заключением лишь отдельных конкретных соглашений, они полезны для понимания подходов стран к проблемам и угрозам в этой сфере. И все же, эти дискуссии должны быть ориентированы на достижение практических результатов. Учитывая очевидную полезность киберинструментов для государств и сложность выработки общего понимания оборонительной, сдерживающей и наступательной деятельности в киберпространстве, а также процесса атрибуции, рассчитывать на согласование международных норм, не говоря уже об их соблюдении на практике, не приходится.
- На правительственном уровне логичной инициативой представляется создание российско-британской «горячей линии» для информирования о

преступной деятельности в киберпространстве, что особенно актуально в связи с проведением в России Чемпионата мира по футболу летом 2018 г. В силу политических причин и соображений безопасности, обмен информацией между правоохранительными органами России и Великобритании является сложной задачей, однако при наличии общей угрозы сотрудничество может осуществляться по политическим каналам, не связанным с правоохранительной деятельностью, либо через третьи страны.

- Операция, которая привела к разгрому преступной кибергруппировки *Avalanche* («Лавина»), показывает, насколько эффективным может быть межюрисдикционное, государственно-частно-некоммерческое сотрудничество. Своим успехом оно обязано взаимодействию правоохранительных органов нескольких стран; многосторонним правоохранительным организациям, в том числе Европолу; частному сектору и таким некоммерческим организациям, как российский Координационный центр национального домена, администрирующий национальные домены .ru и .rf , а также *ICANN* и *Shadowserver*. Хотя проведение операции заняло несколько лет и потребовало больших ресурсов, она продемонстрировала преимущества многостороннего подхода в борьбе с преступностью.
- Совершенствование юридического процесса для обмена информацией было бы выгодно обеим сторонам. И Россия, и Великобритания подписали Европейскую конвенцию 1959 г. о взаимной правовой помощи по уголовным делам. Более того, стороны подписали Меморандум о взаимопонимании между Генеральной прокуратурой Российской Федерации и Королевской прокурорской службой Англии и Уэльса. Эти правовые форматы могут и должны использоваться при расследовании киберпреступлений. Хотя использование правовых инструментов может оказаться громоздким и трудоемким процессом, они создают прочную основу для двусторонних действий по борьбе с киберпреступностью и решению существующих проблем.
- Представляется целесообразным изучить также и другие форматы и механизмы для конструктивного сотрудничества между государственным и частным секторами на национальном и международном уровнях. Было высказано мнение, что удобным форматом для более тесного взаимодействия на межгосударственном уровне могли бы быть группы быстрого реагирования на нарушения компьютерной безопасности *(CERT)*, хотя они и не обладают правоприменительными полномочиями и ограничены в своей деятельности. Платформой для сотрудничества могут также служить Европол и Интерпол.
- Желательно улучшить каналы обмена информацией между бизнес-структурами. Некоторые участники отмечали, что при наличии подозрений о возможной преступной деятельности или мошенничестве, частный сектор не всегда готов на серьезные меры, поскольку это может негативно отразиться на имидже компании. Именно поэтому в подобных ситуациях компании предпочитают решать проблемы в неформальном ключе, полагаясь на личные связи. Там, где это позволяет законодательство, следует

поощрять межкорпоративное *(B2B)* взаимодействие в решении проблем кибербезопасности. Свой вклад в эту деятельность могут внести существующие каналы и площадки, в том числе торговые палаты двух стран.

Сотрудничество на государственно-частном уровне жизненно важно для обеих стран, несмотря на недавние разногласия в отношении отдельных компаний. Эту работу необходимо активизировать как на государственном, так и на международном уровнях.

Кибер- и информационная безопасность: различия в подходах

Концептуальные подходы России и Великобритании к кибертематике существенно разнятся. Базовые расхождения в интерпретации понятий отражены в доктринах двух государств.

Российская Доктрина 2016 г. посвящена обеспечению национальной безопасности Российской Федерации в информационной сфере. Под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений[20]. В официальных документах России приставка/термин «кибер» не используется.

Как подчеркнул один российский эксперт, Доктрина информационной безопасности РФ, а также другие стратегические документы по информации и национальной безопасности основаны на концепции информационной сферы. Россия рассматривает информационную безопасность как неотъемлемую часть стратегической стабильности, что, бесспорно, гораздо шире многих западных трактовок этого понятия.

Эксперт также отметил, что подход Великобритании, так же как и в США и ЕС, ориентирован главным образом на защиту жизненно важной инфраструктуры и других ресурсов в киберпространстве. Поскольку обеспокоенность Москвы дестабилизирующим воздействием трансграничных информационных потоков обычно наталкивается на нежелание западных партнеров принимать ее во внимание, руководители МИДа России и другие высокопоставленные лица, ответственные за принятие решений, рассматривают продвижение концепта кибербезопасности как попытку проигнорировать ее национальные интересы и опасения по поводу безопасности в информационном пространстве.

Таким образом, Россия видит угрозу в возможности применения информации в качестве оружия или ее использования в военных целях иностран-

[20] Министерство иностранных дел Российской Федерации. «Доктрина информационной безопасности Российской Федерации», 5 декабря 2016 г.

ными государствами, террористическими и экстремистскими группами или преступниками. Доктрина направлена, главным образом, на противодействие этой угрозе путем повышения эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности и совершенствованием функционирования системы ее обеспечения.

В Стратегии национальной кибербезопасности Великобритании на 2016-2021 гг. тоже говорится об информационной безопасности, но имеется в виду защита данных от злонамеренных действий или утечек, а не использование информации в качестве оружия. Основное внимание в Стратегии уделяется кибератакам как главной угрозе и необходимости улучшения кибербезопасности, а именно «защите информационных систем (аппаратного и программного обеспечения и связанной с ними инфраструктуры), данных о них и предоставляемых ими услуг от несанкционированного доступа, причинения вреда или неправильного использования»[21]. В этой Стратегии перечисляются возможные злоумышленники: киберпреступники; иностранные государства и спонсируемые ими угрозы; террористы; «хактивисты» и «скрипт-кидди» (неопытные хакеры. – *Прим. ред.*). Таким образом, Великобритания разделяет мнение России, что угрозы исходят от других государств и от отдельных преступников.

В Стратегии национальной кибербезопасности Великобритании содержатся положения, по которым трудно согласовать «правила игры». Это относится к описанию мер по защите и сдерживанию, что особенно актуально для переговоров с Россией. И Россия, и Великобритания подчеркивают важность мер защиты, однако линии разграничения между наступательными, защитными и сдерживающими мерами достаточно размыты. Например, в Стратегии говорится об активной киберзащите, под которой имеется в виду «реализация мер безопасности для укрепления защиты сетей или систем с целью повышения их устойчивости к атакам». Это проактивный подход, направленный на усложнение доступа к британским сетям, и, по мнению экспертов, грань между наступательной и защитной деятельностью может временами стираться. Британские эксперты также привели пример определенных действий России, которые могут быть расценены как разновидность активной киберзащиты. Так, Россия разрабатывает законодательство, среди целей которого обеспечение к 2020 г. прохождения большей части интернет-трафика через территорию страны[22]. По словам одного британского эксперта, в их глазах «это выглядит как активная киберзащита».

Лишь один российский эксперт высказал мнение, что можно достичь понимания по этому вопросу – остальные участники сочли это нереальным. И все же, эволюция угроз может предоставить некоторое пространство для двустороннего диалога. Так, сегодня для обеспечения кибербезопасности глобальная ИТ-индустрия переключает свое внимание с классической три-

[21] Правительство Великобритании. Стратегия национальной кибербезопасности Великобритании на 2016-2021 гг. 1 ноября 2016 г.

[22] Минкомсвязи России. Государственная программа «Информационное общество».

ады сервисов КЦД (конфиденциальность, целостность и доступность) на обеспечение устойчивости к кибератакам. Последнее подразумевает, что в настоящее время не существует способа предотвратить все компьютерные атаки и другие инциденты, связанные с нарушением безопасности, поэтому информационные системы и инфраструктура должны быть способны выполнять критические (жизненно важные) функции даже при атаке или во время инцидента. Концепция и понятие киберустойчивости подчеркиваются в Стратегии национальной кибербезопасности Великобритании на 2016-2021 гг. В то же время, подобные концепции нашли отражение в недавнем всплеске регламентирующей деятельности в России, направленной на обеспечение безопасности критически важной информационной инфраструктуры *(CII)* и передовой практики в частном секторе. Тем не менее участие государства в кибердеятельности будет по-прежнему означать сложность любых обсуждений подобных вопросов.

По мнению отдельных российских экспертов, положение дел в информационном киберпространстве является серьезным вызовом международной безопасности и, следовательно, требует коллективного рассмотрения международным сообществом. Это пространство все больше превращается в мутные воды, в которых всевозможные акторы, в том числе преступники и террористы, могут безнаказанно преследовать свои цели. Как и любая другая область международных отношений, глобальное информационное киберпространство требует согласованного международно-правового регулирования. В частности, необходимо разработать универсальный набор юридических норм, имеющих обязывающую силу, в котором были бы прописаны обязательства государств, установлены процедуры определения нарушений норм и выявления виновных. Необходимо согласовать процедуры мирного разрешения споров, включая создание сети соответствующих национальных и многосторонних механизмов. Разумеется, достижение этих целей может потребовать много времени. Ряд российских экспертов считает возможным, в случае необходимости, разработать поправки к существующим международным документам по предотвращению международных конфликтов и разрешению споров. По логике вещей, это потребует определения границ суверенитета государств в этом пространстве. Несколько участников подчеркнули, что серьезный кризис в российско-американских отношениях, вызванный обвинениями во вмешательстве России в политический процесс в США, должен стать дополнительным стимулом для проведения такого диалога.

Сложности в определении «правил игры»

Учитывая концептуальные различия в подходах России и Великобритании к вопросам кибербезопасности, а также неясность в отношении разграничения защитных и наступательных мер, вряд ли стоит ожидать каких-либо официальных переговоров между двумя странами по этим проблемам. Интересно отметить, что различие в подходах по отношению к вопросам кибербезопасности присуще не только российско-британским отношениям. Даже среди союзных западных стран нет единого мнения, как определять

угрозы и противодействия. Например, законопроект Конгресса США предлагает официально разрешить компаниям взламывать сети хакеров *(hack back)*, называя это активной киберзащитой, что демонстрирует широту разброса мнений по этому вопросу в концептуальном и правовом плане[23]. Кроме того, США рассматривают возможность применения ядерного оружия против страны или группы, которые нанесут серьезный кибердар по критической инфраструктуре США[24].

Актуальность проблемы разработки норм отнюдь не обязательно вызвана исключительно текущим кризисом в отношениях между Россией и Западом. Скорее, сложность проведения «красных линий» в виртуальном мире носит универсальный характер, в первую очередь в силу того, что враждебные действия могут быть произведены под предлогом противодействия определенной силе или злому умыслу. Более того, определенные действия, воспринимаемые как враждебные, могут быть названы эффективной мерой защиты или сдерживания в зависимости от того, кто и как их использует. В глазах отдельных кибер-агрессоров, проведение «красных линий» или четкое отделение определенных секторов критической инфраструктуры будет означать установление границы, за пределами которой можно активно действовать, не опасаясь серьезных ответных мер. Определение межгосударственных норм в отношении киберпространства будет по-прежнему представлять значительную сложность. Главным образом потому, что, как отметил один из участников, они представляют слишком большую ценность, чтобы государства не использовали их в определенных ситуациях.

Дополнительная сложность возникает при определении источника любой враждебной деятельности или атаки. Нормы можно согласовать, однако определить время и источник их нарушения представляется весьма непростой задачей, поскольку атрибуция представляет собой, по выражению одного участника, сложнейшую головоломку. В силу того, что источник кибератаки можно скрыть, используя разные IP-адреса и VPN, а геолокация может быть сфальсифицирована *(false-flag operations)*, вероятность ошибки весьма велика. Это может свести на нет любые законные попытки обосновать обвинения и нанесение ответного удара.

Даже если нормы и будут выработаны, то механизмы обеспечения их соблюдения на международном уровне вряд ли будут работать на практике. Самые известные инициативы по этому вопросу включают работу, проделанную Группой правительственных экспертов (ГПЭ) ООН, и Таллиннское руководство по международному праву, применимому при ведении кибервойны. В последнем демонстрируется, в частности, как международное право и самооборона могут применяться в отношении кибероперациий, однако зачастую страны толкуют данные концепции по-разному во многом ради извлечения политических дивидендов, да и реальные механизмы обеспе-

[23] Congressman Tom Graves, 'Representative Tom Graves Proposes Cyber Self Defense Bill', Пресс-релиз от 3 марта 2017 г.

[24] David E Sanger, 'Nations Seek the Elusive Cure for Cyberattacks', New York Times, 21 января 2018 г.

чения соблюдения норм тоже отсутствуют. Более того, Китай и Россия не высказывают особой поддержки встраиванию положений по деятельности в киберпространстве в существующие форматы международного права, к которым у них имеются свои претензии. Инициативы, подобные Будапештской конвенции Совета Европы[25], предлагают законодательные нормы по борьбе с враждебной деятельностью в киберпространстве. Россия Конвенцию не подписала, не согласившись со статьей 32, которая разрешает трансграничный доступ к хранимым компьютерным данным во время расследования киберпреступлений, и предпочла работу в рамках ООН для разработки собственного проекта.

Один российский эксперт отметил, что проект Конвенции ООН «О сотрудничестве в сфере противодействии информационной преступности», представленный Россией в Вене в 2017 г., стал очередной попыткой вынести рассмотрение этого вопроса на международный уровень, а именно – на уровень ООН[26]. Проект криминализует 14 видов деятельности в Интернете, включая незаконный перехват и изменение данных, организацию сбоев в работе компьютерных сетей, создание вирусов и вредоносных программ, киберкражи, нарушение законов об авторском праве, распространение детской порнографии и т.д. Кроме того, эксперт подчеркнул, что одним из важных аспектов этой инициативы является предлагаемый подход к решению этих проблем. Он базируется на уважении национального суверенитета и не допускает трансграничного доступа к сохраненным данным для нужд расследования без надлежащего разрешения. Судя по всему, на данный момент проект не получил поддержки подавляющего большинства членов международного сообщества, но его появление вполне соответствует проводимому Россией курсу на решение глобальных проблем посредством использования официальных многосторонних каналов и площадок. Между тем, в отсутствие общепризнанного правового инструмента, сотрудничеству в области борьбы с киберпреступностью при наличии благоприятного геополитического контекста способствуют договоры о взаимной правовой помощи (ДВПП), альтернативные региональные или двусторонние соглашения, а также менее официальные каналы.

Определенных успехов можно добиться и в двустороннем формате. На двустороннем уровне были достигнуты некоторые договоренности. Например, в апреле 2015 г. Россия подписала соглашение с Китаем о сотрудничестве в области международной информационной безопасности[27]. На саммите БРИКС в Китае в сентябре 2017 г. Россия подписала аналогичное соглашение с Южной Африкой[28]. США и Великобритания сотрудничают по вопросам кибер-

[25] Council of Europe, 'Convention on Cybercrime' Budapest, 23 ноября 2001 г.

[26] Сообщение телеканала «RT» «Россия готовит новую Конвенцию ООН по борьбе с киберпреступностью, 14 апреля 2017 г.

[27] Подписание Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной нформационной безопасности. Правительство России.

[28] О подписании Соглашения между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности; 1622, Пресс-релиз от 4 сентября 2017 г.

безопасности, в частности, путем обмена разведывательными данными[29]. Очевидно, соглашения по кибервопросам проще заключить на двустороннем уровне, чем на многостороннем, правда, они могут носить довольно расплывчатый и больше символический, чем практический характер.

Это не означает, что обсуждение норм или правил лишено смысла, однако всегда нужно иметь ясное представление, каких конкретно решений и договоренностей от него следует ожидать. Вместе с тем, подобный диалог предоставляет полезные каналы коммуникации, позволяющие лучше понять концептуальное мышление и интересы вовлеченных государств. Чтобы дискуссии о нормах проходили в практической плоскости, следует помнить, что киберпространство – еще одна сфера борьбы за получение конкурентных преимуществ, подобная земле и морю.

Другой российский эксперт отметил, что, по мнению многих, существующий подход к проведению красных линий, определению критической инфраструктуры, объектов атаки и обороны и т.д. с течением времени упрощается и становится самоочевидным, поскольку киберсфера становится пространством вооруженной борьбы, а киберинструментам придается наступательный характер. Однако, по его мнению, этого в действительности не происходит в силу, прежде всего, самой природы кибер- (и информационного) пространства. Стратегическая двусмысленность (как в техническом, так и юридическом плане), которая отличает действия акторов в виртуальном пространстве, не может служить отправной точкой для разработки договоров о контроле над кибероружием.

Также эксперт добавил, что, хотя военные операции в киберпространстве становятся естественной частью полномасштабного конфликта, их трудно отделить от военных действий с применением обычных видов оружия. Именно поэтому проблема сводится к определению рамок допустимого кибер- и информационного вмешательства в мирное время, и для решения этого вопроса нужно выработать соответствующие правила и нормы.

Принимая во внимание сложность межгосударственного сотрудничества по этим вопросам, необходимо поощрять и усиливать существующий диалог между техническими сообществами.

Привлечение частного сектора и технической экспертизы

Несмотря на политическую напряженность между странами, Россия и Великобритания сталкиваются с общими угрозами, исходящими из киберпространства. Хотя отдельные политики по-прежнему не верят в возможность сотрудничества России и Великобритании в этой сфере из-за низкого уровня доверия между ними, такие угрозы вполне реальны и не признают границ. Например, криминальная хакерская группировка *Cobalt* атаковала банки в России, Великобритании, Нидерландах и Малайзии[30]. *MoneyTaker*

[29] The White House, 'FACT SHEET: U.S.–United Kingdom Cybersecurity Cooperation', Пресс-релиз от, 16 января 2015 г.

[30] Отчет Group-IB о деятельности группы Cobalt, атаковавшей банкоматы в странах Европы и Азии, используя новый «бесконтактный» метод.

нанес удар по российской финансовой системе, а также банкам США и британскому поставщику финансового программного обеспечения[31]. Не менее важным представляется и анализ потенциальных угроз, поскольку террористические группы усиливают свои наступательные возможности в киберпространстве.

Определенные шаги могут быть предприняты на правительственном уровне. Так, логичной инициативой выглядит создание российско-британской «горячей линии» для информирования о преступной деятельности, что особенно актуально в связи с проведением в России Чемпионата мира по футболу летом 2018 г. Как только линия будет установлена, должны быть четко определены правила ее работы.

Вместе с тем, конкретные примеры успешной борьбы с преступностью с помощью конструктивного диалога и практического сотрудничества свидетельствуют об эффективности привлечения частного сектора и обмена техническим опытом. Операция, которая привела к разгрому преступной кибергруппировки *Avalanche* («Лавина») служит идеальной иллюстрацией того, как может и должно работать сотрудничество. Своим успехом оно обязано взаимодействию правоохранительных органов нескольких стран; многосторонним правоохранительным организациям, в том числе Европолу; частному сектору; и таким некоммерческим организациям, как *ICANN* и *Shadowserver*. Некоммерческие организации могут быть особенно полезны в качестве посредников между третьими сторонами, помогая странам, которые не могут работать сообща по политическим соображениям.

Однако и проведение подобных операций не лишено своих сложностей. При проведении операции по ликвидации группировки *Avalanche*, стороны столкнулись длительными юридическими процедурами, необходимыми для проведения совместной работы в соответствии с ДВПП. Пусть это и замедлило процесс, операция прошла успешно, пусть и длилась более четырех лет. Полезным было бы оптимизировать процесс обмена информацией, когда того требуют обстоятельства. Для проведения подобных операций также требуются долгосрочные инвестиции. Правоохранительные органы и частный сектор должны быть готовы инвестировать в подобные проекты и время, и ресурсы.

Другая проблема связана с совместимостью правовых систем для борьбы с правонарушениями, наносящими ущерб на территории нескольких государств. Правоохранительные органы Великобритании не могли полноценно участвовать в операции *Avalanche* из-за отсутствия внутреннего законодательства, регулирующего подобные ситуации. В Германии применялись положения уголовного законодательства, в США принятие мер осуществлялось в рамках гражданского законодательства. В то время регламент *CCTLD* не позволял организации участвовать, поэтому она действовала на свой страх и риск. Позднее ее правление приняло соответствующие нормативные

[31] Отчет Group-IB «MoneyTaker: в погоне за невидимкой», 11 декабря 2017 г.

документы, показав тем самым пример доброй воли, которая окупилась в готовой к взаимодействию среде.

Представляется целесообразным продолжить обсуждение вопроса о площадках, а также механизмах и методах сотрудничества, которые можно было бы использовать как для работы внутри страны, так и на двусторонней основе. По мнению экспертов, хорошим форматом для более тесного взаимодействия служат группы быстрого реагирования на нарушения компьютерной безопасности *(CERT)*. Однако тут имеются свои ограничения. Группы *CERT* не всегда имеют право действовать, особенно когда встает вопрос о необходимости осуществления правоприменительной деятельности. Политическая напряженность между Россией и Великобританией может осложнять взаимодействие правоохранителей обеих стран по официальным каналам, однако оно может осуществляться либо по иным политическим каналам, либо через третьи страны. Определенную помощь могло бы оказать использование менее формальных акторов. В успех операции *Avalanche* большой вклад внесли некоммерческие организации, обладающие большими экспертными знаниями и опытом, но некоторые государства не считают НКО полноправными легитимными субъектами международного сотрудничества.

Частный сектор зачастую более гибок в процессе принятия решений, что может повысить эффективность их действий по сравнению с государственными структурами. Вместе с тем, для эффективного противодействия рискам необходимо укрепить каналы обмена информацией между заинтересованными акторами из частного сектора и повысить их мотивацию к такому обмену. Некоторые участники отмечали, что при наличии подозрений о преступной деятельности или мошенничестве, частный сектор не всегда готов к жестким действиям, поскольку это становится достоянием общественности и может негативно отразиться на имидже компании. Именно поэтому в подобной ситуации представители бизнеса предпочитают решать проблемы в неформальном ключе, полагаясь на личные связи. Там, где это позволяет законодательство, необходимо стимулировать межкорпоративное взаимодействие в решении проблем кибербезопасности. Однако его одного будет недостаточно для судебного преследования или сдерживания, что диктует необходимость объединения усилий частного и государственного секторов.

IT-компании нередко сталкиваются с аналогичными проблемами, независимо от своего местонахождения. Так, представитель одной российской компании отметил отсутствие сотрудничества в сфере обмена знаниями и борьбы с поддельными аккаунтами. Если есть доказательства использования конкретной учетной записи в мошеннической схеме или любом другом противоправном действии, то возможные действия ограничиваются лишь информированием или обращением в службу поддержки в надежде на удачный исход. Для тех, кто работает в сфере борьбы с мошенничеством и противоправными действиями в цифровом поле, должна существовать структура для обмена информацией о вредоносных действиях. Это помо-

жет интернет-провайдерам принять в отношении поддельных аккаунтов для безопасности интернета меры.

России и Великобритании следует повысить уровень доверия между государственным и частным сектором. Кроме того, существуют опасения, что борьба с киберпреступностью передается на аутсорсинг частному сектору. Как выразился один британский эксперт, «задача частного сектора – обеспечить безопасность своих клиентов, а не ловить преступников». Отношения государственного и частного сектора в этом пространстве отличают бесконечные споры и разногласия.

Риски частного сектора

Несмотря на то, что возможности укрепления межкорпоративного сотрудничества и взаимодействия между государственным и частным сектором присутствуют, существует немало препятствий для достижения тесных связей в отношениях России с Великобританией и Западом в целом. Прежде всего, это подозрения по поводу политического вмешательства в деятельность частных фирм и программное обеспечение. В качестве меры противодействия в 2015 г. Россия запретила покупку программного обеспечения иностранного производства для нужд правительства. Хотя это и было сделано в рамках российской политики импортозамещения[32], в немалой степени причиной была обеспокоенность тем, что программное обеспечение иностранных компаний может быть использовано для подрыва российской кибербезопасности.

Самым нашумевшим делом на Западе стало обвинение «Лаборатории Касперского» в связях с российскими спецслужбами. Это привело в США *(US DHS BOD 17-01)*[33] и Великобритании (письмо Центра национальной кибербезопасности постоянным секретарям)[34] к публичному и недвусмысленному указанию на риски, связанные с использованием антивирусных продуктов «Лаборатории Касперского» в правительственных ведомствах, а США вычеркнула эту компанию из утвержденных списков поставщиков. Озвученные опасения со стороны США и Великобритании сводились, в основном, к тому, что это российский продукт, занимает большой объем памяти, и что есть подозрения о связях компании с российской разведкой.

В ходе семинара представитель «Лаборатории Касперского» выступил в защиту компании, заявив, что она передает данные только в рамках выполнения своих контрактных обязательств; что нет никаких доказательств, подтверждающих обвинения в связях компании с какими-либо российскими должностными лицами; и что, поскольку «Лаборатория Касперского» не

[32] Минкомсвязи России «Об утверждении плана импортозамещения программного обеспечения». Министерство связи и массовых коммуникаций Российской Федерации.

[33] Department of Homeland Security, 'DHS Statement on the Issuance of Binding Operational Directive 17-01', Пресс-релиз от 13 сентября 2017 г.

[34] National Cyber Security Centre, 'Letter to Permanent Secretaries Regarding the Issue of Supply Chain Risk in Cloud-Based Products', 1 декабря 2017 г.

является телекоммуникационной компанией, она не обязана предоставлять российским властям данные в соответствии с недавно принятым законодательством[35] (как утверждают США). «Лаборатория Касперского» подала иск, заявив, что обвинения в адрес фирмы «основаны на слухах и голословных утверждениях, не имеют под собой существенных доказательств» и нарушают ее право на надлежащее судопроизводство[36].

В настоящее время компания запускает глобальную инициативу по информационной открытости *(Global Transparency Initiative)*, направленную на совершенствование политики и практики информационной безопасности. Начальный этап реализации инициативы включает открытие по всему миру центров прозрачности, в которых доверенные партнеры смогут получить информацию о программном коде «Лаборатории Касперского», обновлениях продуктов, правилах обнаружения угроз и прочей деятельности, а также провести независимую оценку процесса безопасной разработки и стратегии по минимизации рисков в цепочке поставщиков и в программном обеспечении.

Вместе с тем было отмечено различие подходов Великобритании и США при оценке рисков использования продуктов «Лаборатории Касперского». Центр национальный кибербезопасности Великобритании *(NCSC)* совместно с «Лабораторией Касперского» обсудил механизм, позволяющий осуществить независимую верификацию безопасности продуктов и сервисов российской компании, что было по достоинству оценено последней. В отличие от британцев, американцы отказались от обсуждения с «Лабораторией Касперского» выдвинутых ими обвинений. Проблема заключается в том, что обоснование рисков, воспринимаемых как высокие, которые связаны с определенными видами деятельности в частном секторе, не обязательно должно подкрепляться публичными твердыми доказательствами. Власти при этой оценке могут опираться на конфиденциальную информацию или не желать раскрывать данные и механизмы, которые используются для определения такого риска.

И все же этот случай в очередной раз подтверждает, что при наличии подобных проблем возможность взаимодействия в определении рисков с соответствующим актором частного сектора имеется. Как сообщил глава *NCSC* Киарон Мартин, «мы обсуждаем с «Лабораторией Касперского»… возможность выработки механизма, который позволит нам и другим (ведомствам. – *Прим ред*.) осуществлять независимую верификацию безопасности продуктов и сервисов»[37]. На практике представления о частных российских или западных компаниях, действующих в этой сфере, зачастую формируются без желания разобраться в действительной обоснованности этих представлений.

[35] См. Max Seddon, 'Russian Telecoms Groups Mount Fight against Anti-Terror Law', Financial Times, 11 июля 2016 г.

[36] Thomas Fox-Brewster, 'Here's Kaspersky's Full Complaint Against The DHS Over Anti-Virus Ban', Forbes, 19 декабря 2017 г.

[37] National Cyber Security Centre, 'Letter to Permanent Secretaries Regarding the Issue of Supply Chain Risk in Cloud-Based Products', 1 December 2017.

Российский совет по международным делам

Российский совет по международным делам (РСМД) – это некоммерческая организация, ориентированная на выработку практических рекомендаций российским организациям, министерствам и ведомствам, задействованным во внешнеполитической деятельности.

РСМД объединяет усилия экспертного сообщества, органов государственной власти, бизнес-кругов и гражданского общества с целью повысить эффективность внешней политики России.

Наряду с аналитической работой, РСМД ведет активную образовательную деятельность с целью сформировать устойчивое сообщество молодых профессионалов в области внешней политики и дипломатии. Совет выступает в качестве активного участника публичной дипломатии, представляя на международных площадках российское видение в решении ключевых проблем глобального развития.

Члены РСМД – это ведущие представители внешнеполитического сообщества России: дипломаты, бизнесмены, ученые, общественные деятели и журналисты.

Президент РСМД Игорь Иванов, член-корреспондент Российской академии наук (РАН), занимал пост министра иностранных дел Российской Федерации в 1998–2004 гг., и пост секретаря Совета Безопасности Российской Федерации в 2004–2007 гг.

Генеральным директором Совета является Андрей Кортунов. В 1995–1997 гг. он занимал пост заместителя директора Института США и Канады РАН.

Королевский Объединенный институт оборонных исследований

Королевский Объединенный институт оборонных исследований (RUSI) – ведущий британский аналитический центр по вопросам обороны и безопасности, старейшая в мире «фабрика мысли».

В задачи Института входит информирование, оказание влияния и поддержка общественных дискуссий по вопросам формирования более безопасного и стабильного мира.

В основе деятельности организации лежит проведение собственных исследований, предоставление независимого, практико-ориентированного и продвинутого анализа современных комплексных вызовов и угроз.

С момента основания в 1831 г. RUSI опирается на потенциал своих членов, которые оказывают поддержку институту.

Несмотря на различные источники финансирования – доходы от исследовательской работы, публикаций и проведения конференций – Институт на протяжении 185 лет сохраняет свою политическую независимость.

Об авторах

Андрей Кортунов – генеральный директор Российского совета по международным делам (РСМД)

Малкольм Чалмерс – заместитель генерального директора Королевского объединенного института оборонных исследований *(RUSI)*

Сара Лэйн – научный сотрудник британского Королевского объединенного института оборонных исследований *(RUSI)*, в котором занимается анализом российской внешней политики. Ранее она работала в частном консалтинговом агентстве и занималась изучением рисков предпринимательской деятельности в России и странах постсоветского пространства.

Мария Смекалова – координатор проекта по кибербезопасности Российского совета по международным делам (РСМД).

Для заметок

Для заметок

Российский совет по международным делам
Королевский объединенный институт оборонных исследований

РОССИЙСКО-БРИТАНСКИЙ ДИАЛОГ ПО ПРОБЛЕМАМ БЕЗОПАСНОСТИ: ПЕРСПЕКТИВЫ ДВУСТОРОННЕГО СОТРУДНИЧЕСТВА. ЧАСТЬ 2

Доклад № 38/2018

Верстка — О.В. Устинкова

Источники фото на обложке:
справа наверху – REUTERS/Dado Ruvic/Pixstream
слева внизу – REUTERS/KCNA/Pixstream

Формат 70×100 $^{1}/_{16}$. Печать офсетная.
Усл. печ. л. 2,5. Тираж 150 экз.

РОССИЙСКИЙ СОВЕТ ПО МЕЖДУНАРОДНЫМ ДЕЛАМ (РСМД)
119180, Москва, ул. Большая Якиманка, дом 1
Тел.: +7 (495) 225 6283
Факс: +7 (495) 225 6284
E–mail: welcome@russiancouncil.ru
www.russiancouncil.ru