РСМД

Российский совет
по международным
делам

EastWest INSTITUTE

АНАЛИТИЧЕСКАЯ ЗАПИСКА

# Предложения по российско-американскому сотрудничеству в сфере кибербезопасности

**Брюс МакКоннелл**
*Вице-президент по глобальным вопросам Института Восток-Запад*

**Павел Шариков**
*руководитель Центра прикладных исследований Института США и Канады РАН*

**Мария Смекалова**
*координатор проекта по российско-американскому сотрудничеству в сфере кибербезопасности РСМД*

№ 11, сентябрь 2017

Некоммерческое партнерство «Российский совет по международным делам» (НП РСМД) является основанной на членстве российской некоммерческой организацией. Деятельность РСМД направлена на укрепление мира, дружбы и согласия между народами, предотвращение международных конфликтов и кризисное регулирование. Партнерство создано решением учредителей в соответствии с распоряжением Президента Российской Федерации от 02.02.2010 г. № 59-рп «О создании некоммерческого партнерства «Российский совет по международным делам».

**УЧРЕДИТЕЛИ**

Министерство иностранных дел Российской Федерации

Министерство образования и науки Российской Федерации

Российская академия наук

Российский союз промышленников и предпринимателей

Информационное агентство «Интерфакс»

**МИССИЯ РСМД**

Миссия РСМД заключается в содействии процветанию России через интеграцию в глобальный мир. РСМД — связующее звено между государством, экспертным сообществом, бизнесом и гражданским обществом в решении внешнеполитических задач.

*Мнения, выраженные в этой публикации, могут не совпадать с позицией РСМД.*

# Институт Восток-Запад



## Миссия

Институт Восток-Запад (ИВЗ) работает в области снижения международной конфликтности, участвуя в решении проблем, угрожающих мировой стабильности и международной безопасности. Он устанавливает связи и формирует отношения доверия между мировыми лидерами и влиятельными группами, создавая условия для выработки и внедрения новых практических шагов и опираясь на глобальную сеть контактов с лицами, принимающими решения. Эта независимая с момента создания в 1980 году некоммерческая организация имеет представительства в Нью-Йорке, Брюсселе, Москве, Далласе, Вашингтоне (округ Колумбия), Сан-Франциско и Стамбуле.

## История

Традиции работы Института Восток-Запад восходят к временам «холодной войны» – налаживанию связей между военными НАТО и Организации Варшавского договора. В качестве миротворческой организации он участвовал в событиях на Балканах, Ближнем Востоке и Восточной Азии. На современном этапе Институт продолжает играть определяющую роль как посредник, пользующийся доверием сторон, в наиболее трудноразрешимых глобальных конфликтах современности.

## Структура

Свою миссию Институт Восток-Запад осуществляет по трем направлениям: **Глобальная безопасность; Региональная безопасность** и **Выстраивание доверия между великими державами**. Реализуются программы «Глобальное сотрудничество в киберпространстве»; «Экономическая безопасность»; «Ближний Восток и Северная Африка»; «Афганистан»; «Россия и США»; «Турция, миротворчество и региональная стабильность»; «Азиатско-Тихоокеанское пространство».

## Глобальное сотрудничество в киберпространстве

Программа «Глобальное сотрудничество в киберпространстве» направлена на снижение конфликтности, преступности и других деструктивных явлений в киберпростанстве, а также на повышение стабильности, инновационной составляющей и включенности игроков. Работа с лидерами правительств, бизнеса и гражданского общества со всего мира строится вокруг **трех целей** для большей безопасности Интернета: **сдерживание** вредоносной активности в киберпространстве; повышение **безопасности** Интернет-продуктов и услуг; эффективная поддержка трансграничных **потоков** информации и технологий, гармонирующих со страновыми и локальными ценностями. Работой Программы руководит вице-президент ИВЗ по глобальным вопросам Брюс Макконнелл.

*ИВЗ МОСКВА*
*ул. Большая Дмитровка, д. 7/5, стр. 1, Москва, 125009 Россия*
*Тел. +7(495)234-7797, факс +7(495) 662-7162 www.eastwest.ngo*

# Предложения по российско-американскому сотрудничеству в сфере кибербезопасности

*Текущее состояние российско-американских отношений отличается высоким уровнем недоверия. Напряженность нарастала в течение трех лет, государства наложили друг на друга санкции, активно распространяют пропаганду и обмениваются взаимными обвинениями. Ситуация в двусторонних отношениях непредсказуема: если эскалация продолжится, вся система международных отношений может быть дестабилизована. Текущее ухудшение отношений между двумя странами затронуло все сферы взаимодействия, включая кибербезопасность.*

*Взаимодействие в сфере кибербезопасности – достаточно новый аспект, который никогда не входил в число приоритетных направлений наравне с борьбой с терроризмом, украинским и сирийским кризисами, экономическими санкциями и др.*

*Несмотря на то, что государства по обе стороны Атлантического океана осознают необходимость решения ключевых вопросов кибербезопасности, мнения сторон относительно необходимых мер и применения норм международного права к вопросам киберпространства расходятся.*

*В этой связи требуется работа по двум направлениям. Первое – сотрудничество в предотвращении киберпреступлений и принятие мер по борьбе с кибертерроризмом. Россия и США не могут найти общий язык при обсуждении предотвращения киберпреступлений. Отчасти это вызвано отсутствием общепринятой терминологии применительно к киберпространству. Кроме того, анонимность киберпреступлений не только затрудняет процесс атрибуции, но и зачастую подрывает статус-кво в двусторонних отношениях. Второе направление включает в себя разработку норм поведения, а также защиту объектов критической инфраструктуры от кибератак. Хотя группа правительственных экспертов ООН ведет активную работу над разработкой правил игры, государствам необходимо найти способы применения существующих и потенциальных норм на практике. Также необходимо дать четкие определения объектам критической инфраструктуры и киберпреступлений.*

*На данном этапе критически важно продолжение диалога и налаживание взаимопонимания при помощи экспертных встреч и публикаций, сотрудничества на техническом уровне и сбалансированного участия СМИ.*

На протяжении 2016 г. российские и американские эксперты по вопросам кибербезопасности совместно работали над предложениями по решению проблем в двусторонних отношениях, связанных с этой сферой.

В результате двусторонних усилий Российский совет по международным делам (РСМД) и Институт Восток-Запад (ИВЗ) выделили ряд вызовов и проблем в сфере кибербезопасности, а также предложений по их решению для улучшения российско-американского сотрудничества в киберпространстве. Стороны выражают надежду, что изложенные ниже предложения смогут лечь в основу будущего сотрудничества.

## Россия и США: о вражде и дружбе в киберпространстве

**Павел Шариков**, к. полит. н., руководитель Центра прикладных исследований Института США и Канады РАН

*До начала текущего кризиса в двусторонних отношениях России и США удавалось осуществлять совместную работу по укреплению доверия, несмотря на ряд расхождений по вопросу обеспечения безопасности в киберпространстве. Так, была установлена горячая линия Москва–Ва-шингтон, странам удалось найти общий язык по некоторым вопросам управления Интернетом и т.д.*

**АВТОРЫ:**

**Брюс МакКоннелл,** вице-президент по глобальным вопросам Института Восток-Запад
**Павел Шариков,** руководитель Центра прикладных исследований Института США и Канады РАН
**Мария Смекалова,** координатор проекта по российско-американскому сотрудничеству в сфере кибербезопасности РСМД

Большинство мер по укреплению доверия были согласованы в ходе саммита «Группы восьми» в Ирландии в 2013 г. К сожалению, все достижения были аннулированы в ходе текущего кризиса. Многие эксперты сегодня приходят к выводу, что Россия и США вступают в «холодную войну 2.0». В определенной степени такое определение справедливо, учитывая, что представители обеих стран прибегают к использованию риторики, схожей с той, что употреблялась во времена «старой холодной войны», при этом применяя современные технологии, в том числе широкий спектр кибертехнологий.

По мере усиления напряженности между Москвой и Вашингтоном эксперты по обе стороны Атлантического океана соглашаются, что дальнейшее ухудшение ситуации опасно.

***Возможно, величайшим разочарованием в этой ситуации является то, что расширенные возможности информационно-коммуникационных технологий не помогают государствам, а приводят к снижению уровня доверия и уверенности в системе международных отношений.***

## Новые условия

Вопросы, связанные с информационно-коммуникационными технологиями и киберпространством, привели к серьезным изменениям в глобальной системе международных отношений. Глобальное киберпространство – новый феномен, отличающий новую систему международных отношений от той, которая существовала в биполярном мире.

«Старая холодная война» сегодня кажется очень легко объяснимой и предсказуемой, в то время как новая холодная война серьезно от нее отличается.

Распад Советского Союза и неизбежный упадок биполярного мира привел к дестабилизации стратегического баланса сил времен холодной войны. Кроме того, появились новые факторы. Многие эксперты соглашаются, что в результате геополитических сдвигов, произошедших на фоне окончания холодной войны, концепция стратегической стабильности приобрела новое значение. Понятие «стратегические силы» теперь не ограничивается способностью доставить ядерное оружие с одного континента на другой, так как баланс сил больше не сводится к сдерживанию конфликта между двумя сверхдержавами. Технологический прогресс привел к появлению новых способов нанесения серьезного ущерба, создав таким образом новые угрозы для национальной и международной безопасности.

Холодная война была уникальным периодом в истории международных отношений. В первый и до настоящего времени единственный раз система международных отношений носила биполярный характер. Советский Союз и США были единственными сверхдержавами, находившимися в противостоянии на протяжении почти полувека. Тем или иным образом другие государства принимали участие в глобальном соперничестве между двумя огромными и несовместимыми экономическими системами – социализмом и капитализмом.

Распад Советского Союза ознаменовал триумф либеральных идей, биполярный мир остался позади, началось формирование новой системы международных отношений. Большинство экспертов в сфере международных отношений соглашаются, что текущая система МО носит полицентричный характер. США остаются наиболее могущественным государством в мире. В свою очередь, Россия, получив большую часть советского наследия, не смогла сравняться с США ни по одному аспекту, кроме ядерного потенциала.

Безопасность остается одним из ключевых вопросов в российско-американских отношениях после холодной войны, несмотря на то, что Москва и Вашингтон перестали быть единственными осями международной системы. Российско-американские отношения в сфере безопасности развиваются в соответствии с тектоническими сдвигами в миропорядке. Биполярный мир превращается в полицентричный. Информационная революция привнесла серьезные изменения как во внутреннюю политику государств, так и в международные отношения. Киберпространство – уникальный феномен, где внутренние и международные вопросы взаимозависимы настолько, что изучать первые без привязки к вторым практически невозможно. В новой системе международных отношений присутствуют новые типы акторов и новые же формы

их взаимодействия в рамках безграничного киберпространства. Все эти изменения представляют собой серьезный вызов для феномена суверенитета.

Некоторые негосударственные акторы не обладают военной мощью, однако при этом могут представлять серьезную угрозу другим акторам, включая государства. В такой ситуации государства не могут ответить нанесением ответного удара. Невоенные аспекты власти приобретают все большее значение в системе международных отношений. Так как развитие информационных технологий происходило в основном в частном секторе, зависимость от интернет-технологий делает традиционных акторов международных отношений более уязвимыми.

## Идеологическая конфронтация или информационное противоборство?

В основе «старой холодной войны» лежала идеология. Все внутри- и внешнеполитические решения как в СССР, так и в США принимались согласно коммунистической или либерально-демократической линии. СССР и США принадлежали к противостоящим идеологическим парадигмам, несовместимым по своему характеру. Именно поэтому в двусторонних отношениях присутствовало идеологическое противостояние.

***То, что сегодня нам кажется идеологической конфронтацией – лишь одна из форм информационного противостояния, которое включает распространение пропаганды при помощи традиционных СМИ и социальных сетей, Интернета, феномена fake news, альтернативных фактов, утечки информации и т.д.***

Россия сегодня не бросает вызов американскому (или западному в целом) мировому лидерству. Национальный интерес России состоит в том, чтобы оставаться равным партнером США в решении глобальных проблем. С распадом СССР осталось немного акторов, предпринимающих попытки бросить вызов сложившемуся миропорядку: к ним можно отнести террористические группировки или КНДР. Более того, несмотря на все текущие политические проблемы, российское общество сегодня идеологически движется к западным устоям, и оно ближе к ним, чем когда-либо.

Несмотря на то, что упомянутые выше проблемы напрямую не связаны с вопросом киберугроз, все они затрагивают взаимодействие в киберпространстве и обмен информацией. Так, российские власти признают, что технические аспекты безопасности неотделимы от информационного наполнения.

## Доктрины за основу

5 декабря 2016 г. президент России Владимир Путин подписал Доктрину информационной безопасности Российской Федерации. В соответствии с Доктриной, российские власти выступают в качестве ключевого игрока не только в обеспечении информационной безопасности страны, но и в развитии информационных ресурсов.

Следует отметить, что российские власти ценят и технологические, и гуманитарные аспекты информации. В то время как западные страны в основном сосредоточены на обеспечении технической безопасности, российские законодатели считают содержательную часть ключевой. Более того, Интернет позиционируется в качестве важнейшего элемента информационной инфраструктуры Российской Федерации. В целом новая Доктрина вписывается в общую стратегическую позицию российских властей.

***В основе новой Доктрины лежит тенденция к усилению контроля за российским интернет-пространством со стороны правительства и укреплению национального суверенитета в информационном поле.***

В новой Доктрине также указывается, что стратегическое сдерживание и предотвращение вооруженных конфликтов – одно из ключевых направлений информационной безопасности. Российская сторона ждет публикации нового документа по кибербезопасности в США. Несмотря на то, что некоторые догадки по вопросу уже имеются, необходимо дождаться публикации нового документа. Есть надежда на то, что в двух доктринах найдутся точки соприкосновения,

что позволит двум странам выстроить основу для сотрудничества.

Действительно, безопасность контента не менее важна, чем безопасность техническая. Ярчайшим примером тому служит самый обсуждаемый эпизод российско-американского противостояния в киберпространстве, в частности, кибератака на сайт Национального комитета Демократической партии США. Взлом электронной почты не принес Хилари Клинтон такого вреда, как публикация архива *Wikileaks* и освещение этих событий в прессе.

Несмотря на то, что доказательства причастности российских властей к кибератакам так и не появились в широком доступе, сложившаяся ситуация указывает на ряд ключевых проблем, требующих незамедлительного решения.

Во-первых, *необходимо обратить внимание на проблему атрибуции кибератак*. В случае если атака была совершена негосударственным актором, санкции против российских чиновников никак не скажутся на наказании виновных.

Во-вторых, *стала очевидной неспособность системы международных отношений решать проблемы киберпреступлений*. На данный момент не существует международного механизма, на платформе которого можно было бы проводить расследования, предотвращать и наказывать за кибератаки, подобные атаке на сервер Национального комитета Демократической партии США.

В-третьих, *существует проблема адекватного реагирования*. Ответ на кибератаку вынужден быть асимметричным и реализовываться в киберпространстве. Дальнейшая эскалация может привести к использованию инструментов, выходящих за рамки киберпространства, что может привести к серьезным потерям.

Если отставить в сторону все политические разногласия, лидеры России и США должны признать, что использование ИКТ-инструментов против друг друга дестабилизирует хрупкую ситуацию равновесия. Рано или поздно политические противоречия текущего кризиса останутся позади, поэтому необходимо уже сейчас работать над мерами создания и укрепления доверия в двусторонних отношениях.

## Необходимые меры: взгляд из России

В рамках российско-американского сотрудничества в кибербезопасности существует, по меньшей мере, четыре сферы, представляющие взаимный интерес, и в определенной степени жизненно важные для стабильности международных отношений. Решение этих четырех проблем в ближайшем будущем помогло бы частично преодолеть текущий кризис в двусторонних отношениях.

### *Первое направление – борьба с киберпреступностью*

Киберпреступность можно назвать наиболее серьезной угрозой. Действительно, едва ли можно считать угрозой национальной безопасности мелкие хакерские и *DDoS*-атаки, которые случаются каждый день. Тем не менее правительства должны принять срочные меры по уменьшению масштаба и количества подобных инцидентов. Россия и США должны сотрудничать как в формате совместных расследований этих преступлений, так и в форме передачи данных. Подобного рода сотрудничество должно осуществляться и в таких случаях, как атака на сайт Национального комитета Демократической партии США. Российские и американские правоохранительные органы должны выработать совместные механизмы расследования киберпреступлений, судебного преследования преступников, взаимопомощи при минимизации ущерба и обмена информацией о международных киберугрозах.

### *Второе направление – обмен информацией*

Негосударственные структуры, институты гражданского общества и публичной дипломатии могли бы осуществлять совместную работу и обмениваться информацией о террористической активности в Интернете со службами разведки. Как российские, так и американские граждане были неоднократно завербованы через интернет-площадки. Так как террористы используют Интернет в качестве инструмента пропаганды, борьба с деятельностью такого рода должна стать одним из направлений российско-американских антитеррористических мер, осуществляемых через механизмы публичной дипломатии. Логичным шагом в этом направлении может стать создание единой базы киберинцидентов.

***Третье направление – общая позиция по применению кибероружия***

Учитывая общую отрицательную динамику в двусторонних отношениях, российско-американское сотрудничество в сфере кибербезопасности должно служить положительным примером. Чтобы прийти к общему пониманию существующих проблем, правительствам обеих стран необходимо продолжать диалог, особенно на уровне научного сообщества. Россия и США должны опубликовать документ с общей позицией по кибервопросам, содержащий нормы применения наступательных кибервооружений. Кроме того, необходима гармонизация позиций по защите критической инфраструктуры (больницы, электросети, банки, ядерные объекты и т.д.), несмотря на то, что переговоры по этой тематике давались труднее всего.

***Наконец, необходимо работать над проблемой глобального управления Интернетом.***

Россия и США должны продолжить обсуждение правил глобального управления Интернетом, уделяя особое внимание вопросам безопасности. Любые последующие международные режимы кибербезопасности будут формироваться на основе национальных законодательств, разработанных в соответствии со спецификой политических, юридических, экономических и социальных традиций каждой страны. Безусловно, поиск полноценного баланса между государственным контролем в киберпространстве и свободой обмена информацией как на национальном, так и на международном уровне, будет одной из ключевых проблем эффективной информационной (кибер) политики государства.

В целом проблемы кибербезопасности должны быть включены в более широкий список вопросов на повестке двусторонних отношений. И Россия, и США обладают огромным опытом в сфере контроля вооружений, который частично может быть применен и к киберпространству.

## О необходимости сотрудничества

Брюс МакКоннелл, вице-президент по глобальным вопросам Института Восток-Запад

### Конвенциональные киберугрозы

Большая часть западных дискуссий на тему кибербезопасности сосредоточена вокруг вопросов предотвращения и восстановления после кибератак на сети и информацию, которая в них содержится. Серьезными источниками угрозы можно считать организованные преступные группы, действующие в интересах получения прибыли, соперничающие организации, крадущие запатентованную информацию, попытки шпионажа на государственном уровне, кражу интеллектуальной собственности, препятствование деятельности военных или других критически важных систем в качестве одного из способов проявления силы в ходе конфликта.

***Имея большие финансовые ресурсы, источники угрозы постоянно эволюционируют. Наглядным примером служат вирусные программы, которые самостоятельно устанавливаются на компьютеры и получают доступ к персональным данным.***

Десять лет назад владелец вируса связывался с жертвами, угрожая раскрыть их персональные финансовые данные в случае невыплаты требуемой суммы. Сегодня злоумышленники блокируют компьютер жертвы, угрожая держать данные «в заложниках» до выплаты запрошенной суммы. Наиболее распространенными жертвами становятся медицинские учреждения. Для борьбы с подобными и другими атаками предпринимается максимум усилий, нацеленных на понижение уровня уязвимости и продвижение передовых практик кибербезопасности.

***К сожалению, сейчас невозможно предотвратить проникновение хакера, нацеленного на совершение атаки. Если хранение ценной информации подразумевает использование Интернета, ее могут заполучить.***

Исполнитель атаки обнаружит уязвимое мало защищенное место, или же сотрудник компании откроет зараженный вложенный файл, или перейдет по незащищенной ссылке. Пребыва-

ющий в плохом расположении духа системный администратор может незаметно поставить всю систему под угрозу. Тем не менее компании могут понизить значимость уязвимых мест, грамотно применяя современные практики кибербезопасности. На данный момент существует целый ряд предлагаемых вариантов.

Все большее распространение в США получает Программа обеспечения кибербезопасности, подготовленная Национальным институтом стандартов и технологий Министерства торговли США. Программа предлагает основу политики кибербезопасности, которую можно было бы применить в каждой компании. В документе содержатся конкретные меры, которые необходимо принять компаниям для обеспечения базовой защиты: определение рисков, защита систем и информации, выявление атак и ошибок в работе, реакция на инциденты и восстановление после них. Программа дополняется целым рядом рекомендаций, включая документ «Покупка защищенных ИКТ-продуктов и сервисов: руководство покупателя», подготовленный Институтом Восток-Запад. В этом руководстве содержится 25 вопросов, которые покупатели могут задать продавцам ИКТ-продукции, чтобы оценить степень безопасности предлагаемых ими продуктов и сервисов.

## Терроризм и контент

В последние годы специалисты в области безопасности стали уделять больше внимания контенту – информации, передаваемой и хранящейся в киберпространстве, а также последствиям ее распространения, искажения и неправомочного использования для безопасности. Правоохранительные органы по всему миру уже на протяжении долгого времени борются с электронной информацией, содержащей детскую порнографию, и уже практически все страны и ключевые компании сотрудничают в работе по удалению контента подобного рода из Интернета, а также поиске и аресте его создателей. В том, что касается контента, имеющего политическую коннотацию, стороны не столь единогласны. Террористические организации используют Интернет для привлечения единомышленников, рекрутирования новых членов, инструктажа по атаке на целевых людей и организации, планирования операций и разжигания актов агрессии. Международные усилия по борьбе с террористами с использованием Интернета зачастую подрываются отсутствием общего понимания между государствами понятия террористической группировки, а также обеспокоенностью в западных государствах вопросом подавления свободы слова авторитарными режимами.

***Такие международные интернет-компании, как «Фейсбук» и «Твиттер», сталкиваются с все большим давлением относительно удаления контента, противоречащего законам той или иной юрисдикции.***

## Информационное противоборство

***Ключевая проблема в продвижении российско-американского сотрудничества в вопросах кибербезопасности – принципиальные расхождения относительно жертв атак и списка объектов, безопасность которых необходимо обеспечить.***

В центре внимания западных аналитиков стоит, как правило, безопасность сетей и систем, а также использование Интернета преступниками и террористами. Однако российское видение кибербезопасности включает защиту от использования информационного пространства для нанесения ударов по России. Так, например, действия госсекретаря США Хилари Клинтон по защите права на свободу слова и продвижению социальной сети «Твиттер» для высказывания своих политических настроений, были восприняты как попытка стимулирования «цветной революции» в России. Подобным же образом, раскрытие «панамских документов», указывающих на нелегальные финансовые операции, произведенные российскими чиновниками, и обвинения олимпийских атлетов в использовании допинга были восприняты как атаки на Россию со стороны Запада.

Вне зависимости от правомочности обвинений вопрос использования Интернета как инструмента нападения на страну или ее население при помощи негативной информации или попыток дестабилизации режима все чаще обсуждается в диалоге по кибербезопасности. Военная доктрина России признает важность использования такой так-

тики[1]. Подобные техники также используются вооруженными силами западных стран и носят название «операций влияния»[2].

Это измерение отсутствия безопасности в киберпространстве стало особенно очевидно после кибератак, целью которых было влияние на исход выборов в США и Европе, ответственность за которые была возложена на российских хакеров.

## Нормы поведения в киберпространстве

***В неконтролируемую гонку кибервооружений вовлечены все — и независимые маргинальные киберпреступники, и организованные группы, поддерживаемые государствами — лидерами в области кибербезопасности: США, Россией, Китаем и Израилем. Более того, по оценкам, более 30 государств «второго эшелона» обладают наступательным кибероружием.***

У кибероружия есть определенные преимущества – оно не требует крупных затрат, как правило, несмертельно и незаметно. Однако при продолжении неконтролируемых межгосударственных стычек в киберпространстве будет подорвана международная стабильность и безопасность. Как я говорил в своем выступлении в Комитете Министерства внутренней безопасности США в марте 2017 г., растет риск ошибки и эскалации, которая может нанести непосредственный вред жителям развитых стран. В случае если сфабрикованные новости, политический троллинг и боты в социальных сетях продолжат снижать степень доверия к киберпространству, оно станет бесполезным в качестве способа торговли и управления. Опасаясь стать жертвами, потребители уже начинают избегать электронную торговлю.

После десяти лет совместной работы группа правительственных экспертов по кибербезопасности ООН выпустила первоначальный список не имеющих юридической силы норм поведения в киберпространстве.

Среди них:

- не допускать использование информационно-коммуникационных технологий (ИКТ) для намеренного нанесения ущерба критической инфрастуктуре другого государства;
- не допускать осуществление международных кибератак со своей территории;
- отвечать на запросы о помощи от страны, которая подверглась кибератаке, исходящей с территории этого государства;
- предотвращать распространение вредоносных инструментов и технологий, а также использование скрытых вредосносных функций;
- поощрять ответственное информирование об уязвимостях ИКТ и распространение связанной с ними информации;
- не наносить вред информационным системам авторизованных служб реагирования на киберинциденты.

Глобальные ИКТ-компании, в свою очередь, начинают проявлять бóльшую ответственность, сопряженную с их серьезной ролью в киберпространстве. Так, недавно компания «Майкрософт» выпустила нормы поведения, которым следует следовать глобальным ИКТ-компаниям.

Примеры подобного рода норм для компаний включают:

- создание более безопасных продуктов и сервисов;
- недопущение ослабления безопасности коммерческих ИКТ-продуктов и сервисов массового потребления государством;
- ответственное информирование об уязвимостях;

[1] В задачи Вооруженных сил России входит «развитие сил и средств информационного противоборства» путем «воздействия на противника на всю глубину его территории одновременно в глобальном информационном пространстве, в воздушно-космическом пространстве, на суше и море… для создания условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности», включая «борьбу с использованием финансируемых и управляемых извне политических сил, общественных движений». Военная доктрина Российской Федерации (в редакции 2015 г.) URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/976907, проанализирована в Roche, Edward M., Russian Cyber War Doctrine. URL: https://cyberarmscontrolblog.com/2017/01/20/russian-cyber-war-doctrine.

[2] Операции по усилению влияния сосредоточены на изменении восприятия и поведения лидеров государств, групп людей или жителей целых стран. В операциях влияния используются методы по изменению поведения, защите операций, передаче намерений командующего и проецированию точной информации для достижения желаемого эффекта у когнитивного домена. Эти эффекты, как правило, приводят к изменению в поведении или цикле принятия решений соперника, что соответствует целям командующего. Операции по усилению влияния включают психологические операции (*PSYOP*), оперативную маскировку (*MILDEC*), меры обеспечения секретности действий (*OPSEC*), операции по контрразведке (CI), контрпропаганде и связям с общественностью (*PA*). Военно-воздушная доктрина США, цитаты. URL: http://www.au.af.mil/info-ops/influence.htm.

- сотрудничество по защите покупателей от серьезных кибератак и восстановлению после них;
- выпуск обновлений для защиты покупателей вне зависимости от их местоположения.

Чтобы предотвратить крупные случайные или намеренные нарушения глобальной экономической и политической стабильности, прогресс по данному направлению должен быть ускорен.

Глобальная комиссия по стабильности киберпространства будет публиковать и отстаивать необходимость применения детальных рекомендаций для поведения как государств, так штаб-квартир корпораций и широкой публики по всему миру. Ожидается, что первые результаты, включая предложение о том, что ключевая инфраструктура Интернета, от которой мы все зависим, должна быть закрыта от атак, будут опубликованы осенью 2017 г. ИВЗ запустил новую глобальную инициативу по разработке дорожной карты поведения государств в киберпространстве. В работе принимают участие министр иностранных дел Голландии, бывший министр иностранных дел Эстонии, бывший заместитель советника по национальной безопасности Индии, бывший министр внутренней безопасности США и представители корпоративного сектора. Глобальная комиссия по стабильности киберпространства – трехгодичный проект по созданию, оценке и разработке рекомендаций норм поведения для государств и негосударственных игроков а также выдвижению предложений по обсуждениям в более широком формате. Комиссия опубликует список детальных рекомендаций и распространит его по столицам государств, штаб-квартирам организаций и среди широких масс. Первые результаты ее работы, включая предложение по неприкосновенности ключевой инфраструктуре Интернета, должны быть опубликованы осенью 2017 г.

## Техническое сотрудничество

***Несмотря на важность дипломатических и политических усилий, необходимо сотрудничество и на техническом уровне.***

В этой аналитической записке уже указывалось, что России и США необходимо регулярно испытывать систему немедленного взаимного предупреждения о потенциально опасных действиях в киберпространстве. Регулярные испытания «горячей линии» по вопросам кибербезопасности, созданной в 2013 г., снизят вероятность просчетов и острой реакции на события.

*Еще один подход включает сотрудничество по обеспечению безопасности между представителями частного сектора.* Не так давно несколько компаний, занимающихся вопросами кибербезопасности, основали «Альянс киберугроз» – формат взаимодействия работающих в сфере специалистов, нацеленный на бескорыстный обмен информацией об угрозах и повышение степени защиты от профессиональных киберпреступников.

Компании-участницы альянса[3] совместно разрабатывают как закрытые, так и общедоступные руководства по улучшению кибербезопасности на глобальном уровне. Расширение состава Альянса с привлечением большего числа компаний, зарегистрированных за пределами США, могло бы стать полезным шагом для улучшения международного технического сотрудничества в сфере кибербезопасности.

## Распространение кризиса

На все эти действия понадобится время. Несмотря на определенный прогресс, для снижения риска непреднамеренных последствий необходимы конкретные действия. Ключ к успеху – качественный диалог проверенных собеседников. Должны стимулироваться и поддерживаться неформальные инициативы, в том числе продвигаемые Институтом Восток-Запад и Российским советом по международным делам. Мир слишком сильно зависит от безопасного киберпространства, чтобы лишиться его преимуществ из-за просчета или дезинформации. Будучи ключевыми игроками, Россия и США должны со всей серьезностью подойти к своим обязанностям в этой сфере.

[3] Среди участников: *Check Point, Cisco, Fortinet, Intel Security, Palo Alto Networks, Symantec*; а также *Eleven Paths, IntSights, Rapid7, ReversingLabs* и *RSA*.

## ВЫВОДЫ И РЕКОМЕНДАЦИИ

### Вызовы в сфере предотвращения киберпреступлений и антитеррористических мер:

- Широкие массы не обладают достаточными знаниями о киберпространстве и кибертехнологиях.
- Перед странами стоит острая необходимость выработки единой терминологии применительно к киберпреступлениям и кибертерроризму. Несмотря на то, что ни Россия, ни США не заинтересованы в нанесении вреда друг другу, восприятие сторонами понятия «киберпреступление» отличается.
- Наиболее распространенные киберпреступления включают кражу аккаунтов, мошенничество, *DDoS*-атаки и кража интеллектуальной собственности. Наибольшие потери от киберпреступлений несет бизнес-сообщество, при этом правоохранительные органы на данном этапе не могут полноценно участвовать в решении проблем кибербезопасности, с которыми сталкиваются компании.
- Бизнес-круги гораздо больше заинтересованы в скором восстановлении от последствий кибератак, нежели чем в их расследовании. Чем большее время занимает процесс восстановления от кибератаки, тем большие издержки терпит бизнес.
- Контакты между бизнес-сообществом и государственными структурами недостаточно хорошо налажены. Ввиду того, что большинство ИКТ-компаний работают в международном формате, они страдают от недостатка контактов не только в стране размещения, но и на международном уровне. В случае кибератаки компаниям необходимо связаться с партнерами за рубежом, что подразумевает целый ряд юридических трудностей.
- Анонимный характер киберпреступлений. Расследования иногда позволяют отследить *IP*-адрес объекта, но дальнейшее раскрытие затруднено. Из 10 000 преступлений, совершенных в киберпространстве, лишь одно удается успешно расследовать.
- Международный характер киберпреступлений. Так как большинство атак производится с территории других государств, властям не удается провести полноценное расследование преступления ввиду невозможности отслеживания преступников, находящихся в других странах.
- России и США пока не удалось разработать совместную стратегию поведения в киберпространстве. В случае атаки государства переходят к взаимным обвинениям, которые впоследствии ведут к дальнейшему ухудшению в двусторонних отношениях.
- Россия и США сталкиваются с общими угрозами в сфере кибербезопасности, исходящими от третьих сторон. При этом попытки совместного расследования киберпреступлений отсутствуют.
- На данном этапе отсутствует единая база данных совершенных киберпреступлений. У России и США нет согласованного списка видов киберпреступлений, по которым осуществлялась бы взаимопомощь.

### Предлагаемые меры:

1) Необходимо организовать глобальный киберфорум с участием представителей всех заинтересованных стран. Участники форума должны прийти к компромиссу относительно терминов, связанных с киберпространством, и их наполнения, а также выработать нормы поведения в киберпространстве. Необходимо создание нового мультистейкхолдерного института.

2) Органам государственной власти необходимо наладить канал связи с бизнес-сообществом для выработки формата взаимодействия в киберпространстве. Сторонам

необходимо прийти к консенсусу относительно продуктов двойного назначения, их производства и использования.

3) Для обеспечения эффективной борьбы с кибератаками и кибертерроризмом необходимо введение нового механизма работы правоохранительных органов.

4) Критически важно разработать стратегию борьбы с киберпреступлениями и обеспечить международное сотрудничество в отслеживании хакеров. Необходимо обеспечить оперативный и эффективный канал обмена информацией как на двустороннем, так и на многостороннем уровне.

5) Со своей стороны Россия и США должны разработать двустороннее соглашение, определяющее их общую позицию по вопросу и предотвращающее инциденты в двусторонних отношениях, вызванные ситуациями в киберпространстве.

6) России и США необходимо проводить регулярные тестирования системы немедленного взаимного предупреждения о потенциально опасной активности.

7) ИКТ-компаниям и руководству стран необходимо вести совместную работу по снижению риска атак со стороны государств. Государства должны бороться с распространением кибероружия (уже созданные формы должны носить ограниченный и точный характер), в то время как ИКТ-компании не должны использовать Интернет в преступных целях или распространять технологии, усиливающие уязвимость перед кибератаками.

**Вызовы в сфере норм поведения в киберпространстве и защиты критической инфраструктуры:**

1) Применимость норм международного права к сфере кибербезопасности по-прежнему оспаривается.

2) На данном этапе разрабатываются нормы поведения в киберпространстве для бизнес-структур. Группа правительственных экспертов ООН разработала предложения для государств. Вопрос их применимости и эффективности по-прежнему открыт.

3) У России и США отсутствует единое понятие критической инфраструктуры.

4) Существующая законодательная база не позволяет адекватно реагировать на новые вызовы, в том числе в сфере кибербезопасности. В таких условиях невозможно достичь ощутимых результатов.

5) У некоторых государств отсутствует традиция оказания взаимной юридической помощи в случае возникновения киберинцидентов.

6) В случае возникновения кибератаки, произведенной с территории другого государства, пострадавшей стороне приходится действовать через законодательство другой. Зачастую законодательные базы государств существенно различаются: это касается взаимодействия полиции и правоохранительных и законодательных органов, а также бизнес-сообщества.

7) Во многих случаях требуется перевод законов на иностранный язык, что создает дополнительные трудности для расследования преступлений.

8) Юристы не обладают достаточными знаниями в сфере интернет-технологий, что еще более затрудняет процесс выработки адекватных норм поведения в интернет-пространстве.

**Предлагаемые меры:**

1) Необходим положительный настрой: сотрудничество в кибербезопасности сосредоточено вокруг поиска компромиссов, а не конфликтов. Нужно работать над решением вопросов доверия, осуществить переход от передачи информации *(«information sharing»)* к «взаимообмену информацией» *(«information exchange»)*.

2) Российские и американские эксперты сходятся в том, что государства не должны осуществлять кибератаки по объектам критической инфраструктуры друг друга, при этом понятие по-прежнему остается размытым. Необходимо проведение анализа совпадений и расхождений в списках объектов критической инфраструктуры России и США. Такой шаг мог бы способствовать лучшему пониманию концепции.

3) Потенциальные нормы должны быть деполитизированы. Их введение должно быть осуществлено только когда оба государства изъявят четкое стремление к сотрудничеству по вопросу. После введения общих норм оба государства окажутся в выигрышном положении, и их бизнес-сообщества в том числе.

4) Одобрение документов по нормам поведения в киберпространстве со стороны ООН могло бы придать государствам необходимый стимул к действию. В конечном итоге некоторые нормы могли бы не только носить рекомендательный характер, а стать обязательными.

5) России и США необходимо продолжать контакты на уровне экспертного, дипломатического и бизнес-сообществ для достижения компромисса.

**ДЛЯ ЗАМЕТОК**


facebook.com/
russiancouncil


twitter.com/
Russian_Council


vk.com/
russian_council


russiancouncil.
livejournal.com


flickr.com/photos/
russiancouncil


youtube.com/
russiancouncilvideo


slideshare.net/
RussianCouncil


linkedin.com/company/russian-international-affairs-council/
linkedin.com/groups/Russian-International-Affairs-Council-4473529

Тел.: +7 (495) 225 6283
Факс: +7 (495) 225 6284
E-mail: welcome@russiancouncil.ru
119180, Москва, ул. Большая Якиманка, дом 1.

**www.russiancouncil.ru**