Confidential

RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International and of the Centre russe d'études politiques.

This issue is for your personal use only.

Published monthly in Russian and in English by *Trialogue Company Ltd.*

Issue № 5 (255), vol.17. 2018

15 ноября 2018 г.

Олег Демидов и Маргарита Ангмар сообщают из Москвы:

НОВАЯ КИБЕРСТРАТЕГИЯ США: ПЕРСПЕКТИВЫ ДЛЯ РОССИЙСКО-АМЕРИКАНСКИХ ОТНОШЕНИЙ ПО ВОПРОСАМ КИБЕРПРОСТРАНСТВА

АННОТАЦИЯ

В сентябре 2018 г., после нескольких месяцев давления со стороны Конгресса Белый дом обнародовал новую стратегию для киберпространства США. СМИ восприняли документ как поворот новой администрации в сторону более агрессивной наступательной политики в сфере кибербезопасности.

Ряд положений стратегии действительно свидетельствует о намерениях США ужесточить противодействие своим соперникам в киберпространстве с использованием превентивных наступательных мер. Какие еще выводы можно сделать из нового документа и как эти планы отразятся на российско-американских отношениях в сфере кибербезопасности анализирует консультант ПИР-Центра Олег Демидов при участии Маргариты Ангмар.

Ключевые положения новой киберстратегии: а был ли Трамп?

«Национальная стратегия для киберпространства» предполагает активизацию усилий федерального правительства с вовлечением частного сектора и других заинтересованных сторон на четырех основных направлениях («столпах»):

1. Защита американского народа, отечества и американского образа жизни (повышение киберзащищенности информационных сетей федеральных ведомств, обеспечение кибербезопасности критической инфраструктуры, борьба с компьютерной преступностью и реагирование на компьютерные инциденты и т.д.);
2. Укрепление американского процветания (развитие безопасной цифровой экономики, поддержка американского изобретательства и открытий в сфере ИТ и т.д.);
3. Поддержание мира при помощи силы (укрепление стабильности в киберпространстве, атрибуция и сдерживание «неприемлемого поведения» в киберпространстве);
4. Усиление американского влияния в киберпространстве (поддержка открытого, надежного и безопасного Интернета, международное наращивание потенциала и ресурсов в области обеспечения кибербезопасности).

Вопреки тому, что Трамп в своих выступлениях полностью игнорирует принятые при президенте Обаме стратегии в этой области, в большинстве разделов новой стратегии влияние нынешней президентской администрации и лично Трампа просматриваются достаточно слабо. Новая стратегия не *формирует* согласованный вектор деятельности для участников системы государственного управления США, а, скорее *собирает* его по описательному принципу, сводя воедино уже подготовленные в период президентства Обамы концепции и рабочую повестку отдельных федеральных ведомств.

Так, почти весь первый «столп» стратегии Белого дома и, частично, второй, в обобщенном виде воспроизводят положения отдельной ведомственной «Стратегии кибербезопасности» Министерства внутренней безопасности (Department of Homeland Security, DHS), опубликованной 15 мая 2018 г. – деполитизированной и основанной на реализации и развитии ряда долгосрочных инициатив, многие из которых были запущены при предыдущем хозяине Белого дома.

В разделе стратегии о продвижении и поддержке свободного Интернета стратегия дословно повторяет текст и посыл стратегических документов и заявлений американского руководства при Обаме. Парадоксальным выглядит пункт о приверженности модели управления Интернета с участием всех заинтересованных сторон (т.н. мультистейкхолдерная модель), учитывая, что в заявлениях предвыборного штаба Трампа отмечалось, что он «не позволит Обаме передать контроль над Интернетом в руки иностранных держав» (имелась в виду передача координирующей роли в исполнении функций Администрации адресного пространства Интернет, IANA, от правительства США глобальному сообществу заинтересованных сторон).

Стабильность в киберпространстве и кибероборона: полет ястреба

Сказанное выше, однако, не означает, что новая стратегия не несет изменений в политическом курсе новой администрации в киберпространстве. Практически все внимание медиа и экспертного сообщества в связи с публикацией документа оказалось сосредоточено на его третьем «столпе» – стратегии правительства США в сфере

Confidential

укрепления стабильности в киберпространстве и защите Америки от внешних киберугроз.

При этом одним из главных новостных поводов стал не сам текст стратегии, а заявление Советника по национальной безопасности США Джона Болтона, который, анонсируя стратегию 20 сентября 2018 г., подчеркнул: «*Мы не будем задействовать только оборонные меры, мы намерены участвовать в наступательных операциях, и наши соперники должны иметь это в виду*».

В качестве одного из значимых шагов администрации Трампа, который, по словам Болтона, **«развязывает руки» США в части проактивных действий в киберпространстве**, была отмена директивы президента США «О политике США в области кибероперaций» (Presidential Policy Directive 20, PPD 20), принятого в октябре 2012 г. со статусом «Высший уровень секретности» и рассекреченного в июне 2013 г. Эдвардом Сноуденом. Эта директива закрепила механизм контроля над принятием решений о проведении наступательных кибероперaций (решение об их проведении должно было утверждаться отдельно президентом США), а также над реагированием на вредоносную активность в киберпространстве (согласуется через механизмы межведомственной координации).

Теперь, если верить Болтону, все процедуры согласования решений о проведении кибероперaций, отменяются в соответствии с требованиями времени. Потенциальные адресаты этого сообщения были четко обозначены и в самой стратегии, и в заявлении Болтона, и пресс-релизах Белого дома – это Россия, Северная Корея, Иран и Китай.[1]

Но есть ли какая-то опора под заявлениями о «ястребиной линии» и наступательном уклоне новой стратегии администрации Трампа, помимо заявлений Трампа и Болтона? Довольно резкий пересмотр приоритетов в сторону наступательных, превентивных силовых действий в киберпространстве и правда зафиксирован в американских стратегических документах – но, в первую очередь, не в документе Белого дома.

Незадолго до публикации киберстратегии Трампа, 18 сентября 2018 г., краткую выжимку из своей новой «Стратегии для киберпространства» опубликовало **Минобороны США** – и в ней приоритеты расставлены недвусмысленно:

- В Стратегии утверждается, что **США вовлечены в «стратегическое состязание» с Китаем и Россией**, и действия этих двух государств в киберпространстве представляют долгосрочный стратегический риск для американской нации и ее союзников.
- Минобороны планирует проводить кибероперации с целью сбора разведданных и наращивания военного потенциала на случай полномасштабного кризиса.
- Минобороны планирует осуществлять операции в рамках **проактивной кибероборонны** для пресечения, предупреждения и противодействия враждебной активности в киберпространстве, даже если такая активность не достигает порога применения силы по смыслу международного права.
- Также предусматривается, что «в обстановке военного времени» объединенные войска США **задействуют «наступательный киберпотенциал»** и **«инновационные решения»** для проведения кибероперaций на всех театрах военного конфликта.
- Основная цель Минобороны США в киберпространстве, согласно новой стратегии – «обеспечить проактивную оборону, отладить работу в формате каждодневного

[1] Цитата из Стратегии: «*Россия, Иран и Северная Корея проводили безрассудные кибератаки, которые нанесли ущерб американскому и международному бизнесу, нашим союзникам и партнерам. При этом они не заплатили цену, которая бы, вероятно, предотвратила кибератрессию в будущем. Китай был задействован в экономическом шпионаже в киберпространстве и краже интеллектуальной собственности на триллионы долларов*».

Confidential

состязания [со стратегическими соперниками], а также обеспечить готовность к войне», в т.ч. за счет создания более «смертоносных» вооруженных сил в части деятельности в киберпространстве.

Кроме того, как стратегия Минобороны, так и, в большей степени, документ Белого дома обращаются к **вызову враждебных информационных операций** – интернет-пропаганды, кампаний по дезинформации и манипуляции общественным мнением граждан США через киберпространство, прежде всего со стороны России. Бороться с этой угрозой предлагается сочетанием силовых методов, санкций и иных рычагов воздействия на источник «недружественной информационной активности».

С учетом такого стратегического видения Минобороны положения стратегии Белого дома в части ужесточения противодействия соперникам США в киберпространстве, создания для них гарантированных последствий и эффективного сдерживания «недопустимого поведения» в киберпространстве приобретают более конкретное звучание.

Приверженность нормам и альянсам

Одна из принципиально новых задач США, заявленных в киберстратегии, – запустить международную **Инициативу по киберсдерживанию** (Cyber Deterrence Initiative). Цель инициативы – сформировать коалицию совместно с государствами, разделяющими общие ценности и подходы США в отношении кибербезопасности для того, чтобы эффективнее и жестче реагировать на враждебные действия и «недопустимое поведение» третьих сторон в киберпространстве.

Исходя из предлагаемого формата коалиции, речь идет о формировании блока, обеспечивающего совместное реагирование на угрозы кибербезопасности и коллективные действия против недружественных акторов в киберпространстве. Отличие от деятельности НАТО в рамках политики кибероборонь альянса тут разве что в том, что арсенал такой коалиции все же больше ориентирован на политико-дипломатические механизмы, а не на объединение военного потенциала и силовое реагирование. Однако это не значит, что такая коалиция будет «беззубой» и неопасной для потенциальных государств-«нарушителей»: помимо сотрудничества в обмене разведданными, речь может идти о коллективных санкционных механизмах, а также – теоретически – и о легитимизации силового ответа при помощи подтверждения третьими сторонами-участниками коалиции выводов по атрибуции кибератак.

Перспективы российско-американских отношения по вопросам киберпространства: ничего хорошего

Во-первых, сохранение и даже усиление курса США на продвижение добровольных норм ответственного поведения в киберпространстве делает актуальным вопрос о дальнейшей судьбе **Группы правительственных экспертов ООН** (UN GGE) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности – основной площадке для многосторонней разработки и согласования проектов таких норм, созданной по инициативе России более десятилетия назад. Работа 5-й созыва Группы завершилась в июне 2017 г. завершилась болезненным провалом – участники Группы впервые с 2005 г. не смогли прийти к консенсусу и приняли лишь протокольный доклад о своей работе.

Confidential

По итогам заседаний Группы, 26 июня 2017 г. Советник президента США по внутренней безопасности Томас Боссерт[2] заявил, что «формат Группы выработал лимит своих возможностей» и «настало время рассмотреть другие варианты». В том же выступлении г-н Боссерт подчеркнул: «*Не отказываясь от работы в многосторонних форматах, США будут активнее действовать на международной арене в рамках двусторонних форматов, таких как сотрудничество с Великобританией и Израилем, а также продолжат формировать коалицию партнеров, способных действовать сообща*».

С учетом того, что Трамп достаточно методично и даже агрессивно проводит ревизию всех моделей многостороннего взаимодействия – подгоняя ее под текущую трактовку национальных интересов США – либо вообще санкционируя выход из многостороннего механизма, закономерно было ожидать, что такой же итог может постичь и UN GGE.

Наиболее вероятными представлялись две стратегии действий в отношении участия США в UN GGE:

1. Выход США (и их ближайших союзников) из Группы и концентрация усилий на Инициативе по киберсдерживанию.
2. Попытка перезапуска Группы в новом формате и режиме деятельности – например, в качестве постоянной рабочей площадки при ООН с секретариатом и функциями оперативных рабочих встреч и выработки решений по реагированию на трансграничные киберинциденты и киберугрозы.

Первый вариант в значительной мере делегитимизировал и снижал ценность формата Группы для всех остальных ее участников, особенно если решению США о выходе последуют и их ключевые союзники по НАТО и партнеры по G7. Второй вариант мог натолкнуться на сопротивление у России и ряда других ключевых членов Группы – особенно если состав гипотетической новой структуры предполагалось сформировать без их участия.

И хотя сама инициатива по созданию UN GGE была попыткой преодолеть изначальный и все углубляющийся раскол в ценностях и подходах разных групп государств к регулированию киберпространства, в настоящий момент администрация Трампа может – осознанно или нет – сыграть роль катализатора перемен, а то и детонатора для нынешней архитектуры международного диалога и сотрудничества по вопросам стабильности и безопасности в киберпространстве. Для российско-американских отношений вероятным итогом может стать утрата единственной на сегодня универсальной и действующей в рамках ООН площадки многостороннего диалога по кибервопросам.

Последнее развитие событий идет именно по этому сценарию, хотя и неожиданным образом. США пошли неожиданным третьим путем, парадоксальным образом поменявшись с Россией местами в части позиции относительно UN GGE. 9 ноября РФ и США представили в Первый комитет Генассамблеи ООН два конкурирующих проекта резолюций, оба из которых были приняты членами Комитета. В центре обеих резолюций – будущее многостороннего диалога о нормах ответственного поведения государств в киберпространстве и, конкретно, дальнейшая судьба площадки UN GGE:

- Разработанный РФ проект резолюции (A/C.1/73/L.27*) призывает к комплексному перезапуску Группы в 2019 г. с изменением формата ее работы в сторону включения более широкого круга участников. Во-первых, из текста резолюции вытекает необходимость расширения состава государств-участников Группы и более справедливого географического и регионального представительства в ней (в последних созывах Группы участвовали представители 25 государств, которые

[2] Томас Боссерт покинул пост Советника Президента США по внутренней безопасности в апреле 2018 г.

Confidential

в совокупности как бы представляли все международное сообщество). Во-вторых, предлагается сделать Группу открытой для участия других заинтересованных сторон – частного бизнеса, экспертов и технических организаций.

- США (а также их партнеры по НАТО и альянсу «Пяти глаз») отказались поддержать Россию – Вашингтон внес свой проект резолюции (A/C.1/73/L.37), в котором де-факто предлагается возобновить работы Группы в более-менее прежнем формате с рядом точечных нововведений.

Парадоксальным образом, позиция США по отношению к UN GGE развернулась на 180 градусов по отношению к прошлому десятилетию – с 2004 по 2009 гг. главным лоббистом Группы была Россия, по инициативе которой UN GGE и была создана – США же в первые годы относились к новому механизму прохладно и саботировали работу над первым докладом Группы в 2005 г. Теперь же сам Вашингтон выступает за возобновление работы Группы и в тексте резолюции отмечает важность ее наработок в 2013-2015 гг., когда ее участниками были согласованы первые своды предлагаемых добровольных норм ответственного поведения в области использования ИКТ, а также базовые положения о применимости основополагающих принципов международного права к деятельности в киберпространстве. Россия же, напротив, настаивает на том, что ее детище в нынешнем формате неэффективно и нуждается в радикальной трансформации.

Впрочем, итог у этих дипломатических игр один: раскол ранее единой площадки многосторонней работы по регулированию киберпространства, и отчетливый дрейф двух идейных «ядер» международного сообщества в расходящихся направлениях. Предметное представление о составе этих «ядер» дают перечни соавторов двух резолюций:

- «Ядро», возглавляемое США: государства НАТО, Австралия и Украина.
- «Ядро», возглавляемое Россией: Китай и другие государства ШОС, некоторые участники СНГ, КНДР, государства Латинской Америки с «левыми» режимами (Боливия, Венесуэла, Куба, Никарагуа), Сирия и разномастный ряд африканских стран.

Естественно, корень противоречий этих условных групп лежит не в формате или принципах работы многосторонней площадки, а в принципиально разных идейных и доктринальных взглядах на вопросы применения международного права в области использования ИКТ, пределах действия государственного суверенитета в Сети, полномочиях государств в области контроля контента – да и просто в глубоком взаимном недоверии, а то и конфронтации на международной арене.

Более того, обсуждение проектов резолюций США и России практически совпало (с разницей в 3 дня) с третьей независимой инициативой, исходящей от Франции. 12 ноября 2018 г. президент Макрон на всемирном Форуме по управлению Интернетом (IGF) анонсировал «Парижский призыв к обеспечению доверия и безопасности в киберпространстве». В опубликованном тексте декларации не упоминается UN GGE, однако предлагаемые девять направлений действий по большей части перекликаются с наработками Группы образца 2013 и 2015 гг. Разве что более четкий акцент сделан на роль частного сектора (ИТ-корпораций) и технического сообщества.

Практического смысла сопоставлять 9 предлагаемых направлений действий Парижского призыва со списком проектов добровольных норм UN GGE немного: смысл инициативы не в том, чтобы предложить нечто качественно новое с содержательной точки зрения, а в том, чтобы усилить роль Франции как медиатора и двигателя процесса согласования общих норм для киберпространства, пользуясь расколом UN GGE и крахом диалога между США и Россией. Макрон пытается вернуть Франции роль великой дипломатической державы в новой критически важной сфере международных отношений – возрождая

Confidential

историческую роль Парижа как взвешенного и авторитетного медиатора полярных позиций Москвы (а теперь и Пекина) с Вашингтоном.

Однако наиболее вероятный сценарий на ближайшее будущее – не дипломатический триумф Елисейского дворца, а глобальные «лебедь, рак и щука» в повестке выработки норм ответственного поведения государств в области использования ИКТ. Показательная ситуация с одновременным продвижением трех инициатив, которые в общем-то посвящены одним и тем же вопросам, но подчеркнуто позиционируются как альтернативы друг другу, говорит о том, что подлинно глобальный обмен мнениями о нормах, правилах поведения и регулировании киберпространства схлопывается, распадается.

Фрагментация киберпространства, которой так долго пугали мир правительства и РФ, и США, и других стран, теперь распространяется и на уровень международного дипломатического дискурса, глобального диалога о том, как это пространство – или сферу отношений – регулировать. Как учит басня Крылова, воз в этой ситуации никуда не движется.

Во-вторых, перспективы трека по выработке мер доверия в сфере использования ИКТ на площадке **ОБСЕ** выглядят несколько оптимистичнее – разрушать этот механизм особых причин нет, да и сами меры доверия в текущей ситуации остаются более ценным и практичным инструментом, чем добровольные нормы, которые все равно никто не соблюдает. Правда, в части российско-американского взаимодействия о взаимной реализации на практике механизмов доверия (например, взаимодействия национальных CSIRT/CERT) РФ и США в рамках ОБСЕ говорить не приходится. Стороны по-прежнему находятся в ситуации порочного круга, когда для реализации мер доверия необходим стартовый минимальный капитал доверия, которого нет.

В-третьих, остается **двусторонний формат** взаимодействия, где ничего конструктивного не происходит с 2014 г., когда были заморожены российско-американские соглашения о мерах доверия в области кибербезопасности, подписанные Путиным и Обамой всего годом ранее, в июне 2013 г. Пытаться восстановить механизм 2013 г. сейчас – бесперспективный проект для Трампа, прежде всего потому, что оба партийных крыла американского Конгресса оказывают на Белый дом серьезное давление и заставляют Трампа следовать жесткой линии в отношении России, в том числе по вопросам противодействия «российской угрозе в киберпространстве». Кроме того, имеющийся пакет мер доверия – опять же наследие Обамы, один из поздних плодов уже катившейся под откос в 2013 г. «перезагрузки», – и Трамп едва ли сочтет возможным заниматься его восстановлением.

Что остается при таких вводных? Текущая ситуация в краткосрочном горизонте практически не оставляет окна возможностей для *большой сделки* или капитального размена по вопросам соблюдения «правил игры» – не говоря уже о каком-либо конструктивном сотрудничестве. Более того, не особенно понятно, кому и зачем такая «большая сделка» могла бы быть нужна, если она все равно не сможет обратить вспять долгосрочные процессы: наращивание и все более активное применение обеими сторонами разведывательного и военного киберпотенциала, форсированный протекционизм на внутренних ИТ-рынках («импортозамещение») под лозунгами национальной безопасности, все больший фокус на коалиционных форматах продвижения своих подходов и инициатив по вопросам кибербезопасности и киберпространства (с российской стороны речь идет о ШОС, БРИКС и двустороннем взаимодействии с КНР).

Confidential

После обвинений России в огромном массиве кибератак на критическую инфраструктуру США и стран Европы преодолеть логику конфронтации, по крайней мере со стороны Вашингтона, едва ли удастся в ближайшие годы – и новая киберстратегия Белого дома тому лишнее свидетельство.

Сценарии взаимодействия на ближайшие два года

- Наиболее реалистичный формат общения Москвы и Вашингтона по вопросам кибербезопасности и киберстабильности на ближайшие год-два – **рабочие визиты и закрытые совещания** между представителями вооруженных сил и спецслужб, организуемых по мере необходимости.
- Предметом обсуждений и точечных договоренностей могут стать технические форматы и схемы коммуникаций "military-to-military" с целью уведомления или экстренного предупреждения друг друга о проводимых кибероперациях, в том числе тех, которые могут наносить неумышленный (сопутствующий) ущерб одной из сторон взаимодействия.
- Использование таких механизмов может быть особенно актуально для предупреждения прямых столкновений и эскалации конфронтации в третьих странах и на территориях, где обе стороны косвенно или напрямую вовлечены в участие в военной операции или долгосрочном конфликте (например, в Сирии).
- Также предметом точечных непубличных соглашений могут стать **«зеркальные» ограничения** на проведение кибероперации в отношении отдельных категорий объектов критической инфраструктуры – таких как космические спутники военного и двойного назначения, а также стратегическая инфраструктура управления и командования вооруженными силами (C&C Infrastructure).

Авторы статьи: Олег Демидов, консультант ПИР-Центра, Маргарита Ангмар, магистрант факультета прикладной политологии Московского педагогического государственного университета (МПГУ)

Редактор: Юлия Сеславинская

(c) Trialogue Club International: trialogue@pircenter.org;
(c) Centre russe d'etudes politiques: crep@pircenter.org
Москва, Ноябрь 2018 г.

Выдержки из документа «Международный Клуб Триалог. Условия и правила членства».

3. Права членов Клуба

3.1. Индивидуальные члены Клуба имеют право:

3.1.3. Получать 1 экземпляр бюллетеня эксклюзивной аналитики Russia Confidential по электронной почте, на выбранном языке (русском или английском). По правилам Клуба, передача бюллетеня третьим лицам не допускается.[…]

3.2. Корпоративные члены Клуба имеют право:

3.2.3. Получать 2 экземпляра бюллетеня эксклюзивной аналитики Russia Confidential по электронной почте, на выбранном языке (русском или английском) либо на обоих языках одновременно, передавать этот бюллетень другим представителям

Confidential

корпоративного члена Клуба. По правилам Клуба, передача бюллетеня третьим лицам, не являющимся членами Клуба, не допускается.[…]

4. Обязанности членов Клуба

4.1. Все срочные члены Клуба обязаны:

4.1.6. Не передавать полученные материалы бюллетеня Russia Confidential, а также пароли доступа на сайт Клуба физическим и юридическим лицам, не являющимся членами Клуба. […]

6. Russia Confidential

6.1. Бюллетень эксклюзивной аналитики Russia Confidential выпускается ООО «Триалог» исключительно для личного пользования членов Клуба.

6.2. Бюллетень содержит сжатую эксклюзивную аналитику по вопросам международной безопасности, внешней и внутренней политики России и государств СНГ, подготовленную ведущими экспертами специально для Russia Confidential.

6.3. В течение не менее 30 дней со дня выхода материалы бюллетеня являются конфиденциальными и не могут цитироваться и передаваться лицам, не являющимся членами Клуба.

6.4. По прошествии не менее чем 30 дней ООО «Триалог» может снять эксклюзивный и конфиденциальный статус с материала, после чего в этих случаях он может быть опубликован в других изданиях и может быть использован для цитирования членами Клуба.

6.5. Бюллетень распространяется по электронным адресам членов Клуба 1 раз в месяц по русском или английском языке, по выбору члена Клуба.

6.6. По запросу члена Клуба, он может также получить бумажную версию бюллетеня на выбранном им языке.