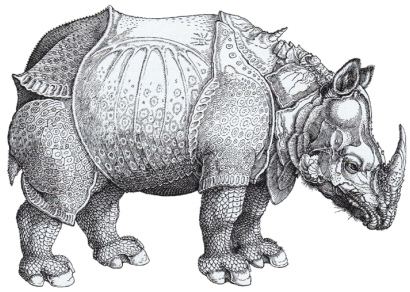


ИНДЕКС БЕЗОПАСНОСТИ
№1 | 2019
ПИР-ЦЕНТР | ТРИАЛОГ

Олег Демидов
Маргарита Ангмар

Киберстратегия США 2018

Значение для глобального диалога о поведении в сфере использования ИКТ и российско-американских отношений

Главный редактор: А.Ф. Зульхарнеев
Редактор: Ю.С. Сеславинская
Рецензент: Е.В. Черненко

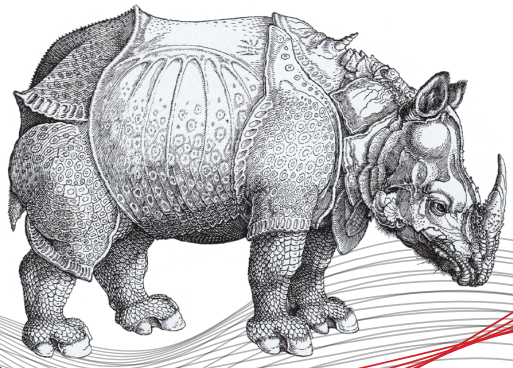
Демидов О.В., Ангмар М.А.

Киберстратегия США 2018. Значение для глобального диалога о поведении в сфере использования ИКТ и российско-американских отношений / Олег Демидов, Маргарита Ангмар. – М.: Триалог, 2019. – 27 с. – (Серия «Индекс Безопасности»).

В сентябре 2018 года была обнародована новая национальная киберстратегия США. Президент США Дональд Трамп в своих выступлениях подчеркивал, что новый документ впервые за долгое время предлагает конкретные меры для обеспечения кибербезопасности страны. СМИ же увидели в стратегии пересмотр приоритетов национальной политики в сторону более наступательного силового подхода. Авторы доклада Олег Демидов и Маргарита Ангмар анализируют содержание основных положений стратегии и ее влияние на развитие международного и российско-американского диалога по проблемам безопасности в киберпространстве.

Данный текст и другие материалы можно
найти на сайте: http://si.pircenter.org

Оглавление



Главное

НАЦИОНАЛЬНАЯ КИБЕРСТРАТЕГИЯ США, обнародованная 20 сентября 2018 года, является продуктом республиканской администрации президента Дональда Трампа. Несмотря на то, что Трамп представил стратегию как самостоятельную и прорывную, ее основные положения опираются на доктринальные документы, принятые в период президентства Барака Обамы. Эта преемственность особенно заметна на примере первого («Защита американского народа, отечества и американского образа жизни») и второго («Содействие американскому процветанию») столпов стратегии.

УПРАВЛЕНИЕ ИНТЕРНЕТОМ – МУЛЬТИСТЕЙКХОЛДЕРИЗМ. Не изменились подходы США к управлению интернетом. Несмотря на предвыборные заявления Дональда Трампа, новая киберстратегия США по-прежнему поддерживает модель управления интернетом с участием всех заинтересованных сторон.

ПРОАКТИВНАЯ ОБОРОНА. Накануне представления национальной киберстратегии, основные положения своей стратегии в кибепространстве опубликовал Пентагон. По сути, они конкретизируют документ Белого дома. В качестве основной деятельности минобороны заявляются проактивная оборона, каждодневное состязание со стратегическими соперниками, обеспечение готовности к войне за счет сбора разведданных и наращивание наступательного киберпотенциала. К стратегическим соперникам относятся Россия, Китай, Иран и Северная Корея.

КОАЛИЦИИ. Новое в стратегии – запуск Международной инициативы по кибersдерживанию – коалиции 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.

ФРАГМЕНТАЦИЯ ГЛОБАЛЬНОГО ДИАЛОГА ОБ ОТВЕТСТВЕННОМ ПОВЕДЕНИИ В КИБЕРПРОСТРАНСТВЕ. В конце 2018 года Россия и США выдвинули проекты резолюции ГА ООН о будущем Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Президент Франции Эммануэль Макрон представил «Парижский призыв к обеспечению доверия и безопасности в киберпространстве». Ситуация с одновременным продвижением трех подчеркнуто альтернативных друг другу инициатив говорит о том, что подлинно глобальный обмен мнениями о нормах и правилах поведения в киберпространстве и его регулировании распадается.

РОССИЯ – США. В отсутствие многостороннего и двустороннего диалога в свете новых доктринальных установок США Москве и Вашингтону остается готовиться к конфронтации, поддерживать каналы экстренной коммуникации и заранее расставлять «красные флажки», которые нельзя обходить ни при каких обстоятельствах – чтобы не перейти от «стратегического состязания» в киберпространстве к полномасштабному военному конфликту.

Забыть наследие Обамы? Основные концепции защиты киберпространства, принятые в президентство Барака Обамы

20 СЕНТЯБРЯ 2018 ГОДА, после нескольких месяцев давления со стороны Конгресса, Белый дом обнародовал новую «Национальную киберстратегию США»[1]. В документе намечены ключевые направления деятельности государственных органов США по обеспечению кибербезопасности и использованию киберпространства для экономического развития и процветания страны.

По словам президента США Дональда Трампа, представленный в сентябре документ — «первая четкая киберстратегия Соединенных Штатов за 15 лет». Таким образом, за предыдущую точку отсчета в американском стратегическом киберпланировании президент взял «Национальную стратегию по защите киберпространства»[2] , разработанную и утвержденную еще в феврале 2003 года при администрации Джорджа Буша-младшего.

Между тем в период президентства Барака Обамы также было принято немало стратегических документов в сфере кибербезопасности. Предыдущая всеобъемлющая стратегия была разработана и опубликована в 2011 году администрацией Барака Обамы[3]. А если говорить о введении конкретных мер, то стратегическим документом, решавшим такую задачу, был Национальный план действий в сфере кибербезопасности[4], утвержденный Бараком Обамой 9 февраля 2016 года.

Были также разработаны и опубликованы доктринальные документы отдельных ведомств, такие как серия стратегий для киберпространства минобороны США (в том числе Стратегия ведения деятельности в киберпространстве[5] 2011 года и киберстратегия 2015 года[6]). Не менее долгосрочное и глубокое стратегическое планирование в этот период осуществляло министерство внутренней безопасности (МВБ, Department of Homeland Security). Правда, к формату собственной ведомственной киберстратегии[7] МВБ пришло только при Трампе в мае 2018 года.

Наконец, нельзя не отметить ряд президентских указов Обамы, заложивших основу среднесрочной политики в сфере обеспечения безопасности, включая кибербезопасность критической инфраструктуры США: указы «Об улучшении кибербезопасности критической инфраструктуры» (2013)[8], «Продвижение обмена информацией о кибербезопасности в частном секторе» (2015)[9] и «О комиссии по повышению национальной кибербезопасности» (2016)[10].

Все это наследие не осталось грудой документов, а во многом сформировало и дополнило организационную и функциональ-

Перед публикацией новой киберстратегии Белого дома, Дональд Трамп предпочел демонстративно проигнорировать доктринальное наследие Барака Обамы, хотя именно оно заложило основу среднесрочной политики США в сфере обеспечения безопасности, включая кибербезопасность критической инфраструктуры

Источник: Michael Vadon

ную структуру госведомств США и определило векторы их деятельности, включая обеспечение кибербезопасности на период с 2011 по 2016 год, и потенциально далее. Так, согласно указу 2013 года, министерство обороны и Администрация общих служб США разработали рекомендации по оценке и внедрению стандартов безопасности в процесс управления контрактами и планирования закупок ИТ-продуктов. Согласно этому же указу, министерство внутренней безопасности разработало основанный на анализе рисков подход к определению критических инфраструктур, подверженных наибольшим рискам (Critical Infrastructure at Greatest Risk, CIGR). Также МВБ и минобороны запустили Углубленную программу услуг по кибербезопасности (Enhanced Cybersecurity Services), в рамках которой госорганы предоставляют данные о киберугрозах и техническую информацию владельцам и операторам критической инфраструктуры (КИ). В соответствии с целями Национального плана по защите инфраструктуры, принятого МВБ в 2013 году (NIPP-2013[11]), была создана базовая платформа для развития и координации взаимодействия между регуляторами, включая правоохранительные органы, и частным сектором – Консультативным советом партнерства по критической инфраструктуре (CIPAC).

Еще одна долгосрочная инициатива, огромная по масштабу задач и фундаментальная по значимости, запущенная при администрации Обамы, – Базовая рамочная программа для уменьшения рисков кибербезопасности КИ (NIST Cybersecurity Framework)[12]. Она реализуется Национальным институтом стандартов и технологий (NIST) с 2014 года. В рамках программы впервые была проведена систематизированная детализация базовых действий, направленных на обеспечение кибербезопасности (идентификация, защита, определение, ответ на инциденты и восстановление после инцидентов), а также их привязка к национальным и международным стандартам, включая стандарты самого NIST, а также стандарты COBIT, ИСО/МСЭ серии 27001, ISA серии 62443 и прочие. Вторая редакция базовой программы находится в разработке с 2015 года, ее доработка и развитие продолжаются и в настоящее время.

В своих выступлениях, приуроченных к публикации новой киберстратегии Белого дома, Дональд Трамп предпочел демонстративно проигнорировать это доктринальное наследие.

Такой принцип закономерен и присущ подходу новой президентской администрации и лично президента США к широкому кругу вопросов. В первый год своего президентства Трамп методично и даже с азартом занялся разрушением ключевых проектов и договоренностей, реализованных предыдущим хозяином Белого дома, – от пересмотра национальных программ медицинского страхования и налоговой политики до соблюдения Совместного всеобъемлющего плана действий (СВПД) по ядерной программе

Ирана и политики в отношении Китая, Кубы, европейских партнеров, союзников по НАТО и ряда других государств. Наиболее резко и рельефно такая деконструкция наследия Обамы проявляется в областях, связанных с национальной безопасностью и внешней политикой.

Вполне логично, что и вопросы обеспечения кибербезопасности американской нации не могли остаться вне этого процесса деконструкции – хотя бы потому, что громкий скандал по поводу предполагаемого вмешательства российских правительственных хакеров в президентскую избирательную кампанию 2016 года оставил стойкий след на репутации Трампа. Учащающиеся случаи масштабных хакерских атак и хищений данных также требовали (и продолжают требовать) внятной реакции и программы действий от Белого дома.

А был ли Трамп? Ключевые положения новой киберстратегии США

Ключевым продуктом первых 100 дней президентства Дональда Трампа стал проект президентского указа «Об укреплении кибербезопасности и возможностей США в киберпространстве» (Strengthening U.S. Cyber Security and Capabilities) – впоследствии он был переработан и превратился в президентский указ 13800 «Об укреплении кибербезопасности федеральных сетей и критической инфраструктуры» от 11 мая 2017 года[13]. Именно этот документ, а также проделанная в рамках его исполнения работа федеральных ведомств США во многом и составили концептуальную и логическую базу для новой киберстратегии Белого дома. Указ 13800 распределял среди федеральных ведомств (преимущественно по линии МВБ) три группы задач:

1.
Повышение уровня киберзащищенности федеральных информационных сетей, включая составление программы замены/обновления устаревшей ИТ-инфраструктуры федеральных ведомств, активизацию работы по выявлению и устранению уязвимостей в федеральных ИТ-системах и др.

2.
Обеспечение кибербезопасности критических инфраструктур, включая анализ и составление планов действий федеральных ведомств по поддержке и иному взаимодействию с операторами объектов КИ по вопросам обеспечения кибербезопасности; анализ, разработку планов действий и рекомендаций по улучшению мер обеспечения

защищенности объектов КИ, подверженных наибольшим рискам (CIGR); вовлечение вендоров и других частных субъектов в разработку и реализацию решений по повышению устойчивости объектов КИ перед ботнетами и другими сетевыми угрозами и др.

3.
Укрепление кибербезопасности американской нации, включая продвижение ценностей и проектов по развитию свободного интернета, разработку мер противодействия противникам США в киберпространстве, развитие международного сотрудничества в сфере кибербезопасности и борьбы с компьютерными преступлениями, наращивание потенциала национальных трудовых ресурсов и человеческого капитала для индустрии кибербезопасности и др.

Около 80% этой работы велось уже при администрации Обамы, но, возможно, в менее централизованном виде и не под прямым контролем исполнения президентских поручений. В ряде случаев форматы деятельности, практиковавшиеся давно, и уже установленные рабочие треки были попросту переименованы для целей отчетности о реализации указа. Например, в качестве основы для анализа акторов – потенциальных противников США в киберпространстве был взят ежегодный совместный доклад разведсообщества США о глобальных угрозах национальной безопасности (Statement for the Record Worldwide Threat Assessment of the US Intelligence Community), который включает раздел, где перечисляются источники угроз для США в киберпространстве как минимум с 2014 года. По большинству других пунктов отчеты во исполнение указа были подготовлены и опубликованы (в основном МВБ) только 30 мая 2018 года и не содержали предложений кардинально пересмотреть действующие политику и методологическую базу работы федеральных органов[14]. Основным результатом публикации отчетов стала разработка детальных дорожных карт по реализации отдельных пунктов указа, а также предложений по усилению и совершенствованию регулирования и обновлению действующих практик по отдельным вопросам. В частности, по вопросам усиления защиты инфраструктуры электросетей и инфраструктуры, задействованной в обеспечении электоральных процессов, а также реализации серии мероприятий по повышению уровня устойчивости федеральных ИТ-систем и сетей к сетевым атакам.

Таким образом, революции в подходе федеральных органов США к обеспечению кибербезопасности после принятия указа и выполнения поручений по нему не случилось, и ожидать ее было невозможно. Федеральная бюрократическая машина, еще пребывавшая в несколько смятенном состоянии по итогам президентских выборов, успешно сгенерировала на бумаге необходимую отчетность по исполнению указа и продолжила жить своей жизнью, по большей части реализуя уже выдвинутые ранее инициативы и запланированные мероприятия.

На все это важно обратить внимание потому, что нынешняя киберстратегия Белого дома во многом выстроена в той же логике имитации бурной деятельности по всем фронтам с претензией на радикальные нововведения и смену подхода. По факту же около 50% содержания новой киберстратегии Белого дома напрямую вытекает из того же президентского указа 13800, который, в свою очередь, отталкивается от доктринальной базы, разработанной и принятой в период президентства Обамы.

Национальная киберстратегия 2018 года предполагает активизацию усилий федерального правительства с вовлечением частного сектора и других заинтересованных сторон на четырех основных направлениях:

1.
ЗАЩИТА АМЕРИКАНСКОГО НАРОДА, ОТЕЧЕСТВА И АМЕРИКАНСКОГО ОБРАЗА ЖИЗНИ, включая:

1.1.
ПОВЫШЕНИЕ КИБЕРЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СЕТЕЙ ФЕДЕРАЛЬНЫХ ВЕДОМСТВ, в том числе централизация и повышение эффективности управления кибербезопасностью в госучреждениях, включая риск-менеджмент в сфере кибербезопасности; повышение качества управления цепочками поставок ИТ-продукции для федеральных ведомств и контроля за ними, а также обеспечение лидерства федеральных органов в области внедрения и стимулирования инноваций в ИТ-секторе (в основном в соответствии с указом 13800).

1.2.
ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ КИ, в том числе более четкое распределение функций различных структур в части киберзащиты КИ, приоритизация действий в соответствии с выявленными ключевыми рисками кибербезопасности КИ, стимулирование провайдеров технологий для объектов КИ к выполнению роли провайдеров кибербезопасности, защита от компьютерных атак и вмешательств в информационные системы, задействованные в электоральных процессах (по итогам событий 2016 года), стимулирование инвестиций в обеспечение кибербезопасности со стороны владельцев и операторов объектов КИ, повышение приоритета R&D в нише обеспечения кибербезопасности, повышение кибербезопасности морских и сухопутных систем транспортных коммуникаций, а также повышение киберзащищенности космической КИ США (в основном в соответствии с указом 13800).

1.3.
БОРЬБУ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ И РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ, в том числе совершенствование систем реагирования на компьютерные инциденты, обновление нормативно-правовых актов по электронному сбору данных и противодействию компьютерной преступности; снижение угроз, исходящих от трансграничных акторов, и повышение рисков для киберпреступников, действующих против США из других юрисдикций, а также укрепление и совершенствование механизмов правоприменения в рамках соглашений о борьбе с трансграничной компьютерной преступностью с государствами-партнерами (прежде всего в рамках Конвенции Совета Европы о борьбе с компьютерной преступностью от 2001 года) (в основном в соответствии с указом 13800).

Около 50% новой киберстратегии были ранее отражены как в президентских указах Трампа, так и в доктринах Барака Обамы – это особенно заметно на примере первого и второго столпов стратегии.

2.
СОДЕЙСТВИЕ АМЕРИКАНСКОМУ ПРОЦВЕТАНИЮ. Это направление предполагает следующие меры:

2.1.
РАЗВИТИЕ БЕЗОПАСНОЙ И РАСТУЩЕЙ ЦИФРОВОЙ ЭКОНОМИКИ путем содействия развитию рынка совместимых и безопасных ИТ-продуктов, продвижения инноваций в технологическом секторе, наращивания и стимулирования инвестиций в новые инфраструктурные проекты (например, сотрудничество с компаниями, развивающими технологии связи 5G, а также анализ возможностей использования искусственного интеллекта и квантовых вычислений), поощрения и поддержки новых разработок в области ИТ, а также продвижения концепции сквозного обеспечения кибербезопасности в рамках всего жизненного цикла ИТ-продуктов.

2.2.
ПОДДЕРЖКА И ЗАЩИТА АМЕРИКАНСКОГО ПОТЕНЦИАЛА ИЗОБРЕТАТЕЛЬСТВА И ОТКРЫТИЙ В СФЕРЕ ИТ, в том числе изменение системы регулирования иностранных инвестиций и ведения бизнеса на территории США, поддержка и укрепление национальной системы защиты интеллектуальной собственности, а также защита американских идей и изобретений и обеспечение конфиденциальности при их разработке.

2.3.
РОСТ ЧИСЛА ВЫСОКОКВАЛИФИЦИРОВАННЫХ КАДРОВ, РАБОТАЮЩИХ В ОБЛАСТИ ИТ И КИБЕРБЕЗОПАСНОСТИ, в том числе формирование и поддержка «конвейера талантов» в области ИТ и кибербезопасности, расширение возможностей переобучения и повышения квалификации для рабочих кадров страны, повышение квалификации человеческих трудовых ресурсов федеральных ведомств, а также вовлечение госорганов в деятельность по выявлению и стимулированию талантов в сфере ИТ и кибербезопасности (в основном в соответствии с указом 13800).

3.
СОХРАНЕНИЕ МИРА ЧЕРЕЗ УКРЕПЛЕНИЕ СИЛЫ, что включает следующие шаги:

3.1.
УКРЕПЛЕНИЕ ГЛОБАЛЬНОЙ СТАБИЛЬНОСТИ В КИБЕРПРОСТРАНСТВЕ за счет разработки и продвижения среди членов международного сообщества добровольных норм ответственного поведения государств.

3.2.
ОПРЕДЕЛЕНИЕ ИСТОЧНИКА КИБЕРАТАК (АТРИБУЦИЯ) И СДЕРЖИВАНИЕ НЕПРИЕМЛЕМОГО ПОВЕДЕНИЯ В КИБЕРПРОСТРАНСТВЕ, в том числе активизация целевой разведывательной работы с опорой на взаимодействие и обмен

данными с государствами-союзниками, обеспечение последствий для акторов, практикующих недружественные и неприемлемые действия против США в киберпространстве, разработку и реализацию инициативы по сдерживанию угроз и враждебных акторов в киберпространстве, а также противодействие враждебным информационным операциям и скрытому влиянию на общественное мнение и социально-политические процессы через киберпространство.

4.
ПРОДВИЖЕНИЕ АМЕРИКАНСКОГО ВЛИЯНИЯ В КИБЕРПРОСТРАНСТВЕ:

4.1.
ПОДДЕРЖКА ОТКРЫТОГО, ОСНОВАННОГО НА СОВМЕСТИМЫХ ТЕХНОЛОГИЯХ, НАДЕЖНОГО И БЕЗОПАСНОГО ИНТЕРНЕТА, в том числе продвижение и поддержка свободы доступа и использования интернета, вовлечение в сотрудничество и совместную работу заинтересованных сторон в государствах, поддерживающих открытый и свободный интернет; продвижение модели управления интернетом с участием всех заинтересованных сторон; поддержка и продвижение связности, надежности и отказоустойчивости коммуникаций, а также совместимости протоколов, стандартов и технологий глобальной сети; расширение международных рынков для внедрения американских ИТ-инноваций, идей и изобретений.

4.2.
Наращивание международного потенциала и ресурсов в области обеспечения кибербезопасности, в том числе в формате совместных международных программ.

Из текста документа можно сделать несколько выводов. Прежде всего в большинстве разделов новой стратегии почерк и влияние новой президентской администрации и лично Дональда Трампа либо просматриваются достаточно слабо, либо не просматриваются совсем.

Можно даже утверждать, что документ вообще не является стратегией в строгом смысле этого слова – то есть документом долгосрочного планирования, поскольку не формирует и не задает согласованный вектор деятельности для участников системы государственного управления США. Новая стратегия этот вектор скорее собирает 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 («Защита американского народа, отечества и американского образа жизни») и частично второй (в области увеличения количества высококва-

Предвыборные заявления Трампа о неприятии мультистейкхолдерной модели не отразились в новой стратегии: документ декларирует поддержку участию всех заинтересованных сторон в управлении интернетом.

лифицированных кадров для отрасли кибербезопасности) в обобщенном виде воспроизводят положения отдельной ведомственной Стратегии кибербезопасности МВБ[15], опубликованной 15 мая 2018 года, – деполитизированной и основанной на реализации и развитии ряда долгосрочных инициатив, многие из которых были запущены при предыдущем хозяине Белого дома.

Это наблюдение подкрепляется и тем, что деятельность МВБ в области защиты объектов КИ, подверженных наибольшим рискам, до сих пор ведется[16] на основе методологии и риск-ориентированного подхода, описанных в упомянутом президентском указе Обамы от 2013 года. На уровне же организационной структуры центром работы по обеспечению киберзащищенности КИ и реагированию на компьютерные инциденты на объектах федеральной ИТ-инфраструктуры является созданный в 2009 году Национальный центр по интеграции кибербезопасности и коммуникаций (NCCIC)[17], подструктурами которого выступают US-CERT и ICS-CERT.

Раздел стратегии МВБ, а также доклад ведомства[18] президенту в рамках исполнения указа 13800 более амбициозны и подразумевают масштабную программу «наведения порядка» по направлениям модернизации федеральных ИТ-систем. В частности, по направлениям оценки и повышения киберзащищенности таких систем, централизации управления и упорядочивания функций госструктур в цепочках поставок, контроле внедрения и мониторинге безопасности федеральных ИТ-систем, выявлении и устранении уязвимостей в них. Это работа своевременна и необходима, но ее появление в стратегии не связано с политическими приоритетами новой президентской администрации.

Проблема существования разновозрастного и разноплатформенного набора федеральных ИТ-систем в США хроническая, ей не меньше 15-20 лет, и с каждым годом ее масштаб лишь нарастает пропорционально разрастанию ИТ-инфраструктуры федеральных ведомств. Именно поэтому централизация полномочий в выборе новой архитектуры устанавливаемых систем и обеспечения их совместимости, а также в части закупок и внедрения ИТ-систем для федеральных ведомств уже давно присутствует на повестке дня. Следует понимать, что повышение уровня кибербезопасности федеральных ИТ-систем – лишь один из потенциальных дивидендов от решения этой проблемы. Для российских читателей понятной аналогией будет сравнение с вереницей программ по информатизации и цифровизации отечественных госорганов (программы «Электронное правительство», «Информационное общество», «Цифровая экономика») – только в США программ и вовлеченных субъектов в несколько раз больше. Из этого следует, что администрация Трампа, как и отдельные ведомства, была обречена в той или иной степени заняться этим вопросом, особенно с учетом роста успешных кибератак на ИТ-системы американских госучреждений за последние годы.

Не менее ярким и даже парадоксальным примером того, насколько киберстратегия Трампа преемственна по отношению к наработкам администрации Обамы, служит раздел документа о продвижении и поддержке свободного интернета. В этой части стратегия показательно консервативна и дословно повторяет текст и посыл стратегических документов и заявлений американского руководства при Бараке Обаме: США поддерживают открытый и свободный интернет, выступают за беспрепятственный доступ и использование глобальной сети во всем мире, а также по-прежнему приверже-

ны модели управления интернетом с участием всех заинтересованных сторон (так называемая мультистейкхолдерная модель).

Парадоксальным выглядит именно последний пункт – о приверженности мультистейкхолдерной модели управления технической инфраструктурой интернета.

Предвыборные заявления Трампа о неприятии этой модели никак не отразились на целях и ценностях новой киберстратегии: раздел про поддержку участия всех заинтересованных сторон в управлении интернетом словно скопирован из документов обамовской администрации. Этому есть два возможных объяснения. Первое заключается в том, что, в отличие от остальных договоренностей, достигнутых бывшим хозяином Белого дома и пересмотренных новым президентом, в сфере управления инфраструктурой интернета слом итогов работы администрации Обамы оказался бы совсем непродуктивен и потенциально катастрофичен для репутации американского правительства. Поэтому администрации Трампа пришлось хотя бы временно оставить все как есть, смириться с итогами IANA Stewardship Transition и двигаться по накатанным рельсам, превознося завоевания мультистейкхолдерной модели. Но нельзя исключать и второе возможное объяснение. Разобравшись с сутью произошедших изменений, Трамп мог осознать, что никакой утраты контроля США над интернетом в пользу России и Китая не произошло, а завершенный в сентябре 2016 года процесс в большей степени являлся давно назревшей организационно-технической реформой, получившей не совсем адекватное освещение в масс-медиа, и тогда эта история перестала его интересовать.

КОНТЕКСТ: ЧТО ТАКОЕ IANA STEWARDSHIP TRANSITION

Одним из ключевых процессов, который администрации Обамы удалось успешно довести до точки невозврата незадолго до президентских выборов 2016 года, стала так называемая передача координирующей роли в исполнении функций Администрации адресного пространства интернет (IANA) от правительства США глобальному сообществу заинтересованных сторон (IANA Stewardship Transition[19]). Активная фаза этого процесса была запущена в 2014 году, на волне международного скандала с разоблачениями Эдварда Сноудена, бросившего серьезную тень на репутацию США как глобального гаранта свободы и соблюдения прав пользователей в интернете. Ключевым итогом процесса стало то, что правительство США в лице Национальной администрации по телекоммуникациям и информации (NTIA) перестало быть стороной контракта с Корпорацией интернета по присвоению имен и номеров (ICANN) и как следствие перестало осуществлять координирующую роль в исполнении функций технического подразделения корпорации (IANA) по обслуживанию глобальной системы уникальных идентификаторов интернета, включая глобальную систему доменных имен (DNS).

Для СМИ и широкой общественности, включая политические круги в самих США, день истечения контракта NTIA с ICANN (30 сентября 2016 года) стал днем, когда «правительство США отдало контроль над глобальным интернетом». Несмотря на то что фактически суть процесса была гораздо более специфической и узкой, медийное освещение и ажиотаж вокруг него привели к тому, что ряд политических сил стал рассматривать[20] IANA Stewardship Transition чуть ли не как капитуляцию администрации демократов перед авторитарными государствами, стремящимися установить в сети глобальную цензуру и якобы получившими шанс взять техническую инфраструктуру интернета под собственный контроль. На этой волне пытался спекулировать и Дональд Трамп в ходе своей избирательной кампании – так, в заявлениях его предвыборного штаба отмечалось[21], что «Трамп не позволит Обаме передать контроль над интернетом в руки иностранных держав». Правда, после избрания Трампа новым президентом США вопрос потенциального пересмотра решения о выходе NTIA из контрактных отношений с ICANN довольно быстро исчез из его повестки. 19 января 2017 года министр торговли США Уилбур Росс заявил о невозможности пересмотра итогов IANA Stewardship Transition. Однако в той или иной форме интерес ключевых фигур новой администрации Белого дома к усилению роли и статуса правительства США в новой, постпереходной конструкции технических организаций, обслуживающих глобальную инфраструктуру сети, сохранился по сей день[22].

Полет ястреба: стратегия проактивной обороны и коалиция по киберсдерживанию

Сказанное выше, однако, не означает, что ни одна из составляющих новой стратегии не несет изменений в политическом курсе и не отражает взглядов новой администрации на обеспечение кибербезопасности и защиту интересов США в киберпространстве. Практически все внимание СМИ и экспертного сообщества в связи с публикацией документа оказалось сосредоточено на его третьем столпе – стратегии правительства США в сфере 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 Джона Болтона, который, анонсируя стратегию 20 сентября 2018 года, подчеркнул: «Мы не будем задействовать только оборонные меры, мы намерены участвовать в наступательных операциях, и наши соперники должны иметь это в виду»[23]. Акцент на расширение возможностей по проактивным действиям против стратегических соперников и иных враждебных акторов в киберпространстве, а также на готовность санкционировать и осуществлять такие операции звучал в выступлении Болтона неоднократно.

В качестве одного из значимых шагов администрации Трампа, который, по словам Болтона, развязывает руки США в части проактивных действий в киберпространстве, стала отмена директивы президента США «О политике США в области кибероперций» (Presidential Policy Directive 20, PPD 20)[24], принятой в октябре 2012 года со статусом «высший уровень секретности» и рассекреченной в июне 2013 года Эдвардом Сноуденом. В числе принципов и процессов принятия решений директива предусматривала следующие процедуры:

- Решение о проведении кибероперций с существенными последствиями (Cyber Operations with Significant Consequences, к ним могут относиться защитные и проактивные кибероперации, а также сбор данных в киберпространстве) должно отдельно утверждаться президентом США[25].

- Для принятия решения о проведении операций по реагированию на систематическую вредоносную активность в киберпространстве (Responses to Persistent Malicious Cyber Activity) закрепляется процедура координации между ответственным ведомством (минобороны и Объединенное киберкомандование ВС США) и рядом других федеральных органов власти (Госдепартамент, министерство юстиции, МВБ, ФБР и др.).

- Действия в киберпространстве в чрезвычайных обстоятельствах (Emergency Cyber Actions), необходимые для срочного отражения длящейся кибератаки или нейтрализации непосредственной угрозы из киберпространства, минобороны и его руководство могут осуществлять без получения предварительного согласия от президента США, если на это нет времени. Однако по возможности необходимо координировать такие действия с другими федеральными ведомствами (см. предыдущий пункт), а о предпринятых действиях необходимо отчитаться президенту через советника по национальной безопасности.

- Сходные механизмы межведомственной координации и согласования решений, в том числе по проактивным кибероперациям (Offensive Cyber Effects Operations, OCEO).

Теперь, если верить Болтону, эти процедуры согласования и утверждения решений о проведении кибероперациий, включая проактивные кибероперации и операции с существенными последствиями, отменяются в соответствии с духом новой стратегии и требованиями времени. Потенциальные адресаты этого сообщения были предельно четко обозначены и в самой стратегии, и в заявлении Болтона, и в пресс-релизах Белого дома. Список «обычных подозреваемых» из числа «стратегических соперников США в киберпространстве» не меняется около последних 6 лет: это Иран, Китай, Россия и Северная Корея[26]. Пожалуй, можно констатировать разве что укрепление позиций России в этом рейтинге в связи с глобальным ажиотажем вокруг российских государственных хакеров в последние годы. Претензии к остальным участникам злополучной четверки стандартны: стратегический кибершпионаж и «триллионные» хищения американской интеллектуальной собственности со стороны Китая; кибератаки, компьютерная преступность и подрыв стабильного и свободного киберпространства со стороны Ирана и КНДР. При этом в самой стратегии речь напрямую не идет о ставке на проактивные и наступательные кибероперации. В тексте говорится лишь о том, что США будут использовать «все доступные средства», в том числе политико-дипломатические, экономические и военные меры воздействия, включая действия в киберпространстве и применение кинетических вооружений.

Насколько сильно такой посыл отличается от доктрин периода Обамы? Исходя из текста стратегии, непринципиально – допустимость использования всех доступных средств, включая обычные вооружения для реагирования на агрессию и враждебные действия в киберпространстве, закрепилась в американской оборонной доктрине еще в 2011 году с принятием Стратегии для киберпространства минобороны США[27]. Кроме того, сами наступательные кибероперации были допустимы в теории и проводились на практике и при Обаме с прямым участием минобороны и АНБ. В качестве примера достаточно вспомнить Stuxnet, кибератаку на государственных телекоммуникационных провайдеров в Сирии или «кибероперации против России», санкционированные Обамой в конце 2016 года в качестве ответа на предполагаемое вмешательство российских хакеров в избирательную кампанию США. Директива PPD 20 лишь закрепила механизм контроля над принятием решений об их проведении, но отнюдь не сделала их недопустимыми или нелегальными с точки зрения самих США.

Список «обычных подозреваемых» из числа «стратегических соперников США в киберпространстве» не меняется около последних 6 лет: это Иран, Китай, Россия и Северная Корея.

Но есть ли какое-то основание под заявлениями о ястребиной линии и наступательном уклоне новой стратегии администрации Трампа помимо заявлений самого Дональда Трампа и Джона Болтона? Ответ на этот вопрос положительный. 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 года, краткую выжимку из своей новой киберстратегии опубликовало минобороны США[28] – и в ней приоритеты расставлены недвусмысленно:

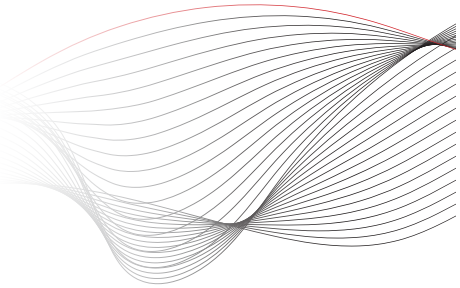
Пересмотр приоритетов Соединенных Штатов в сторону наступательных силовых действий зафиксирован в новой стратегии минобороны США.

- 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;
- Приоритетом для минобороны США является каждодневное участие в этом стратегическом состязании с первоочередным приоритетом стратегического противодействия Китаю и России в киберпространстве;
- Минобороны планирует проводить кибероперации с целью сбора разведданных и наращивания военного потенциала на случай полномасштабного кризиса;
- Минобороны планирует осуществлять операции в рамках проактивной кибероборонs 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 кибероперацій на всех театрах военного конфликта;
- Основнаые цели минобороны США в киберпространстве, согласно новой стратегии, – «обеспечить проактивную оборону, отладить работу в формате каждодневного состязания [со стратегическими соперниками], а также обеспечить готовность к войне», в том числе за счет создания более «смертоносных» вооруженных сил в части деятельности в киберпространстве.

Как и стратегия минобороны, документ Белого дома затрагивает и проблему 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», а также более тесным взаимодействием государственных органов с экспертными структурами, частным сектором и гражданским обществом в США и союзных государствах.

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.



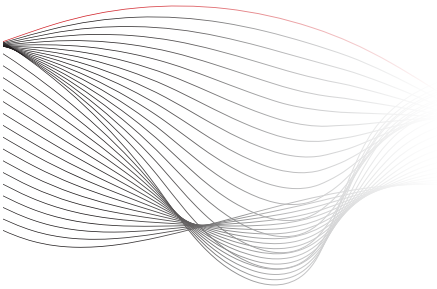
Одна из принципиально новых задач США, заявленных в киберстратегии, – запустить международную инициативу по киберсдерживанию (Cyber Deterrence Initiative). Цель инициативы – сформировать коалицию совместно с государствами, разделяющими общие ценности и подходы США в отношении кибербезопасности для того,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

Планируется, что участники коалиции будут:

- обмениваться разведданными о киберугрозах и враждебных акторах;
- проверять и подтверждать атрибуцию трансграничных кибератак;
- публично поддерживать проводимые партнерами по коалиции операции по реагированию на киберугрозы и кибератаки;
- совместными усилиями обеспечивать наступление последствий для субъектов, осуществляющих враждебную деятельность 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 состоит 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 подтверждении выводов по атрибуции кибератак третьими сторонами–участниками коалиции.



Кроме того, состав такого альянса никак не планируется ограничивать географически – единственный критерий: приверженность ценностям и подходу США в области международного противодействия «злонамеренным субъектам» в киберпространстве.

Еще одно любопытное направление действий, фигурирующее в последних стратегиях Пентагона и Белого дома, – продвижение международных норм и иных трансграничных инициатив, направленных на сдерживание враждебных акторов и предупреждение «неприемлемого поведения» в киберпространстве. Подход США к вопросу о международно-правовом ограничении действий государств в киберпространстве опять же окончательно оформился в последние годы президентства Обамы – примерно к 2014-2015 году. С тех пор Америка делает упор на необходимость международных норм ответственного поведения, распространяющихся прежде всего на государства и связанных с ними акторов-посредников. При этом такие нормы должны носить в основном добровольный и необязывающий характер – идея юридически обязывающего международного договора или иного соглашения об ограничении использования силы, или иного неприемлемого поведения в киберпространстве, много лет продвигаемая Россией, рассматривается как преждевременная, нереалистичная и чреватая усилением глобальной цензуры в киберпространстве. Вторым важным инструментом считаются меры прозрачности и доверия в области кибербезопасности (TCBMs), образцом которых могут служить соглашения между РФ и США от июня 2013 года, а также расширенный набор подобных мер, сформированный к 2016 году на площадке ОБСЕ.

Вопрос в том, насколько администрация Трампа будет на практике заинтересована в продвижении и реализации таких многосторонних механизмов – особенно за пределами условного круга государств, имеющих сходные позиции и подходы к вопросам обеспечения кибербезопасности и поведения в киберпространстве. Иначе говоря, понадобятся ли Белому дому добровольные нормы и меры доверия в отношениях с другими ключевыми кибердержавами (включая, конечно, Россию и Китай), если на данный момент в качестве основного «рабочего инструмента» рассматриваются наступательные кибероперации и расширение военных возможностей США в киберпространстве?

Инициативы Москвы, Вашингтона и Парижа – лебедь, рак и щука выработки норм ответственного поведения государств в области использования ИКТ

Эволюция стратегической мысли США неизбежно влияет на подходы Вашингтона к многосторонним и двусторонним механизмам кибербезопасности.

Сохранение и даже усиление курса США на продвижение добровольных норм ответственного поведения в киберпространстве ставит вопрос о дальнейшей судьбе Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ ООН). Эта группа, созданная по инициативе России в 2004 году, является основной площадкой для многосторонней разработки и согласования проектов таких норм. Работа пятого созыва группы завершилась в июне 2017 года болезненным провалом – после двух успешных докладов 2013 и 2015 годов, а также согласования предварительного перечня добровольных норм участники группы впервые с 2005 года не смогли прийти к консенсусу и приняли лишь протокольный доклад о своей работе. Камнем преткновения для группы стал предложенный США и поддержанный западными государствами проект норм, интерпретирующих положения Устава ООН и корпус норм международного гуманитарного права применительно к действиям в киберпространстве в обстановке военного конфликта. Представители Кубы и России сочли, что такой подход легитимирует превращение киберпространства в арену военных действий, и в качестве альтернативы вновь предложили разработать и принять международное юридически обязывающее соглашение об ответственном поведении и соблюдении государствами международно-правовых норм деятельности в киберпространстве.

По итогам заседаний группы 26 июня 2017 года советник президента США по внутренней безопасности Томас Боссерт[29] заявил, что «формат группы выработал лимит своих возможностей» и «настало время рассмотреть другие варианты»[30]. В том же выступлении 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».

Все это вполне соответствует посылу новой стратегии Белого дома – за прошедшие полтора года с выступления Боссерта и завершения работы пятой ГПЭ ООН акценты в новом документе сильнее сместились в сторону коалиционной логики (учитывая вышеупомянутую инициативу по киберсдерживанию).

Томас 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».

Источник: Mandel Ngan/AFP/Getty Image

Все это однозначно плохие новости и для Группы правительственных экспертов ООН, и для тех сил в России, которые выступают за восстановление диалога и механизмов сотрудничества с США в области кибербезопасности. Прописанный в стратегии подход очень логично встраивается в общий курс новой администрации, практикующей активный и жесткий пересмотр участия США в многосторонних архитектурах соглашений и сотрудничества по многим направлениям – кибербезопасность не стала исключением.

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 деятельность США в рамках ГПЭ ООН.

Наиболее вероятными до недавнего времени представлялись две стратегии действий в отношении участия США в ГПЭ ООН:

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 последовали бы и их ключевые союзники по НАТО и партнеры по Группе семи. Второй вариант мог натолкнуться на сопротивление России и ряда других ключевых членов группы, особенно если состав гипотетической новой структуры предполагалось сформировать без участия этих государств.

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 внезапно пошли по третьему пути, парадоксальным образом поменявшись с Россией местами

в части позиции относительно ГПЭ ООН. 9 ноября 2018 года Россия и США представили в Первый комитет Генассамблеи ООН два конкурирующих проекта резолюций, оба они были приняты членами комитета. В центре обеих резолюций – будущее многостороннего диалога о нормах ответственного поведения государств в киберпространстве и конкретно дальнейшая судьба ГПЭ ООН:

- Разработанный Россией проект резолюции призывает к комплексному перезапуску группы в 2019 году с изменением формата ее работы в сторону большей открытости и прозрачности ее рабочего процесса[31]. Во-первых, из текста резолюции вытекает необходимость расширения состава государств-участников и более справедливого географического и регионального представительства в ней. В прошлых созывах группы участвовали представители 25 государств. Российский проект резолюции предлагает дать возможность участия представителям всех без исключения государств. Во-вторых, предлагается сделать группу открытой для участия других заинтересованных сторон – частного бизнеса, экспертов и технических организаций. Наконец, резолюция предусматривает повышение статуса группы до полноценной рабочей площадки Генассамблеи ООН, уполномоченной самостоятельно готовить и рекомендовать к принятию государствам–членам ООН проекты документов, включая, например, проекты международных договоров.

- США (а также их партнеры по НАТО и альянсу «Пяти глаз»)[32] отказались поддержать Россию – Вашингтон внес свой проект резолюции, в котором де-факто предлагает возобновить работу группы в более или менее прежнем формате с рядом точечных нововведений[33]. Предмет и направления ее работы также в целом предлагается не менять, сохранив акцент на исследовании и обмене мнениями о применении международного права к действиям в киберпространстве, наращивании потенциала в области ИКТ, а также развитии сотрудничества с региональными международными структурами (ОБСЕ, ЕС, Региональный форум АСЕАН, Африканский союз и проч.). Проект резолюции содержит реверанс в сторону большей открытости рабочей группы – предлагается организовать на ее площадке серию консультативных встреч открытого состава, в которых смогут принять участие представители всех заинтересованных государств. Однако такой формат не меняет механизма принятия решений, замкнутого на экспертов–представителей 25 «постоянных» участников группы.

Парадоксальным образом позиция США по отношению к ГПЭ ООН развернулась на 180 градусов – с 2004 по 2009 год главным лоббистом группы была Россия, США же в первые годы относились к новому механизму прохладно и саботировали работу над первым докладом группы в 2005 году. Теперь сам Вашингтон выступает за возобновление ее работы и в тексте резолюции отмечает важность наработок группы в 2013-2015 годах, когда ее участниками были согласованы первые своды предлагаемых добровольных норм ответственного поведения в области использования ИКТ, а также базовые положения о применимости основополагающих принципов меж-

дународного права к деятельности в киберпространстве. Россия же, напротив, настаивает на том, что ее детище в нынешнем формате неэффективно и нуждается в радикальной трансформации.

5 декабря 2018 года российский проект резолюции был принят Генассамблеей ООН. В соответствии с принятым документом уже летом 2019 года должны быть организованы первые заседания новой рабочей площадки открытого состава. Процесс принятия проекта резолюции США чуть затянулся в связи с согласованием дополнительных бюджетных расходов, которые будут необходимы в случае ее принятия. Серьезных сомнений в том, что и американский проект будет принят, однако, нет – а значит, впереди уникальная ситуация параллельного сосуществования, работы и, вероятно, взаимной конкуренции двух рабочих механизмов с примерно одинаковым мандатом при Генассамблее ООН[34].

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.

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 списки соавторов двух резолюций:

- «Ядро», возглавляемое США: государства НАТО, Австралия и Украина.
- «Ядро», возглавляемое Россией: Китай и другие государства ШОС, некоторые участники СНГ (Азербайджан, Белоруссия, Казахстан, Таджикистан, Узбекистан), КНДР, государства Латинской Америки с левыми режимами (Боливия, Венесуэла, Куба, Никарагуа), Сирия и 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 три дня) с третьей независимой инициативой, исходящей от Франции. 12 ноября 2018 года президент Эммануэль Макрон на всемирном Форуме по управлению интернетом анонсировал «Парижский призыв к обеспечению доверия и безопасности в киберпространстве»[35]. В опубликованном тексте декларации не упоминается ГПЭ ООН, однако предлагаемые девять направлений действий по большей части перекликаются с наработками группы образца 2013 и 2015 годов. Разве что более четкий акцент сделан на роль частного сектора и технического сообщества.

Практического смысла сопоставлять девять предлагаемых направлений действий Парижского призыва со списком проектов добровольных норм ГПЭ ООН немного: смысл инициативы не в том, чтобы предложить нечто качественно новое с содержательной точки зрения, а в том, чтобы усилить роль Франции как ме-

диатора и двигателя процесса согласования общих норм для киберпространства. Пользуясь расколом ГПЭ ООН и крахом диалога между США и Россией, Макрон пытается вернуть Франции роль великой дипломатической державы в новой критически важной сфере международных отношений – возрождая 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 распадается.

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

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 хорошей новостью здесь стоит считать разве что отсутствие плохих новостей. 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 и пока не предвидится.

Эмманюэль Макрон на всемирном Форуме по управлению интернетом анонсировал «Парижский призыв к обеспечению доверия и безопасности в киберпространстве»

Источник: Ludovic Marin / AP

Расставить красные флажки. Перспективы российско-американского диалога в сфере безопасного использования ИКТ

Остается двусторонний формат взаимодействия, где ничего конструктивного не происходит с 2014 года, когда были заморожены российско-американские соглашения о мерах доверия в области кибербезопасности, подписанные Владимиром Путиным и Бараком Обамой всего годом ранее, в июне 2013 года. Пытаться восстановить механизм 2013 года сейчас – бесперспективный проект для Дональда 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 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, капитального размена по вопросам соблюдения правил игры и поддержания стабильности в киберпространстве между Москвой и Вашингтоном, не говоря уже о каком-либо конструктивном сотрудничестве.

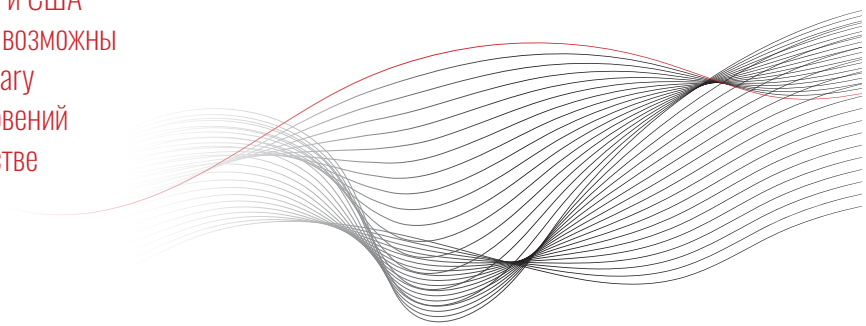
Более того, не особенно понятно, кому и зачем такая большая сделка могла бы быть нужна, если она все равно не сможет обратить вспять долгосрочные процессы: наращивание и все более активное применение обеими сторонами разведывательного и военного киберпотенциала, форсированный протекционизм на внутренних 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).

После обвинений России в совершении ряда 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.

Остается готовиться к такой конфронтации и по возможности заранее расставлять *красные флажки*, которые нельзя переходить ни при каких обстоятельствах, чтобы не перейти от «стратегического состязания» в киберпространстве к полномасштабному военному конфликту.

Наиболее реалистичный сценарий общения Москвы и Вашингтона по вопросам кибербезопасности и киберстабильности на

Говорить о сотрудничестве России и США не приходится: в ближайшие годы возможны контакты по линии military-to-military во избежание случайных столконовений между странами в киберпространстве

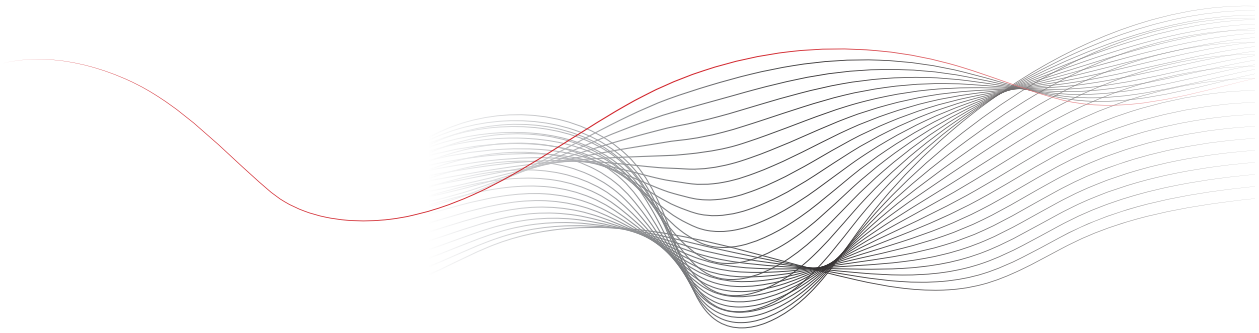


ближайшее время – развитие механизмов предупреждения столкновений и эскалации в киберпространстве.

Коммуникация и взаимодействие сторон, скорее всего, будут преимущественно непубличными и лишенными постоянной рабочей площадки – скорее речь будет идти о встречах ad-hoc, 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 в долгосрочном конфликте, например в Сирии.

Также предметом точечных непубличных соглашений могут стать зеркальные ограничения на проведение кибероперациий в отношении отдельных категорий объектов критической инфраструктуры, таких как космические спутники военного и двойного назначения, а также стратегическая инфраструктура управления и командования вооруженными силами.



ПРИМЕЧАНИЯ

[1] National Cyber Strategy of the United States of America. September 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[2] The National Strategy to Secure Cyberspace. February 2003. URL: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[3] International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. May 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[4] Cybersecurity National Action Plan. February 2016. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

[5] Department of Defense Strategy for Operating in Cyberspace. July 2011. URL: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

[6] The Department of Defense Cyber Strategy. April 2015. URL: http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf

[7] U.S. Department of Homeland Security Cybersecurity Strategy. May 2018. URL: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

[8] Executive Order – Improving Critical Infrastructure Cybersecurity. February 12, 2013. URL: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[9] Executive Order – Promoting Private Sector Cybersecurity Information Sharing. February 13, 2015. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

[10] Executive Order – Commission on Enhancing National Cybersecurity. February 09, 2016. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity

[11] National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. URL: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

[12] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[13] Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (Executive Order 13800). May 11, 2017. URL: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[14] DHS Report on Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. May 2017. URL: https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure

[15] U.S. Department of Homeland Security Cybersecurity Strategy. May 2018. URL: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

[16] Support to Critical Infrastructure at Greatest Risk ("Section 9 Report") Summary. August 2018. URL: https://www.dhs.gov/publication/support-critical-infrastructure-greatest-risk-section-9-report-summary

[17] National Cybersecurity and Communications Integration Center. URL: https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

[18] Report to the President on Federal IT Modernization. 2017. URL: https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf

[19] IANA Stewardship Transition для непосвященных — что происходит? ПИР-Центр. 2016. http://pircenter.org/media/content/files/13/14737442960.pdf

[20] Cruz slams Obama for 'internet giveaway'. Politico. August 8, 2016. URL: https://www.politico.com/story/2016/09/internet-transition-icann-227864

[21] TRUMP: ICANN'T EVEN! America won't hand over internet control to Russia on my watch. The Register. September 21, 2016. URL: https://www.theregister.co.uk/2016/09/21/trump_wading_into_iana_transition/

[22] Is the Trump administration really trying to reverse the IANA transition? Domain Incite. January 29, 2018. URL: http://domainincite.com/22579-is-the-trump-administration-really-trying-to-reverse-the-iana-transition

[23] John Bolton: US is going on the offensive against cyberattacks. September 20, 2018. URL: https://edition.cnn.com/2018/09/20/politics/us-cybersecurity-strategy-offense-john-bolton/index.html

[24] Presidential Policy Directive 20. October 2012. URL: https://fas.org/irp/offdocs/ppd/ppd-20.pdf

[25] Под «существенными последствиями» в PPD 20 понимаются: «Гибель людей, существенные ответные действия против США, существенный ущерб собственности, серьезные недружественные последствия для США во внешнеполитической сфере или существенные экономические последствия для США»

[26] 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 киберагрессию в будущем. Китай был задействован в экономическом шпионаже в киберпространстве и краже интеллектуальной собственности на триллионы долларов»

[27] Department of Defense Strategy For Operating in Cyberspace. July 2011. URL: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

[28] Summary. Department of Defense Cyber Strategy. 2018. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[29] Томас Боссерт покинул пост советника президента США по внутренней безопасности в апреле 2018 г.

[30] Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017. June 26, 2017. URL: https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/

[31] A/C.1/73/L.27*. Developments in the field of information and telecommunications in the context of international security. URL: https://undocs.org/A/C.1/73/L.27

[32] Австралия, Канада, Новая Зеландия, Великобритания и США.

[33] A/C.1/73/L.37. Advancing responsible State behaviour in cyberspace in the context of international security. URL: https://undocs.org/A/C.1/73/L.37

[34] 7 December 2018. Press release on the adoption of a Russian resolution on international information security at the UN General Assembly. MFA of Russia. http://www.mid.ru/en_GB/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3437775

[35] Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace. November 12, 2018. URL: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

АББРЕВИАТУРЫ И СОКРАЩЕНИЯ, ИСПОЛЬЗУЕМЫЕ В ТЕКСТЕ

АНБ – Агентство национальной безопасности США

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

ИКТ – информационно-коммуникационные технологии

ИСО – Международная организация по стандартизации

ИТ – информационные технологии

КИ – критическая инфраструктура

МВБ – министерство внутренней безопасности США

МСЭ – Международный союз электросвязи

ОБСЕ – Организация по безопасности и сотрудничеству в Европе

НПА – нормативно-правовой акт

СНГ – Содружество независимых государств

ШОС – Шанхайская организация сотрудничества

CERT – Cyber Emergency Response Team (Компьютерная группа реагирования на чрезвычайные ситуации)

CIGR – Critical Infrastructure at Greatest Risk (критические инфраструктуры, подверженные наибольшим рискам)

COBIT – Control Objectives for Information and Related Technologies

CSIRT – Computer Security Incident Response Team (Команда компьютерной безопасности по реагированию на инциденты)

DNS – Domain Name System (Глобальная система доменных имен)

IANA – Internet Assigned Numbers Authority (Администрация адресного пространства интернет)

ICS-CERT – Industrial Control Systems Cyber Emergency Response Team (Компьютерная группа реагирования на чрезвычайные ситуации в системах управления производственными процессами)

NCCIC – National Cybersecurity and Communications Integration Center (Национальный центр по интеграции кибербезопасности и коммуникаций)

NIPP – National Infrastructure Protection Plan (Национальный план по защите инфраструктуры)

NTIA – National Telecommunications and Information Administration (Национальная администрация по телекоммуникациям и информации)

PPD 20 – Presidential Policy Directive 20 (директива президента США «О политике США в области кибероперацій»)

R&D – Research & Development (научно-исследовательские и опытно-конструкторские работы)

US-CERT – United States Computer Emergency Readiness Team (Компьютерная группа реагирования на чрезвычайные ситуации США)

ОБ АВТОРАХ

ДЕМИДОВ ОЛЕГ ВИКТОРОВИЧ
Консультант ПИР-Центра, специалист по вопросам кибербезопасности и цифровой трансформации. С апреля 2018 года – руководитель Центра анализа и прогнозирования Фонда поддержки предпринимательства Республики Татарстан. В 2013-2014 годах руководил программой ПИР-Центра «Глобальное управление интернетом и международная информационная безопасность». Окончил факультет государственного управления МГУ им. М.В. Ломоносова. С 2012 года – эксперт Комиссии по информационной безопасности и киберпреступности Российской ассоциации электронных коммуникаций (РАЭК). Участник Рабочей группы по кибербезопасности АТССБ в 2011 году, участник международного проекта «Новый концерт держав в XXI веке» Франкфуртского института по изучению проблем мира и конфликтов (PRIF) (2011-2014). Автор монографии «Глобальное управление интернетом и безопасность в сфере использования ИКТ. Ключевые вызовы для мирового сообщества» (2015) и статей по вопросам информационной безопасности, глобального управления интернетом.

АНГМАР МАРГАРИТА АНДРЕЕВНА
В 2018 году окончила магистратуру Московского педагогического государственного университета «Политические исследования России и постсоветского пространства: Russian Studies». Тема магистерской диссертации «Стратегия кибербезопасности и Организация договора о коллективной безопасности». В августе–ноябре 2017 года – стажер ПИР-Центра. Работала в экспертной группе «Первый советникъ» и Ассоциации юристов России.

ИНДЕКС БЕЗОПАСНОСТИ

Серия докладов, аналитических статей, комментариев, интервью и других материалов, отражающих позиции российских и зарубежных экспертов по актуальным вызовам глобальной безопасности и политики России в этой сфере. Задача серии – дать понятный анализ проблем международной безопасности и предложить конкретные, реалистичные идеи и решения. Издается ООО «Триалог» в сотрудничестве с ПИР-Центром и другими партнерами.

ТРИАЛОГ

Российская компания, занимающаяся научными исследованиями, издательской, информационной и образовательной деятельностью, организацией научных мероприятий в сфере международной безопасности. Организатор Международного клуба *Триалог* – созданного в 1993 г. места регулярных встреч российских и зарубежных дипломатов, политиков, ученых, представителей бизнес-сообщества для обсуждения ключевых вопросов мировой повестки дня и внешней политики. Многолетний партнер ПИР-Центра.

ПИР-ЦЕНТР

ПИР-Центр, основанный в 1994 г., является ведущей в России неправительственной организацией, специализирующейся на изучении вопросов глобальной безопасности.

С начала 2000-х гг. эксперты ПИР-Центра ведут исследования в сфере информационной безопасности. В 2001 г. вышла книга «Информационные вызовы национальной и международной безопасности», первое издание по данной теме в России. В 2011 г. создана программа ПИР-Центра «Глобальное управление Интернетом и международная информационная безопасность». В 2015 – 2017 г. в рамках взаимодействия с Всемирным экономическим форумом была подготовлена серия докладов об информационной безопасности критической инфраструктуры гражданских ядерных объектов. В 2016 г. вышла монография О.В. Демидова «Глобальное управление Интернетом и безопасность в сфере использования ИКТ. Ключевые вызовы для мирового сообщества», а в 2017 г. в сотрудничестве с Центром стратегических разработок (ЦСР) подготовлен доклад «Будущее информационной безопасности: глобальные трансформации и сценарии для России».

В исследовании вопросов управления Интернетом и влияния ИКТ на глобальную безопасность ПИР-Центр сотрудничает с российскими государственными органами, частным сектором, отечественным и глобальным техническим сообществом, а также международными организациями, включая структуры ООН (ЭКОСОС, ЮНИДИР, МСЭ). Эксперты ПИР-Центра участвуют в крупнейших российских международных встречах и форумах по вопросам международной информационной безопасности и кибербезопасности, вносят вклад в развитие глобальных и региональных подходов к решению ключевых проблем в этой сфере.

Серия «Индекс Безопасности»

Демидов Олег Викторович
Ангмар Маргарита Андреевна

Киберстратегия США 2018. Значение для глобального диалога о поведении в сфере использования ИКТ и российско-американских отношений

Корректор
Е.Р. Хубларова

Дизайн и компьютерная верстка
Т.В. Рогович

В оформлении доклада используется фрагмент гравюры Альбрехта Дюрера «Носорог»

Адрес
Россия, 119019, Москва, а/я 137
secretary@trialogue-club.ru

Тираж
Подписано в печать 24.01.2019 г.
Печать: ООО «ЦПУ «Радуга»
Отпечатано по заказу ООО «Триалог»


Триалог


ПИР-ЦЕНТР