ИНСТИТУТ
ИССЛЕДОВАНИЙ
ИНТЕРНЕТА

АНАЛИЗ ДОКУМЕНТОВ СТРАТЕГИЧЕСКОГО ПЛАНИРОВАНИЯ СОЕДИНЕННЫХ ШТАТОВ АМЕРИКИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Москва, 2019

Содержание

О Национальной Киберстратегии
Соединенных Штатов Америки

I.

В исторической ретроспективе нельзя не сказать о том, что в мае 2011 года США представили документ «Международная стратегия США в отношении киберпространства. Процветание, безопасность и открытость сетевого мира» (*International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World*)[1]. Названный документ (далее – «Международная Стратегия киберпространства США»), по-видимому, можно рассматривать как первый политико-стратегический документ в котором, во-первых, киберпространство было обозначено как самостоятельная предметная сфера регулирования, требующая международного сотрудничества, во-вторых, предложен комплексный подход регулирования по широкому спектру вопросов, относящихся к сфере киберпространства.

Принятие Международной Стратегии киберпространства США во многом было обусловлено тем, что Правительство США неоднократно выражало озабоченность по поводу политических и технологических вызовов, сопровождающих функционирование, а также перспективы развития сетевых технологий и интернета, как их центрального звена. При оценке Международной Стратегии киберпространства США с позиций 2019 года важно учитывать временно*й* фактор ее принятия, т.е. внутри-национальную политико-экономическую ситуацию в США, международно-правовой, геополитический и т.п. контексты, существовавшие в 2011 году, которые по сути определили содержательный формат документа.

В настоящее время, несмотря на прошедшие восемь лет, Международная Стратегия киберпространства США сохраняет свое значение, т.к. киберпространство продолжает позиционироваться Правительством США как критически важный объект, требующий сохранения его природы (т.е. как открытого, функционально совместимого (интероперабельного), безопасного пространства), а также совместных усилий всех заинтересованных сторон (государств, технического, гражданского, научного сообщества и т.д.) по снижения возникающих угроз и вызовов безопасного использования киберпространства.

[1] *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World*. – URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

В Международной Стратегии киберпространства США определены *семь взаимосвязанных стратегических направлений,* по каждому из которых Правительство США намеревается сотрудничать на международном, региональном и национальном уровне с частными и государственными структурами. Все направления призваны создать синергетический эффект вектора действий Правительства США в сфере киберпространства, и таковыми являются следующие.

1. *Экономика: укрепление международных стандартов и инноваций, открытые рынки.* Глобальный охват интернета во многом отражается в распространении более дешевых и повсеместно доступных компьютеров и сетевых технологий. Конкуренция на этих рынках стимулирует инновации, а среда свободной торговли дает производителям возможность поддерживать конкурентные цены и высокие стандарты. Уважительное отношение к международным стандартам разработки технологий и торговли представляет собой существенную часть поддержания открытых рынков и позволяет компаниям, занимающимся высокими технологиями, быстро доводить до потребителя преимущества своих инновационных продуктов и услуг. В течение нескольких будущих десятилетий глобализация разработки технологий будет только нарастать, принося ощутимые выгоды для сетей и потребителей.

Реализация экономического направления охватывает решение следующих задач: поддержка пространства свободной торговли, поощряющее технологические инновации через доступные, глобально связанные сети; защита интеллектуальной собственности, в том числе коммерческие секреты производства, от незаконного использования; обеспечение приоритета функционально совместимых и безопасных технических стандартов, вырабатываемых техническими экспертами.

2. *«Защита наших сетей: усиление безопасности, надежности и отказоустойчивости».* США считают стратегическим направлением усилия по достижению регионального и международного консенсуса по ключевым видам деятельности, связанным с киберпространством, в том числе по вопросу правил киберпространства. Правительство США намерено способствовать сотрудничеству по вопросам киберпространства, в частности, в области норм поведения государств и кибербезопасности на двустороннем уровне и в рамках многосторонних организаций и многостороннего сотрудничества, например, Организации американских государств (*OAS*), Регионального форума Ассоциации государств Юго-Восточной Азии (*ASEAN*), Организации Тихоокеанского экономического сотрудничества (*APEC*), Организации по безопасности и сотрудничеству в Европе (OSCE), Африканского союза (*AU*), Организации

экономического сотрудничества и развития (*OECD*), «Большой восьмерки» (*G-8*), Европейского союза, ООН и Совета Европы.

Во взаимосвязанной глобальной среде низкий уровень безопасности систем одной страны создает риск для других. Правительство США принимает обязательства делиться уникальной информацией о своих сетях и сотрудничать с другими странами в ситуациях, когда те или иные события могут угрожать всем. Кроме того, США будут прилагать усилия по международному участию в учениях, посвященных безопасности в киберпространстве, по повышению качества и усилению существующих оперативных процедур вместе с партнерами. Правительство США обеспечит принятие необходимых мер по управлению инцидентами, отказоустойчивость, а также жизнеспособность информационной инфраструктуры, и будет бороться за уменьшение числа вторжений в сети США и срывов их работы. совершенствовать безопасность высокотехнологичной цепочки поставок по согласованию с бизнес сообществом.

3. *«Правопорядок: расширение сотрудничества и правовое регулирование».* Для укрепления доверия в киберпространстве и преследования тех, кто хотел бы осуществить компьютерное вторжение в сетевые устройства, Правительство США предполагает принимать полноценное участие в развитии международной политики по вопросам киберпреступности. США обязуются активно участвовать в обсуждениях по вопросам выработки международных норм и мер по противодействию киберпреступности на двустороннем и многостороннем уровне, на форумах, доказавших свою компетентность и имеющих достижения в плане продвижения эффективных принципов борьбы с такой преступностью. Обсуждения подобного рода будут включать сложившиеся механизмы, например, по расширению области влияния таких инструментов, как Будапештская конвенция по киберпреступлениям. [2] Правительство США стремится гармонизировать на международном уровне правовые нормы в сфере киберпреступности, расширяя круг участников, присоединившихся к Будапештской конвенции по киберпреступлениям.

США зачастую оказываются поставленными в зависимость от сотрудничества с другими странами и их содействия при расследовании киберпреступлений и привлечении нарушителей к ответственности. Такое сотрудничество наиболее эффективно и полноценно, когда страны имеют схожие правовые нормы о преступлениях в киберпространстве, что облегчает получение доказательств, экстрадицию и другие формы координации действий. Будапештская конвенция по борьбе с киберпреступностью дает странам модель для выработки проектов таких правовых норм и совершенствования своего законодательства, и доказала свою эффективность в качестве механизма

[2] См. Консультант плюс. ИБ Версия Проф. И.Б. Международное право

углубления международного сотрудничества при расследовании киберпреступлений. США продолжат поддерживать другие страны в вопросе присоединения к Конвенции и оказывать содействие не присоединившимся странам применять Конвенцию в качестве основы для разработки собственных правовых норм; в краткосрочной перспективе это позволит облегчить двустороннее сотрудничество, а в долгосрочной – подготовит такие страны к присоединению к Конвенции.

Действия преступников в киберпространстве должны встречать эффективное обеспечение правопорядка, а не на политику ограничения законного доступа к интернету или контенту интернета. Для достижения этой цели Правительство США работает на двусторонней и многосторонней основе для обеспечения понимания другими странами того, что акцент в борьбе против онлайн-преступлений должен быть сделан на предупреждении таких деяний, задержании и наказании нарушителей, а не на общем ограничении доступа к интернету, поскольку широкое ограничение доступа может затронуть и добросовестных пользователей. США, совместно со своими партнерами намерены защитить неприкосновенность частной жизни, основных свобод и инноваций в сфере борьбы с преступлениями в киберпространстве. Правительство США делает упор в правовых нормах по вопросам киберпреступности на противодействии противоправной деятельности, а не на ограничении доступа к Интернету и стремиться лишить террористов и прочих преступников возможности использовать интернет для планирования операций, их финансирования или проведения кибератак.

США стремятся реализовывать разнообразные международные программы по наращиванию потенциала и обучению по вопросам борьбы с киберпреступностью, которые содействуют законодательным и правоохранительным органам в разработке и применении эффективных правовых конструкций, накоплении знаний и опыта в данной сфере деятельности для расследования и преследования лиц, использующих Интернет для террористических или иных преступных целей. Лишение террористов возможностей (тем более их расширения) действовать с помощью хакеров и мафиозных средств является важным приоритетом для международного сообщества, требует эффективного законодательства по вопросам киберпреступности. США исполнены решимости выявлять и пресекать работу сетей финансирования террористов и киберпреступников, используя для этого технический инструментарий и структуры международного сотрудничества, такие как Международная группа по разработке финансовых мер борьбы с отмыванием денег (*FATF*).

4. *«Военная сила: подготовка к вызовам безопасности XXI-ого века».* Это направление предполагает осуществление следующих задач: учитывать растущие

потребности военных в надежных и безопасных сетях, и адаптироваться к этим потребностям; создавать и совершенствовать существующие военные союзы для противостояния возможным угрозам в киберпространстве; расширять сотрудничество с союзниками и партнерами в киберпространстве в целях повышения коллективной безопасности.

5. *«Управление использованием интернета: содействие эффективным и всеобъемлющим структурам»*. Возможность оперативного распространения информации в Интернете является ключевым моментом современной экономической, политической, научной и образовательной деятельности, а также активности пользователей. Правительства в глобальном масштабе признают ценность Интернета; вместе с тем многие из них накладывают произвольные ограничения на свободу распространения информации или используют подобные меры для подавления деятельности инакомыслящих или оппозиции. В различных странах применяются самые разные методы и формы реализации таких ограничений, равно как и обоснования для применения подобных мер, но мы не должны допустить такую перестройку управления использованием интернета или технической архитектуры интернета, при которой возможно было бы осуществлять действия, нарушающие основные свободы или неоправданно сдерживающие инновации. Эффективное и всестороннее управление использованием интернета может помочь в обеспечении того, чтобы действия, грубо нарушающие международные нормы допустимого управления сетями, не облегчались технической структурой или структурой управления. Сохранение, облегчение и расширение доступа к открытому глобальному интернету являются отчетливым политическим приоритетом. США продолжат уделять первостепенное внимание открытости и инновациям в интернете.

Для управление использованием интернета необходимо сохранять безопасность и стабильность глобальной сети, включающую систему доменных имен (*Domain Name System, DNS*). Учитывая важность интернета для мировой экономики, представляется существенным, чтобы эта «Сеть сетей» и лежащая в ее основе инфраструктура (*DNS*) оставались стабильными и безопасными. Необходимо поддерживать площадки для расширенного состава заинтересованных сторон, обсуждающих вопросы управления использования интернетом и содействовать работе таких площадок.

Сама архитектура интернета олицетворяет собой модель социальной и технической организации – децентрализованной, скоординированной и многоуровневой. Каждая из этих характеристик фундаментальна с точки зрения преимуществ и выгод интернета. Такая архитектура питает свободу инноваций, содействует экономическому росту. Она

поддерживает свободу слова и объединений, что способствует социальному и политическому развитию и функционированию демократических обществ по всему миру. США твердо отстаивают свою убежденность в том, что когда международное сообщество встречается для обсуждения целого спектра вопросов, связанных с управлением использования интернетом, то такие встречи должны проводиться с привлечением всех заинтересованных сторон. Правительство США в дальнейшем намерено оказывать поддержку эффективным площадкам, подобным Форуму по управлению использования интернета (*IGF*)[3], который отражает открытую и всестороннюю природу самого интернета, давая возможность участникам, не представляющим государства, участвовать в обсуждении наряду с представителями государств и на равноправной основе.

6. *«Международное сотрудничество: потенциал, безопасность и процветание»*. Для глобального укрепления сетевых технологий, повышения надежности сетей общего пользования и формирования сообщества ответственных участников в киберпространстве. Правительство США стремится обеспечивать страны, желающие создать технический потенциал и потенциал в сфере кибербезопасности, необходимыми знаниями, обучением и прочими ресурсами; непрерывно совершенствовать и развивать практические подходы в сфере международной кибербезопасности и регулярно делиться такими наработками; укреплять способность государств к борьбе с киберпреступностью, в том числе путем обучения правоохранительных органов, судейских кадров, юристов и законодателей; принимать решения с целью наращивания технического потенциала, обеспечивая постоянные и продолжительные контакты с экспертами и их партнерами из Правительства США.

7. *«Свобода интернета: защита основных свобод и частной жизни».* Реализация этого стратегического направления связана с поддержкой представителей гражданского общества в создании надежных и безопасных площадок для свободы слова и объединений. В Стратегии безопасности отмечается, что люди по всему миру могут использовать цифровые средства для выражения мнений, обмена информацией, наблюдения за выборами, разоблачения коррупции, организации социальных и политических движений. Правительство США намерено сотрудничать с гражданским обществом и неправительственными организациями в установлении мер безопасности их деятельности в Интернете от незаконных цифровых вторжений; поощрять международное сотрудничество для действенной защиты коммерческих конфиденциальных данных. Защита неприкосновенности частной жизни имеет существенное значение с точки зрения

[3] The Internet Governance Forum - орган, который функционирует на основании мандата ООН и действует под эгидой ООН. См. http://www.intgovforum.org. http://www.intgovforum.org

доверия, на котором базируется использование Интернета для экономических и социальных целей.

Пользователи должны быть уверенны в том, что информация, которую они передают в интернете, будет получена в том виде, в каком она была отправлена, причем в любой точке мира. Столь же важным является то, что в нормальных условиях информация будет распространяться через границы вне зависимости от места отправления или места назначения. Обеспечение целостности информации, передаваемой по интернету, должно вызывать у пользователей доверие к Сети и сохраняет Сеть в качестве открытой площадки для инноваций, питающей рост мировой экономики и стимулирующей обмен идеями между людьми всего мира. Соединенные Штаты стремятся обеспечить сквозную совместимость для всеобщей доступности интернета.

Семь пунктов Международной Стратегии киберпространства США – это не конкретные инструкции, но, скорее широкие принципы, обрисовывающие приоритеты Правительства США в сфере киберпространства.

II.

При новой Администрации США был принят документ – Национальная Киберстратегия Соединенных Штатов Америки (*National Cyber Strategy of the United States of America*). Названный документ, принятый в сентябре 2018 г.[4] (далее – «Киберстратегия США») основывается, во-первых, на Стратегии Национальной Безопасности США (*National Security Strategy of the United States of America*), которая была принята после 11 месяцев начала работы нынешней Администрации Президента США, т.е. в декабре 2017 г.[5], во-вторых, на Административном распоряжении Президента США (*Executive Order, EO*) 13800 «Об усилении кибербезопасности Федеральных сетей и критической инфраструктуры» (*Executive Order,* «*Strengthening of Federal Networks and Critical Infrastructure*»)[6].

Несмотря на то, что Киберстратегия США формально не ссылается на рассмотренную ранее принятую Стратегию киберпространства США, в предметном и содержательном плане ключевые подходы и термины (кибербезопасность, процветание,

[4] *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

[5] *National Cyber Strategy of the United States of America* (December 2017). – URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[6] President Executive Order 13800 «*Strengthening of Federal Networks and Critical Infrastructure* – URL: https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure
Executive Order – Административное распоряжение Президента США является нормативно-правовым актом

безопасность, открытость) – остаются неизменными, также, как и неизменным остается и приверженность к стратегическим целям и задачам, которые сопрягаются с функционированием и использованием киберпространства. Сопоставительная таблица, которая завершает настоящее заключение, как представляется, наглядно подтверждает высказанный тезис.

Киберстратегия США предваряет обращение Президента США и в ней определены следующие ключевые направления укрепления потенциала кибербезопасности, а также обеспечения защиты США от киберугроз: защита США посредством сохранения сетей, систем, функциональных элементов и данных; содействие американскому благоденствию посредством содействия безопасной, процветающей цифровой экономики и стимулирования сильных внутренних инноваций; сохранение мира и безопасности посредством укрепления способности США сдерживать и, в случае необходимости, принимать меры воздействия на тех, кто использует кибер-инструменты в злонамеренных целях, при этом такие способности осуществляются во взаимодействии с союзниками и партнерами; усиление американского влияния за рубежом с тем, чтобы расширить основополагающие принципы открытого, функционально совместимого, интероперабельного, надежного и безопасного интернета.

Киберстратегия США структурно коррелирует со Стратегией Национальной Безопасности США 2017 г., о чем свидетельствует рубрикация обоих документов и названия разделов. Киберстратегия США и Стратегии Национальной Безопасности США 2017 г. структурно содержат 4 исходные опоры или основополагающие элементы (см. Таблицу 2), которые сформулированы таким же образом, как и в Стратегии Национальной Безопасности США 2017 года. При этом, в отличие от соответствующих основополагающих элементов Стратегии Национальной Безопасности США, в каждом из 4 основополагающих элементов Киберстратегии США сформулирована конкретная цель, а также соответствующие приоритетные действия.

Во Введении в Киберстратегию США дважды упоминается Россия, однако, такое упоминание осуществлено в контексте таких стран как Китай, Иран и Северная Корея. При этом Китай также дважды упомянут в разделе Введение, при этом один раз в контексте обозначенных стран (Россия, Иран и Северная Корея) и один раз *отдельно* от этих стран, как страна, которая занималась «кибер-поддержкой экономического шпионажа и кражей триллион-долларовой интеллектуальной собственности».

Целесообразно в общем плане обозначить 4 основополагающих элемента Киберстратегии США, цели, а также содержательные разделы, определяющие приоритетные действия.

Основополагающий элемент I: *Защитить американский народ, Отечество и американский образ жизни* формулирует ключевую цель: управлять рисками кибербезопасности для повышения защиты и устойчивости информации граждан США и информационных систем. Этот основополагающий элемент охватывает три раздела.

Раздел первый – обеспечение безопасности Федеральных сетей и информации предполагает приоритетные действия: дальнейшую централизацию управления и надзора за Федеральной гражданской безопасностью; согласование управления рисками и деятельностью в сфере информационных технологий; совершенствование управления рисками Федеральной системы логистических цепочек; усиление кибербезопасности Федеральных подрядчиков; обеспечение лидирующих позиций Правительства по лучшим инновационным практикам.

Раздел второй – защита критической инфраструктуры, охватывает следующие приоритетные действия: совершенствование распределения функций и сфер ответственности; определение приоритетов действий в зависимости от характера идентифицированных национальных рисков; привлечение провайдеров информационно-коммуникационных технологий, как посредников кибербезопасности; защиту американской демократии; создание благоприятных условий для инвестиций в кибербезопасность; определение приоритетов национальных исследований и содействие развитию инвестиций; улучшение транспортной, морской и космической кибербезопасности.

Раздел третий – борьба с киберпреступностью и улучшение отчётности об инцидентах предусматривает такие приоритетные действия: меры по улучшению отчетности и реагирования на инциденты; повышение эффективности электронного надзора, а также совершенствование права о компьютерных преступлениях; снижение угроз от транснациональных преступных организаций в киберпространстве; упрощение задержания преступников, находящихся за рубежом; укрепление потенциала правоохранительных органов стран-партнеров в борьбе с киберпреступностью.

Основополагающий элемент II: *Содействие американскому процветанию* определяет в качестве ключевой цели: сохранение влияния США в технологической экосистеме, а также развитие киберпространства в качестве открытого двигателя экономического роста, инноваций и эффективности. В этот основополагающий элемент включены три раздела.

Раздел первый – содействие развитию жизнеспособной и устойчивой цифровой экономики, направлен на такие приоритетные действия как: стимулирование гибкой и защищенной технологической торговли; определения приоритета инноваций;

инвестирование в инфраструктуру следующего поколения; содействие свободному трансграничному потоку данных; поддержания лидерства США в передовых технологиях; содействие полному жизненному циклу кибербезопасности.

Раздел второй – поощрение и обеспечение инновационности США предполагает, что приоритетные действия – это: обновление механизмов обзора иностранных инвестиций и деятельности в США; поддержание сильной и сбалансированной системы защиты интеллектуальной собственности; защиту конфиденциальности и целостности американских идей.

Раздел третий – создание высококлассного кадрового штата сотрудников кибербезопасности подразумевает следующие приоритетные действия: создание и поддержание кадрового резерва; расширение возможности для переподготовки и образования для американских служащих и рабочих; увеличение кадрового персонала кибербезопасности Федерального уровня; использование исполнительных органов для выявления и поощрения талантливых кадров.

Основополагающий элемент III: *Сохранение мира посредством силы,*

в качестве ключевой цели формулирует: выявление, противодействие, пресечение, ослабление интенсивности, а также сдерживание действий в киберпространстве, которые дестабилизирует и противоречат национальным интересам США, с сохранением превосходства США в киберпространстве и посредством киберпространства. Данный основополагающий элемент охватывает два раздела.

Раздел первый – повышение кибер-стабильности посредством норм ответственного поведения государств в качестве приоритетных действий предполагает поощрение всеобщей приверженности к нормам, действующим в киберпространстве.

Раздел второй – обнаружение и сдерживание неприемлемого поведения в киберпространстве, направлен на необходимость таких приоритетных действий как: руководство заявленными целями, а также взаимодействие с разведывательными органами; введение соответствующих мер воздействия за негативные последствия в киберпространстве; создание кибер-сдерживающих инициатив; противодействие вредоносному кибер-влиянию и информационным операциям.

Основополагающий элемент IV: *Усиление американского влияния,* как ключевую цель формулирует: сохранение долгосрочной открытости, функциональной совместимости, безопасности и надежность интернета, который поддерживается и усиливается интересами США. Этот основополагающий элемент включает два раздела.

Раздел первый – содействие открытому, функционально совместимому надежному и безопасному интернету, в качестве приоритетных действий определяет: защиту и

содействие свободе интернета; сотрудничество со странами-единомышленниками, промышленностью, академическим и гражданским сообществом; содействие многосторонней модели управления использования интернета; содействие многосторонней функциональной совместной надежной коммуникационной инфраструктуре и подключения к интернету; поддержание рынков в отношении инновационности США по всему миру.

Раздел первый – создание международного кибер-потенциала, связывается с приоритетными действиями, направленными на улучшение кибер-мобилизующих мер.

В связи с тем, что в настоящем заключении представлен перевод на русский язык всего текста документа Киберстратегии США, выделим лишь один фрагмент, который представляется важным в контексте текущей ситуации в России.

В настоящее время, когда выбор стратегического вектора социально-экономического развития современных государств ориентирован на цифровую экономику, и Россия не является в этом плане исключением[7], усиливается конфликт между, с одной стороны, персональными данными/данными личного характера, приобретающими все бо́льшую экономическую значимость и коммерческую ценность и, с другой стороны, их защитой и обеспечением конфиденциальности. Несомненно, средства, методы разрешения этого конфликта, а также меры правовой защиты и т.д. будут претерпевать радикальные изменения и варьироваться в зависимости от специфики национальных правопорядков государств.

В этом плане нельзя не обратить внимание на тот подход, который закреплен в Киберстратегии США. Во-первых, содействие развитию жизнеспособной и устойчивой цифровой экономике выделено в самостоятельный раздел. Во-вторых, в разделе отмечается, что «ограничительные положения о локализации данных» нередко используется в качестве оправдания для цифрового протекционизма, подводятся под категорию национальной безопасности.

Таблица 1

«Международная Стратегия США в отношении киберпространства» 2011 г. **Стратегические направления**	«Национальная Киберстратегия США» 2018 г. ***Основополагающие элементы и Цели***

[7] См. Распоряжение Правительства РФ от 28.07.2017 № 1632-р
«Об утверждении программы «Цифровая экономика Российской Федерации». СПС Консультант

1. Экономика: укрепление международных стандартов и инноваций, открытые рынки.	
2. Защита наших сетей: усиление безопасности, надежности и отказоустойчивости	**Основополагающий элемент I:** ***Защитить американский народ, Отечество и американский образ жизни.*** **ЦЕЛЬ:** Управлять рисками кибербезопасности для повышения защиты и устойчивости информации граждан США и информационных систем. **Разделы:** Обеспечивать безопасность Федеральных сетей и информации; Защищать Критическую Инфраструктуру; Бороться с киберпреступностью и улучшать отчётность об инцидентах
3. Правопорядок: расширение сотрудничества и правовое регулирование	**Основополагающий элемент II:** ***Содействовать американскому процветанию*** **ЦЕЛЬ:** Сохранить влияние США в технологической экосистеме и развивать киберпространство как открытого двигателя экономического роста, инноваций и эффективности. **Разделы:** Способствовать развитию жизнеспособной и устойчивой Цифровой экономике; Поощрять и обеспечивать инновационность США; Создавать высококлассный штат сотрудников кибербезопасности
4. Военная сила: подготовка к вызовам безопасности XXI-ого века	**Основополагающий элемент III:** ***Сохранить мир посредством силы*** **ЦЕЛЬ:** Выявлять, противодействовать, пресекать, ослаблять интенсивность и сдерживать действия в киберпространстве, которые дестабилизирует и противоречат национальным интересам, сохраняя при этом превосходство США в киберпространстве и посредством него. **Разделы:** Повышать кибер-стабильность посредством норм ответственного поведения государств; обнаружение и сдерживание неприемлемого поведения в киберпространстве.
5. Управление использованием интернета: содействие эффективным и всеобъемлющим структурам	**Основополагающий элемент IV:** ***Усилить американское влияние*** **ЦЕЛЬ:** Сохранять долгосрочную

	открытость, функциональную совместимость, безопасность и надежность интернета, который поддерживается и усиливается интересами США. **Разделы:** Способствовать открытому, функционально совместимому надежному и безопасному интернету; Создавать международный кибер-потенциал
6. Международное сотрудничество: потенциал, безопасность и процветание	
7. Свобода интернета: защита основных свобод и частной жизни	

Таблица 2

«Стратегии Национальной Безопасности США» 2017 г. **Основополагающие элементы**	«Национальная Киберстратегия» 2018 г. ***Основополагающие элементы и Цели***
Основополагающий элемент I: Защитить американский народ, Отечество и американский образа жизни	**Основополагающий элемент I:** ***Защитить американский народ, Отечество и американский образ жизни***
Основополагающий элемент II: Содействовать американскому процветанию	**Основополагающий элемент II:** ***Содействовать американскому процветанию***
Основополагающий элемент III: Сохранить мир посредством силы	**Основополагающий элемент III:** ***Сохранить мир посредством силы***
Основополагающий элемент IV: Усилить американское влияние	**Основополагающий элемент IV:** ***Усилить американское влияние***

Приложение 1.

Международная стратегия в отношении киберпространства

2011 года

МЕЖДУНАРОДНАЯ СТРАТЕГИЯ В ОТНОШЕНИИ КИБЕРПРОСТРАНСТВА[8]

Процветание, безопасность и открытость сетевого мира

Май 2011 года

Белый дом

Вашингтон

Киберпространство и реализующие его технологии позволяют людям всех национальностей, рас, религий и убеждений общаться между собой, сотрудничать и преуспевать, как никогда раньше. Сегодня любая американская компания может вести бизнес в любой точке мира благодаря подключению к Интернету, что обеспечивает бесчисленное число рабочих мест и открывает бесчисленные возможности для американцев. Женщина-мать где-нибудь в сельской глубинке Африки может продавать свои изделия семье в Латинской Америке, внося свой вклад в расширение экономического развития. Лаборатория в Европе может выполнять текущие исследования на

8 http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf\

оборудовании, изготовленном в Азии, с использованием программного обеспечения, написанного в Северной Америке, а студенты в Австралии и на Ближнем Востоке могут учиться вместе посредством видеоконференций. И, как никогда прежде, благодаря информационным технологиям граждане по всему земному шару получают дополнительные возможности в том, чтобы сделать правительства более открытыми и отзывчивыми.

Сегодня, когда страны и народы овладевают преимуществами окружающих нас сетей, у нас появляется выбор. Мы можем либо работать сообща для реализации потенциала этих сетей с целью продвижения к дальнейшему процветанию и безопасности, либо проявить узость интересов и поддаться неуместным страхам, ограничивая движение по пути прогресса. Кибербезопасность важна не сама по себе; это, по сути дела, обязательство, которое наши правительства и общества должны добровольно взять на себя для того, чтобы инновации развивались, стимулировали рынки и улучшали нашу жизнь. В условиях, когда преступность и агрессия, существовавшие вне Сети, проникли в цифровой мир, мы будем последовательно противостоять этому, базируясь на принципах, воспринимаемых нами как фундаментальные: на свободе слова и объединений, на неприкосновенности частной жизни, на свободе информационных потоков.

Цифровой мир более не является «территорией вне закона», как не является он и уголком для немногочисленной элиты. Это сфера, все глубже и глубже пронизываемая нормами ответственного, обоснованного и миролюбивого поведения государств и народов. Это один из наиболее впечатляющих примеров самоорганизующегося сообщества, когда гражданское общество, научное сообщество, частный сектор и правительства работают сообща над эффективным управлением цифрового мира. Самое важное заключается в том, что этот мир продолжает расти, развиваться и нести с собой процветание, безопасность и открытость – то есть то, что было присуще ему с момента изобретения. Это то, что выделяет Интернет из общей международной среды, и именно поэтому так важно обеспечить его защиту.

В этом контексте я предлагаю настоящую Международную стратегию США в отношении киберпространства. Уже не в первый раз моя администрация высказывает озабоченность по поводу политических вызовов, сопровождающих сетевые технологии, но впервые наша страна предложила комплексный подход к нашему сотрудничеству с международными партнерами по всему спектру вопросов, относящихся к сфере киберпространства. И в этой связи данная стратегия не просто очерчивает некоторое видение будущего киберпространства – это своего рода план реализации. Она предлагает контекст будущих усилий нашим партнерам как в стране, так и за рубежом для уяснения

наших приоритетов и намечает совместные подходы к сохранению природы киберпространства и снижению возникающих угроз.

Сам по себе, Интернет не возвещает новую эру международного сотрудничества. Над этим еще предстоит поработать нам – бенефициарам Сети. Сообща мы сможем работать над формированием будущего киберпространства – открытого, универсально совместимого, безопасного и надежного. Это то будущее, к которому мы стремимся, и мы призываем все страны и народы присоединиться к нашим усилиям.

I. Формирование политики в сфере киберпространства

«Этот мир – мир киберпространства – является тем миром, от которого зависит наша повседневная жизнь ... [Он] создает для нас возможности большей взаимосвязи, чем когда-либо прежде в истории человечества.»

Президент Барак Обама, 29 мая 2009 года

Цифровая инфраструктура во все большей степени становится главной опорой процветающих экономик, энергичных научных сообществ, мощных венных держав, исповедующих принципы прозрачности правительств и свободных обществ. Как никогда прежде, информационные технологии благоприятствуют транснациональному диалогу и облегчают глобальные потоки товаров и услуг. Такие социальные и торговые связи становятся совершенно необходимыми для нашей повседневной жизни. Особо важные инфраструктурные системы, обеспечивающие нас электричеством и водой, контролирующие движение воздушных судов, поддерживающие нашу финансовую систему – все они зависят от объединенных в сети информационных систем. В настоящее время страны стремятся рационализировать оказание основных услуг средствами так называемого «электронного правительства». Социальные и политические движения строят свою работу на основе Интернета как способа достижения новых, более широких организационных форм и акций. Охват сетевых технологий поистине впечатляющ и глобален. Для всех стран мира базовая цифровая инфраструктура является или станет в скором будущем национальным активом.

Для полномасштабной реализации тех преимуществ и выгод, которые сетевые технологии способны дать миру, такие системы должны работать надежно и безопасно. У людей должна быть уверенность в том, что информация будет доставляться адресату безошибочно и без срывов. Обеспечение свободных информационных потоков, безопасности и конфиденциальности информации, надежной работы связанных между собой сетей имеет жизненно важное значение для процветания экономики США и всего мира, безопасности и укрепления всеобщих прав.

Почти треть населения мира пользуется Интернетом, и гораздо больше людей так или иначе затрагиваются Всемирной сетью в повседневной жизни. Сегодня в мире насчитывается свыше четырех миллиардов цифровых беспроводных устройств. Каких-то пятьдесят лет назад это число равнялось нулю. Мы переживаем тот редкий исторический момент, когда имеется реальная возможность обеспечить, на фундаменте успехов киберпространства, его безопасное будущее для граждан США и всего мирового сообщества.

Для того, чтобы эти технологии продолжали открывать новые возможности людям, улучшать общество, содействовать научным исследованиям, развитию и инновациям, столь важным для формирования современных экономик, Интернет должен сохранить открытость и функциональную совместимость, которые до сих пор неизменно сопровождали его взрывное развитие. В основе этого лежат технические принципы и эффективные структуры управления, требующие нашей поддержки. В то же время наши сети должны быть надежными и безопасными; они должны сохранять доверие к себе со стороны граждан, бизнеса и правительств, демонстрируя устойчивость к случайным или злоумышленным нарушениям в работе.

Миру надлежит сообща осознать угрозы, связанные с вмешательством злоумышленников в киберпространство, и соответствующим образом модернизировать и укрепить национальные и международные принципы в этой сфере. Действия в Интернет-пространстве находят отражение для нашей жизни в обычном, физическом мире, и мы должны работать над укреплением верховенства закона, над устранением того, чтобы риски перевешивали преимущества Сети. Будущее открытого, функционально совместимого, безопасного и надежного киберпространства зависит от того, насколько страны осознают и сумеют защитить то наиболее важное, что должно быть сохранено, и насколько эффективно они будут противодействовать тем, кто хотел бы дестабилизировать или подорвать наш мир, все более тесно объединяемый Сетью.

Стратегический подход

Подход Соединённых Штатов к принципам международного киберпространства основывается на убеждении, что сетевые технологии обладают огромным потенциалом для страны и мира. На протяжении последних трех десятилетий мы, Соединенные Штаты Америки, наблюдали за тем, как эти технологии революционизируют нашу экономику и

преобразуют нашу повседневную жизнь. Мы наблюдали также за тем, как в киберпространство проникают проблемы извне, к примеру, эксплуатация и агрессия. Адаптируясь к этим вызовам, мы будем подавать пример другим. Соединенные Штаты будут придерживаться таких принципов в отношении международного киберпространства, которые бы открывали возможности для инноваций, стимулирующих развитие экономики и обеспечивающих повышение качества жизни в нашей стране и за рубежом. В основу этой работы будут заложены принципы, имеющие жизненно важное значение не только для внешней политики США, но и для будущего Интернета как такового.

Опора на достижения

Соединенные Штаты Америки привержены сохранению и развитию преимуществ цифровых сетей для наших обществ и экономик.

Эти преимущества разнообразны и глубоки. Для граждан компьютерные сети означают способ повышения производительности труда и благосостояния, они помогают бороться с дефектами и ограничениями в дееспособности, возвращают в общество тех, кто изолирован по языковому признаку или вследствие редкого заболевания, помогают поддерживать связи между членами семей и друзьями, разделенными расстояниями и границами. Они повышают скорость реакции на чрезвычайные ситуации, расширяют возможности обмена информацией при расследовании преступлений, позволяют оповещать о коррупции, облегчают проведение политических акций и привлечение внимания к причинам, которые в противном случае остались бы незамеченными. Для бизнеса компьютерные сети – это путь на новые рынки и создание предприятий с капитализацией в миллиарды долларов. Для правительств они означают повышение прозрачности, эффективности, удобства и сближение лидеров с теми, кому эти лидеры призваны служить. Для международного сообщества компьютерные сети позволили создать площадку для нового глобального рынка идей и направить в нужное русло поразительную отзывчивость, проявляемую перед лицом трагедий. Чем свободнее распространяется информация, тем сильнее становятся наши общества. При правильном использовании эти технологии помогут стать нам всем сильнее, и мы продолжим усилия по расширению

сфер охвата сетей и совершенствованию их работы как внутри страны так и за рубежом.

Осознание вызовов

Соединенные Штаты признают, что развитие этих сетей несет с собой новые вызовы для нашей национальной и экономической безопасности, равно как и для безопасности мирового сообщества.

Эти вызовы могут принимать различные формы. Стихийные бедствия, аварии и диверсии могут выводить из строя кабели, серверы и беспроводные сети на территории США и за рубежом. Вызовы технического характера также могут приводить к срывам, например, применяемый той или иной страной способ блокирования работы веб-сайта может порождать гораздо более масштабный каскадный срыв работы международной сети. Вымогательство, мошенничество, кража персональных данных, эксплуатация детского труда могут подрывать доверие пользователей, вовлеченных в торговлю через Интернет, использующих социальные сети, и даже порождать угрозы для личной безопасности пользователей. Кража интеллектуальной собственности угрожает конкурентоспособности национальной экономики и инновациям, стимулирующим повышение такой конкурентоспособности. Подобные вызовы выходят за пределы национальных границ. Низкая стоимость вхождения в киберпространство и возможность сохранения анонимного виртуального присутствия позволяют также преступникам устраивать себе «безопасные гавани», известные или неизвестные государству. Угрозы для кибербезопасности могут даже создавать опасность для мира и международной безопасности в более широком смысле, по мере того, как традиционные формы конфликтов распространяются на киберпространство.

Приверженность принципам

Соединенные Штаты будут противостоять этим вызовам, исходя из защиты наших ключевых принципов.

Наша политика зиждется как на сохранении всего лучшего, что есть в киберпространстве, так и на приверженности нашим принципам. Наша политика в отношении международного киберпространства отражает нашу принципиальную

приверженность *защите основных свобод*, *неприкосновенности частной жизни* и *свободе распространения информации.*.

Основные свободы. Наша приверженность свободе слова и свободе объединений остается неизменной, но не в ущерб общественной безопасности или защите наших граждан. В числе этих гражданских свобод, которые обычно на международном уровне именуются «основными свободами», безграничные возможности поиска, получения и распространения информации и идей с помощью различных носителей, становятся важными, как никогда прежде. Как государство, мы не закрываем глаза на Интернет-пользователей со злостными намерениями, но одновременно признаем, что следует очень осторожно и взвешенно подходить к ограничениям на свободу слова в киберпространстве. К примеру, детская порнография, пропаганда насилия и организация террористических актов, не допустимы ни в каком обществе и потому им не место в Интернете. При этом, Соединенные Штаты продолжат борьбу с этими явлениями, используя средства, не противоречащие нашим базовым ценностям, тщательно подходя к решению этих вопросов, не спекулируя на ценности Интернета для общества.

Неприкосновенность частной жизни. Наша Стратегия увязывает взятые обязательства по защите наших граждан и интересов с обязательствами в отношении неприкосновенности частной жизни. По мере того, как Интернет все глубже проникает в общественную жизнь и частную жизнь граждан, они хотят быть уверенными в неприкосновенности частной жизни: люди должны иметь возможность понять, как могут быть использованы их персональные данные, и хотят быть уверенными в том, что с этими персональными данными будут обращаться надлежащим образом. При этом они хотят также получить защиту от мошенничества, краж, угроз для личной безопасности, которые могут таиться в Сети, и ожидают, что в их распоряжении будут все средства обеспечения соблюдения законности для выявления и преследования лиц, использующих Интернет для эксплуатации других. Соединенные Штаты обязуются сохранять баланс между обеими сторонами этого уравнения, предоставляя правоохранительным органам необходимые им права в части расследований и защищая права личности посредством надлежащего судебного надзора и контроля за обеспечением законности.

Свобода распространения информации. Государства не делают и не должны делать выбор между свободой распространения информации и безопасностью своих сетей. Наилучшие решения по обеспечению безопасности в киберпространстве

отличаются динамизмом и адаптивностью, оказывая лишь минимальное влияние на производительность сети. Такие инструменты обеспечивают безопасность систем без ущерба для инноваций, без ущемления свободы слова или объединений и без помех для глобальной функциональной совместимости (интероперабельности). В отличие от этого мы наблюдаем другие подходы, к примеру, национальные фильтры и межсетевые экраны. Они создают лишь иллюзию безопасности, но затрудняют поддержание эффективности и развитие Интернета как открытой, интероперабельной, безопасной и надежной среды обмена данными. Такой же подход справедлив и в отношении бизнеса: киберпространство должно оставаться пространством с «равными правилами игры», поощряющей инновации, предпринимательство и предприимчивость, а не ареной, где государства по своему усмотрению нарушают свободу распространения информации для приобретения незаслуженных преимуществ. Соединенные Штаты сохраняют приверженность международным инициативам и подходам, направленным на развитие киберпространства в контексте защиты свободной торговли, расширении распространения информации, признавая нашу глобальную ответственность, наряду с национальными интересами.

Слишком часто такие принципы характеризуются как не совместимые с эффективным соблюдением законности, сохранением анонимности, защитой детей и безопасностью инфраструктуры. На самом деле надлежащая кибербезопасность способна повысить уровень неприкосновенности частной жизни, а эффективная правоприменительная деятельность в сфере противоправного поведения, поможет защитить основные свободы. Законность - гражданский порядок, при котором добросовестное соблюдение законов защищает граждан и их интересы, приносит стабильность на мировых рынках и ставит злоумышленников под международный контроль – одновременно поддерживает нашу национальную безопасность и продвигает наши общие ценности.

II. Будущее киберпространства

Представьте себе будущее, в котором надежный доступ к Интернету имеется практически в любой точке земного шара, причем по ценам, вполне доступным для бизнеса и обычных семей. Компьютеры могут связываться друг с другом в эффективно интегрированном пространстве глобальных сетей, обеспечивающих защищенное мгновенное соединение с друзьями и коллегами как в пределах того или иного блока, так

и по всему миру. Информационные ресурсы (контенты) представлены на национальном языке, и эта информация свободно перетекает через государственные границы, а все более совершенный цифровой перевод открывает для миллионов все богатство знаний, новых идей и плодотворных дискуссий. Новые технологии, повышающие уровень сельского хозяйства или здравоохранения, предлагаются тем, кто в них нуждается, и решение сложных проблем облегчается благодаря глобальному сотрудничеству экспертов и новаторов. Вот, лишь частично, то будущее киберпространство, к которому стремятся США, и то будущее, над приближением которого мы работаем.

В таком будущем граждане и бизнес смогут быстро и легко получать инструментарий, необходимый для индивидуального нахождения конкретного пользователя в Интернете; доменные имена и адреса станут доступными, их использование будет безопасным, должным образом поддерживаемым, не требующим обременительных лицензий или излишнего раскрытия персональной информации. Лучшие инженеры мира работают рука об руку над разработкой новых стандартов для информационных систем с повышенной проходимостью и надежностью сетей, стимулирующих инновации и расширяющих доступ. Высокотехнологичная индустрия сотрудничает с заказчиками в создании программного и аппаратного обеспечения и услуг с более высоким уровнем безопасности, надежности и учета конкретных потребностей.

Это будущее, в котором университеты и компании не знают ограничений в исследованиях и разработке новых концепций или продуктов, поскольку уверены в том, что их интеллектуальная собственность и ценные данные находятся в безопасности даже в сетях с общим доступом. Граждане знают угрозы для их персональных компьютеров и могут применять простые в использовании средства для защиты своих систем. Частные компании также несут ответственность за «сетевую гигиену», понимая, что тем самым они защищают собственные инвестиции. В тех случаях, когда безопасность киберпространства требует тех или иных действий со стороны государства, чиновники в состоянии обнаружить такие угрозы на ранней стадии и распространить соответствующую информацию в реальном масштабе времени для смягчения последствий или минимизации воздействий крупного срыва – и все это при сохранении всей широты свободного распространения информации. При совершении преступления на международном уровне правоохранительные органы смогут сотрудничать в целях обеспечения защиты, совместного доступа к следственным материалам и привлечения виновных к судебной ответственности.

Такое будущее сулит не только повышение благополучия и более надежную работу сетей, но и повышение международной безопасности и стабильности мира. Государства будут выступать в киберпространстве в качестве ответственных сторон, формируя конфигурацию сетей, не создавая угрозы срывов их работы для других и не позволяя преступникам использовать Интернет для осуществления их замыслов из «безопасных гаваней». Государства знают, что сетевая инфраструктура должна быть защищена, и предпринимают меры для обеспечения ее безопасности от нарушений и диверсий. Они продолжат двустороннее, многостороннее и международное сотрудничество на универсальном уровне для перехода мира к «эпохе информации» и достижения консенсуса между странами, стремящимися к сохранению основополагающих особенностей Интернета.

Соединенные Штаты и растущее число их партнеров уже заложили фундамент для такого будущего. Однако успех пока нельзя считать предрешенным, и мы не справимся с этим в одиночку. Несмотря на то, что прогресс может оказаться медленным и потребовать огромных ресурсов, международное сообщество должно сплотиться в поддержке таких долгосрочных инвестиций. Мы должны делать это, отчетливо понимая, что описанное выше киберпространство отвечает национальным интересам настолько же, насколько оно служит международным целям. Определяющими для нашего успеха станут следующие полвека развития информационных технологий, не менее эволюционными, чем последние 50 лет, поскольку мы начинаем понимать в полной мере выгоды (и сводить к минимуму риски) глобальной взаимозависимости.

Будущее, к которому мы стремимся

Сфера киберпространства, к которой мы стремимся, поощряет инновации и поддерживает предпринимателей, соединяет индивидуумов и укрепляет общность; влияет на деятельность правительств и способствует «прозрачности» действий правительств; стоит на страже основных свобод и обеспечивает неприкосновенность личной жизни; она способствует пониманию, уточняет нормы поведения и повышает национальную и международную безопасность. **Для поддержания такой среды наилучшей практической формой является международное сотрудничество – это первый принцип.**

Наша цель

Соединенные Штаты Америки будут сотрудничать на международной арене с целью содействия развитию **открытой, функционально совместимой (интероперабельной), безопасной и надежной** инфраструктуры информационных технологий и связи, поддерживающей международную торговлю, повышающей международную безопасность и благоприятствующей свободе слова и инновациям. Для достижения этой цели мы сформируем и будем поддерживать пространство, в котором нормы ответственного поведения регулируют действия государств, поддерживают партнерство, а также верховенство закона в киберпространстве.

Открытость и функциональная совместимость (интероперабельность): киберпространство, которое предоставляет возможности

В основе цифровых инноваций лежит возможность добавлять новую функциональность объединенным в сеть машинам. Открытость цифровых систем объясняет их взрывной рост, стремительное развитие и непреходящее значение. Базовый инструментарий сетевых технологий характеризуется устойчивым повышением доступности и снижением цен по мере того, как компьютеры и доступ в Интернет распространяются по всем странам мира. Для продолжения удовлетворения потребностей постоянно растущей части человечества, имеющей выход в Сеть, производители аппаратного обеспечения и операционных систем должны продолжить наделять соответствующими правами как можно более широкие круги разработчиков по всему миру. В условиях, когда компании продолжают стимулировать инновации при разработке собственного программного обеспечения, мы также приветствуем идею открытого источника программных продуктов, что дает разработчикам и потребителям возможность выбора разработанных сообществом программистов решений, наиболее подходящих для конкретных нужд.

Соединенные Штаты поддерживают сквозную функциональную совместимость (интероперабельность) Интернета, так как это позволяет людям по всему миру подключаться к источникам знаний, идей и связываться друг с другом с помощью технологии, отвечающей их потребностям. Свободный поток информации зависит от функциональной совместимости (интероперабельности) – принципа, подтвержденного 174 странами в Тунисском обязательстве, провозглашенном на Всемирной встрече на высшем уровне (ВСИС) по вопросам информационного общества. Альтернативой глобальной открытости и функциональной совместимости (интероперабельности) является фрагментированный Интернет, в котором большие группы населения земного

шара будут лишены доступа к высокоуровневым прикладным технологиям и к разнообразным информационным ресурсам в угоду политическим интересам отдельных стран. Совместная разработка основанных на консенсусе международных стандартов по информационным технологиям и технологиям связи представляет собой ключевую составляющую усилий по сохранению открытости и функциональной совместимости (интероперабельности), развитию цифровых экономик и продвижению наших обществ вперед.

Безопасность и надежность: киберпространство, которое выдерживает испытание временем

Для того, чтобы киберпространство смогло пройти проверку временем, мы должны доверять сетевым системам. Пользователи должны быть уверены в том, что их данные находятся в безопасности как в процессе прохождения по Сети, надежности доставки, так и в их сохранности. Эффективная стратегия потребует действий на многих направлениях, коллективной ответственности всех слоев общества, начиная с конечного пользователя и заканчивая сотрудничеством между странами.

Обеспечение устойчивости потребует надежных технических стандартов и решений, эффективного контроля безопасности, надежных программно-технических средств и защищенности логистических цепочек. Снижение рисков в глобальном масштабе нуждается в эффективном обеспечении правоприменительной деятельности; согласованных международным сообществом норм поведения государств; мер по повышению доверия и информационной открытости; активной информированной дипломатии; и надлежащих средствах сдерживания. Наконец, противодействие нарушениям потребует более интенсивного сотрудничества и обмена технической информацией с частным сектором и международным сообществом. В полной мере, такая работа не по силам одной стране или одному сектору – это ответственность и обязанность, которые должны разделить между собой все страны и народы этих стран.

Устойчивость сети – краеугольный камень нашего глобального благополучия, и обеспечение безопасности этих сетей выходит за рамки чисто технических проблем. В экономическом отношении мы обязаны обеспечивать устойчивый рост и осуществлять инвестиции в инфраструктуру как у себя в стране, так и за рубежом, стимулируя усилия по повышению сетевой устойчивости и проясняя обязанности компаний и государств. В политическом отношении мы должны содействовать поддержанию пространства, не

нарушающего техническую инфраструктуру, с тем, чтобы споры не становились поводами для срывов в работе сетей и ухудшения их состояния. В социальном аспекте нам надлежит довести до понимания пользователей их ответственность в том, что касается поддержания своего оборудования и устройств в безопасном состоянии и эксплуатации такого оборудования безопасными способами.

Стабильность с помощью создания норм.

США, вместе с государствами-единомышленниками, будут работать над формированием таких условий требований или норм поведения, которые обеспечивали бы взаимную «притирку» внешней политики и политики в области обороны и направляли бы международное сотрудничество. В последние двадцать лет наблюдалось стремительное и беспрецедентное развитие Интернета как социальной среды; общества во все возрастающей степени полагались на сетевые информационные системы в части контроля инфраструктурных объектов и систем связи, критически важных для современной жизни; и со всей очевидностью правительства стремились осуществлять традиционные функции власти с помощью киберпространства. Эти процессы развивались в отсутствие четко согласованных норм, регламентирующих допустимое поведение государств в киберпространстве. Для устранения этого вакуума мы намерены работать над достижением консенсуса по вопросу о том, чтó следует понимать под допустимым поведением, и сотрудничать с теми, кто считает функционирование таких систем существенным фактором с точки зрения национальных и коллективных интересов.

Роль норм. В других сферах международных отношений достижение общего понимания по вопросу допустимого поведения позволило повысить стабильность и создать основу для международных действий в случаях, когда требуются принятие мер по устранению недостатков. Соблюдение таких норм вносит предсказуемость в поведение государств, содействуя предотвращению разногласий, способных порождать конфликты.

Разработка норм поведения государств в киберпространстве не требует ни обновления обычного международного права, ни переработки существующих международных норм. Проверенные временем международные нормы, регламентирующие поведение государств (в мирное время или во время конфликтов), применимы и к киберпространству. Тем не менее, уникальные свойства сетевых технологий требуют дополнительной работы с тем, чтобы определить, как эти нормы следует применять и какие дополнительные меры для реализации этих норм могут

оказаться необходимыми. Мы продолжим работу на международном уровне для достижения консенсуса по вопросам, связанным с применением норм поведения в киберпространстве, исходя из того, что важный первый шаг в этом направлении заключается в переносе в киберпространство ясно выраженных надежд на миролюбивые подходы, в том числе в межгосударственном взаимодействии в киберпространстве.

Нормативная основа. Правила, стимулирующие порядок и мир, способствующие сохранению элементарного человеческого достоинства и поощряющие свободную экономическую конкуренцию, существенны для любого международного пространства. Эти принципы дают базовые ориентиры для государств, стремящихся выполнить свои традиционные международные обязательства в отношении киберпространства, и во многих случаях отражают обязанности государств, сохраняющиеся вне зависимости от конкретного контекста. К числу существующих принципов, которые следует соблюдать в киберпространстве, относятся следующие:

- **Защита основных свобод**: Государства должны уважать фундаментальные свободы слова и объединений – как в Сети, так и вне ее;
- **Охрана права собственности**: Государства, в своих обязательствах и средствами национального законодательства, должны соблюдать права интеллектуальной собственности, включая патенты, коммерческие секреты, товарные знаки, авторские права;
- **Ценность частной жизни**: Граждане должны иметь защиту от произвольного или незаконного вмешательства государства в их частную жизнь, когда они пользуются Интернетом;
- **Защита от преступлений**: Государства должны выявлять и наказывать киберпреступников, обеспечивать отсутствие в законах и правоприменительной практике лазеек для создания преступниками убежищ, своевременно сотрудничать при проведении международных уголовных расследованиях;
- **Право на самооборону**: В соответствии с Уставом ООН, государства обладают неотъемлемым правом на самооборону, которая может потребоваться после определенных актов агрессии в киберпространстве.

Из перечисленных выше традиционных принципов межгосударственного поведения могут быть выведены обязательства, в большей степени соответствующие киберпространству. Они сфокусированы, прежде всего, на сохранении функциональности глобальной сети и повышении уровня безопасности киберпространства. Многие из этих

обязательств уходят своими корнями в технические реалии Интернета. Поскольку базовая функциональность Сети зиждется на системах доверия (к примеру, протокол BGP – протокол пограничной маршрутизации), государства должны осознавать возможные международные последствия своих технических решений и действовать уважительно по отношению к сетям других стран и Интернету в широком смысле. Аналогичным образом, при разработке следующего поколения таких систем мы должны отстаивать общие интересы, поддерживая наиболее здравые технические стандарты и структуры управления, а не те, что нацелены лишь на повышение национального престижа или усиление политического контроля. Эти новейшие нормы, также являющиеся основополагающими для рассматриваемого пространства, включают следующее:

- **Глобальная функциональная совместимость (интероперабельность):** Государствам надлежит действовать в рамках своих полномочий для содействия обеспечению сквозной функциональной совместимости общедоступного Интернета;
- **Сетевая устойчивость**: Государствам следует уважительно относиться к свободе распространения информации в национальных сетевых конфигурациях, избегая произвольного вмешательства в международную взаимосвязанную инфраструктуру;
- **Надежный доступ:** Государствам не следует произвольно лишать граждан доступа в Интернет или к иным сетевым технологиям либо нарушать такой доступ;
- **Многостороннее управление**: Усилия по управлению Интернетом не должны сводиться к действиям правительств – они должны включать всех заинтересованных лиц;
- **Предварительная оценка безопасности киберпространства**: Государствам надлежит признать свою ответственность в части защиты информационных инфраструктур и обеспечения безопасности национальных систем от повреждения или злоупотреблений и действовать, исходя из такой ответственности.

В процессе развития киберпространства как динамичной среды, международная деятельность в этом пространстве должна основываться на принципах ответственного национального управления, миролюбивого поведения государств и надежного управления сетью. По мере развития этих идей, Соединенные Штаты будут поощрять дискуссии и полноценно участвовать в них, продвигая принципиальный подход к выработке решений в отношении Интернета и добиваясь оптимальных общих договоренностей по каждому вопросу.

Для реализации такого будущего и содействия пропаганде конкретных норм Соединенные Штаты будут сочетать дипломатию, оборону и развитие для содействия процветанию, безопасности и открытости с тем, чтобы каждый мог воспользоваться выгодами сетевых технологий. Эти три составляющие являются центральной осью наших усилий на международной арене. Во второй половине 20-ого века США внесли свой вклад в формирование новой послевоенной архитектуры международного сотрудничества в экономике и безопасности. В 21-ом столетии мы будем работать над реализацией представленного мирного и надежного киберпространства в таком же духе сотрудничества и коллективной ответственности.

Дипломатия: укрепление партнерства

Распространение принципов мира и безопасности на киберпространство (при сохранении его преимуществ и природы) потребует укрепления партнерства и расширения инициатив. Мы будем вовлекать международное сообщество в откровенный и настойчивый диалог для достижения консенсуса в отношении принципов ответственного поведения в киберпространстве и необходимых для этого действий (как внутри страны, так и со стороны международного сообщества), а также для формирования условий стабильности киберпространства.

Дипломатическая цель

Соединённые Штаты будут создавать стимулы и вырабатывать консенсус по вопросам международного пространства, в котором государства, признающие ценность открытого, функционально совместимого, безопасного и надёжного киберпространства, будут вместе работать и выступать в качестве ответственных участников.

Укрепление партнерства

Через наши международные связи и контакты мы будем стремиться к тому, чтобы как можно больше заинтересованных сторон разделили представленное выше видение киберпространства — именно в связи с его экономическими, социальными, политическими преимуществами и преимуществами в области безопасности. Такие

усилия будут поддерживаться содержательным сотрудничеством с частным сектором как внутри страны, так и за рубежом.

Распределенные системы требуют согласованной работы, поскольку никакая единая организация, договоренность, никакой документ или инструмент не будут в полной мере отвечать нуждам нашего сетевого мира. Для того, чтобы киберпространство в полной мере реализовало свой потенциал, важны усилия буквально всех, начиная с пользователей, продавцов аппаратного и программного обеспечения, представляющих частный сектор, Интернет-провайдеров и заканчивая региональными, многопрофильными и многосторонними организациями.

В частности, на международной арене государствам надлежит продолжить усилия по сохранению мира, поощрению инноваций, защите экономических интересов и интересов национальной безопасности, защите и продвижению прав граждан. В международных отношениях США будут работать над созданием международных требований, которые увязывают внешнюю политику с политикой в области обороны и содействуют укреплению наших международных отношений.

Двустороннее и многостороннее сотрудничество. Мы намерены взаимодействовать с другими государствами на двусторонней основе для налаживания сотрудничества по вопросам киберпространства, важным для наших правительств и народов. Формирование широкого международного взаимопонимания по правилам поведения в киберпространстве должно начинаться с четкого соглашения между государствами-единомышленниками. Мы будем стремиться к образованию широкого сообщества партнеров по таким усилиям и включим связанные с киберпространством вопросы в обширный спектр двусторонних диалогов на всех уровнях работы правительства и по широкому кругу нашей деятельности. Мы будем содействовать общности действий в ответ на возникающие в связи с киберпространством вызовы, основываясь на уже проверенных временем инструментах и принципах принуждения. Более того, мы будем активно вовлекать развивающиеся страны и позаботимся о том, чтобы их голоса по таким вопросам были услышаны.

Международные организации и организации многостороннего управления. Региональные организации оказались особенно эффективными в решении проблем киберпространства, затрагивающих членов таких объединений. Они будут играть все более важную роль в разработке и применении норм поведения. Мы продолжим использовать наше членство в этих организациях, равно как и в более масштабных международных объединениях, для разработки продуктивных повесток дня, соответствующих опыту каждой такой организации и реализующих конкретные выгоды для их участников. В том, что касается принципов управления Интернетом, были сделаны важные шаги для обеспечения реагирования и международного представительства в ключевых организациях. Соединенные Штаты приветствуют такие усилия и по-прежнему высоко оценивают уникальный вклад таких форумов, представляющих все Интернет-сообщество, объединяющих частный сектор, гражданское общество, академические круги и правительства в единое многостороннее пространство.

Сотрудничество с частным сектором. Несмотря на то, что частный сектор уже играет важную роль в международных организациях и организациях многостороннего управления, мы продолжим использовать существующие механизмы партнерства для установления партнерских отношений. В частности, мы намерены тесно сотрудничать с владельцами и операторами инфраструктурных объектов (ответственными за бóльшую часть сетевой функциональности) для расширения инициатив по обеспечению безопасности сетевой экосистемы, сохранения преимуществ и природы киберпространства, предотвращения ненужных помех для технологической эволюции и обобщения принципов мира и безопасности. Мы также будем добиваться участия частного сектора в управлении Интернетом, поскольку считаем это существенным фактором поддержания многостороннего характера Сети, и продолжим выступать за включение представителей частного сектора в работу форумов, обсуждающих подобные вопросы.

Система обороны: сдерживание и предупреждение

США будут защищать свои сети вне зависимости от того, исходит ли угроза от террористов, киберпреступников, государств или их представителей. Не менее важно, что мы будем поощрять тех, кто действует с добрыми намерениями, и обуздывать и сдерживать тех, кто своими действиями в киберпространстве создает угрозы миру и стабильности. При этом будет применяться дублирование политики, сочетающей национальные и международные меры по повышению сетевой устойчивости с

бдительностью и набором надежных вариантов реагирования. Во всех наших оборонительных усилиях мы будем защищать гражданские свободы и неприкосновенность частной жизни в соответствии с нашими законами и принципами.

Цель в области обороны

Соединенные Штаты вместе с другими странами будут поощрять ответственное поведение и противостоять тем, кто пытается нарушать работу сетей и систем, будут обуздывать и сдерживать злоумышленников, сохраняя за собой право защищать эти жизненно важные национальные ценности необходимыми и адекватными средствами.

Сдерживание

Защита сетей такой колоссальной важности потребует наличия мощных оборонительных возможностей. Соединенные Штаты продолжат усиливать средства защиты сетей и нашего потенциала в плане противодействия срывам в работе и другим атакам, а также потенциала восстановления после таких срывов и атак. При более изощренных атаках, причинивших ущерб, мы будем реагировать в соответствии с тщательно разработанными планами по локализации и смягчению наносимого нашим машинам ущерба, ограничивая его последствия для наших сетей и потенциальные каскадные воздействия вне наших сетей.

Внутренние силы и средства. Обеспечение устойчивости наших сетей и информационных систем требует коллективных согласованных действий в общенациональном масштабе, начиная с правительства, которое должно в этом плане сотрудничать с частным сектором и отдельными гражданами. В течение последних десяти лет США содействовали воспитанию культуры безопасности в киберпространстве и созданию эффективного инструментария для снижения рисков и реагирования на чрезвычайные происшествия. Мы по-прежнему делаем акцент на том, что систематическое внедрение здравых практических подходов в области информационных технологий (в государственном и частном секторах) снижает уязвимость нашей страны и укрепляет наши сети и системы. Нам по-прежнему удается сохранять устойчивый прогресс в том, что касается общей ситуационной осведомленности об уязвимости сетей и сетевых рисках, возникающих в государственных и частных сетях. Мы выступили с новыми инициативами, сформулированными нашей национальной группой по реагированию на инциденты в сфере компьютерной безопасности. Эти инициативы

касаются распространения информации среди государственных органов, ключевых отраслей, объектов жизнеобеспечения и других заинтересованных лиц. И мы постоянно ищем новые пути к укреплению партнерства с частным сектором для повышения безопасности систем, которые используются и общественным, и частным сектором.

Внешние силы и средства. Указанная модель обороны доводилась до сведения других стран в рамках образовательных и учебных программ, а также в рамках текущих политических отношений. Сегодня, благодаря существующему и развивающемуся сотрудничеству в технической и оборонительной сферах, государства получают беспрецедентные возможности в части обнаружения инцидентов и реагирования на них. Это исключительно важный шаг на пути к лишению потенциальных злоумышленников возможностей для нанесения постоянного ущерба нашим национальным и международным сетям. Однако надо иметь в виду, что глобальная распределенная сеть требует глобально распределенных средств раннего предупреждения. Мы обязаны продолжить работу над глобальным созданием новых средств реагирования на инциденты в области компьютерной безопасности и способствовать организации взаимосвязей между этими средствами и повышению качества защиты компьютерных сетей. Соединенные Штаты разделяют общий интерес к оказанию содействия менее развитым странам в части формирования оборонительных возможностей, и в сотрудничестве с нашими партнерами мы активизируем усилия в этом направлении. Укрепление связей с нашими друзьями и союзниками позволит повысить общую коллективную безопасность в масштабе всего международного сообщества.

Предупреждение

США продолжат работу над тем, чтобы риски, связанные с атаками на наши сети или использованием этих сетей не по назначению, намного перевешивали те выгоды, которые можно было бы извлечь в результате таких злоупотреблений. Мы в полной мере осознаем, что деятельность в киберпространстве может иметь последствия вне этого пространства; такие действия могут повлечь за собой необходимость мер самообороны. Аналогичным образом, связанные между собой сети связывают более тесно и государства, и потому атака на сети одного государства может иметь последствия, выходящие далеко за его границы.

Что качается преступников или иных лиц, создающих угрозы нашей национальной и экономической безопасности, национальные меры сдерживания требуют, чтобы все государства имели процедуры, позволяющие им проводить расследование действий, аресты и уголовное преследование тех лиц, которые вмешиваются в работу сетей или подрывают их функционирование - будь то на территории государства или за рубежом. На международном уровне правоохранительные органы должны сотрудничать между собой везде, где возможно, в части сохранения данных, которые могут быть быстро ликвидированы, будучи при этом крайне важными для проводимых расследований, сотрудничать с законодательными органами и министерствами юстиции для согласования их усилий, содействовать надлежащему отправлению правосудия и соблюдению законности, – все это ключевые принципы Будапештской конвенции о преступности в сфере компьютерной информации.

В случае необходимости Соединенные Штаты будут реагировать на враждебные действия в киберпространстве так же, как реагировали бы на любую другую угрозу для нашего государства. Все государства обладают неотъемлемым правом на самооборону, и мы полагаем, что некоторые враждебные действия, осуществляемые через киберпространство, могут вынудить нас пойти на те или иные ответные меры в силу обязательств перед нашими партнерами по военным договорам. Мы оставляем за собой право использовать любые необходимые средства — дипломатические, информационные, военные и экономические — которые представляются адекватными и не противоречат существующему международному праву, для защиты нашей Нации, наших союзников, партнеров и наших интересов. При этом мы, по возможности, будем избегать применения военной силы, пока не будут исчерпаны все другие средства, тщательно взвешивать цену и риски действий, сопоставляя их с ценой бездействия, и действовать, сообразуясь с нашими ценностями и укреплением законности, опираясь везде, где возможно, на широкую международную поддержку.

Развитие: благополучие и безопасность

Соединенные Штаты будут по-прежнему демонстрировать нашу приверженность убеждению, что преимущества объединенного сетью мира являются всеобъемлющими. Достоинства открытого, способного к взаимодействию, безопасного и надежного киберпространства должны стать доступнее, и Соединенные Штаты, как мировой лидер

информационной экономики, считает своим долгом делиться техническими ресурсами и опытом с другими.

Наша страна может и будет играть активную роль в предоставлении знаний и возможностей в том, что касается создания и защиты новых и существующих цифровых систем, и тем самым будет содействовать формированию консенсуса государств с тем, чтобы они действовали как ответственные заинтересованные лица. Наращивание потенциала для реализации указанных целей – это не краткосрочные вложения, а разумные долгосрочные инвестиции и обязательства нашего правительства в части продолжения диалога и партнерства.

Задачи развития

Соединенные Штаты будут содействовать наращиванию потенциала в сфере безопасности киберпространства за рубежом, на двусторонней основе, в рамках многосторонних организаций, с тем, чтобы каждая страна имела средства для защиты своей цифровой инфраструктуры, будут укреплять глобальные сети, устанавливать более тесное сотрудничество на принципах консенсуса для создания открытых, функционально совместимых, безопасных и надежных сетей.

Наращивание технического потенциала

Доступ к сетевым технологиям является во все более возрастающей степени основой развития. Правительства и телекоммуникационная отрасль уже сделали ряд существенных шагов по обеспечению связи с пользователями в регионах с недостаточным уровнем обслуживания и регионов с полным отсутствием такого обслуживания. Международные информационные инфраструктуры продолжают расширяться и развиваться, предоставляя все большему числу стран возможность в глобальном распространении информации. Рост сетей по всему миру и расширение доступа к ним обогащает мировое сообщество, однако вместе с тем порождает новые вызовы и открывает возможности для сотрудничества по общепризнанным вопросам и вопросам безопасности в киберпространстве. Во многом этот потенциал наращивается благодаря инвестициям частного сектора, и Соединенные Штаты продолжат работу с

правительствами других стран и телекоммуникационная отраслью в целом по созданию климата, который благоприятствует таким усилиям и в котором эти усилия действительно были бы благотворны для удовлетворения основных потребностей стран в плане дальнейшего развития.

Правительства представляют собой один из решающих факторов того, принесет ли эта новая сфера взаимодействия положительные плоды или израсходует свой потенциал вхолостую. В наибольшей степени от наращивания указанного потенциала выиграют те государства, которые воспринимают технологии для повышения благосостояния и повышения социальной сплоченности, а не занимаются ограничением доступа к ним в целях политического контроля. По этой причине поддерживаемые Соединенными Штатами технические проекты по своему замыслу нацелены на повышение безопасности и содействие коммерции, на защиту свободы распространения информации и стимулирование глобальной функциональной совместимости сетей.

Наращивание потенциала в части безопасности киберпространства

Благополучие нельзя построить на фундаменте страха и ненадежности, и Соединенные Штаты являются приверженцами наращивания потенциала кибербезопасности наряду с технологическим развитием самих государств. Повышение безопасности киберпространства развивающимися государствами на национальном уровне дает непосредственное и долгосрочное преимущество, поскольку большее число стран получает в свое распоряжение средства для противодействия угрозам, зарождающимся на их территории и, в свою очередь, формирует доверие к глобальным сетям и способствует сотрудничеству в борьбе с преступными формами использования информационных технологий. Кроме того, весьма важно развивать динамичные международные исследовательские сообщества, способные отвечать на возникающие вызовы безопасности в киберпространстве.

Признавая, что кибербезопасность представляет собой глобальную проблему, которая должна решаться национальными усилиями всех стран, мы будем и в дальнейшем расширять и упорядочивать инициативы, нацеленные на наращивание потенциала в области кибербезопасности, делая акцент на повышении осведомленности, правовом и техническом обучении, поддержке разработке принципов. Такие программы не должны ограничиваться чисто технологическими аспектами. Мы будем сотрудничать с другими

странами для уяснения всей широты вызовов кибербезопасности, помогать им в развитии собственных стратегий и наращивать потенциал по целому спектру секторов – начиная от безопасности сетей и создания групп реагирования на нарушения компьютерной защиты в сети Интернет (CERT), продолжая обеспечением соблюдения законности на международном уровне и сотрудничеством в области обороны и заканчивая плодотворными связями с отечественным и международным частным сектором и гражданским обществом.

Укрепление политических связей

Содействие Соединенных Штатов в части укрепления потенциала рассматривается как инвестиция, обязательство и важная возможность для диалога и партнерства. По мере того, как страны будут вносить вклад в решение вопросов кибербезопасности, мы будем переносить наш диалог на более высокий уровень – от укрепления потенциала к активному экономическому, техническому, правоприменительному и дипломатическому сотрудничеству по вопросам, касающимся всех заинтересованных сторон. Мы продолжим также укреплять связи между странами, развивающими потенциал в сфере кибербезопасности (используя для этих целей региональные форумы и технические органы, обладающие особыми компетенциями) и будем, как и раньше, содействовать распространению самых передовых практических подходов, усвоенного практического опыта и осуществлению международного обмена технической информацией.

III. Политические приоритеты

Соединенные Штаты продолжат усилия по содействию построению и поддержанию открытых, интероперабельных, безопасных и надежных сетей внутри страны и за рубежом, как для наших граждан, так и для мирового сообщества. Наш подход базируется на фундаментальных принципах, определяется генеральной целью и поддерживается методами, сформулированными в настоящем документе – в совокупности они образуют основу международной стратегии Соединенных Штатов Америки по вопросам киберпространства.

Для того, чтобы приблизить будущее, в котором это пространство сможет в полной мере реализовать свой потенциал для всех, правительство Соединенных Штатов структурирует свою деятельность по семи независимым направлениям, для каждого из которых потребуется сотрудничество внутри правительства, с международными партнерами и с частным сектором. Все это вместе создаст векторы действий в общей структуре стратегических принципов.

Те многие министерства и ведомства правительства США, которые уже включены в эту работу, умножат предпринимаемые важные усилия. Те министерства и ведомства, которые в настоящее время разрабатывают планы мероприятий для осуществления тех или иных обязанностей применительно к киберпространству, выработают контекст и обеспечат единство усилий. Представленные здесь политические приоритеты предусматривают и определяют те конкретные действия (с должным учетом как акцентов, расставленных в прошлом, так и текущих и будущих акцентов), которые требуют совместного внимания и координации ресурсов на национальном уровне.

Экономика: продвижение международных стандартов и инновационных, открытых рынков

С тем, чтобы киберпространство и дальше удовлетворяло потребности наших экономик и новаторов, мы будем:

- **поддерживать свободное рыночное окружение, поощряющее технологические инновации через доступные, глобально связанные сети.** Подобно тому, как свобода потоков информации исключительно важна для функционирования наших сетей, свободная торговля способствует поддержке инноваций и рыночному росту в эпоху информации. Глобальный охват Интернета во многом отражается в распространении более дешевых и повсеместно доступных компьютеров и сетевых технологий. Конкуренция на этих рынках стимулирует инновации, а среда свободной торговли дает производителям возможность поддерживать конкурентные цены и высокие стандарты. Уважительное отношение к международным стандартам разработки технологий и торговли представляет собой существенную часть поддержания открытых рынков и позволяет компаниям, занимающимся высокими технологиями, быстро доводить до потребителя преимущества своих инновационных продуктов и услуг. В течение нескольких будущих десятилетий глобализация разработки

технологий будет только нарастать, принося ощутимые выгоды для наших сетей и потребителей. Соединенные Штаты будут работать над поддержанием такой среды свободной торговли (прежде всего в секторе высоких технологий) для обеспечения будущих инноваций;

- **защищать интеллектуальную собственность, в том числе коммерческую тайну, от воровства**. Те же самые сети, что питают инновации, открывают также новые лазейки для промышленного шпионажа и кражи интеллектуальной собственности и коммерческой информации. Киберпространство может использоваться для воровства беспрецедентных объемов информации у компаний, университетов и государственных органов. Потери от кражи информации и технологий могут достигать миллиардов долларов. Отдельные инциденты зачастую остаются незамеченными или необнаруженными. Результат таких действий может варьироваться от недобросовестной конкуренции до банкротства целых компаний, а в национальном масштабе последствия могут быть на несколько порядков более серьезными. Постоянные кражи интеллектуальной собственности, будь то преступниками, иностранными фирмами или агентами тех или иных государств, могут подрывать конкурентоспособность в мировой экономике и снижать инновационные возможности бизнеса. Соединенные Штаты будут принимать меры для обнаружения неправомерных действий и реагирования на такие действия с тем, чтобы укреплять международную среду, в которой подобные действия признаются противозаконными, недопустимыми и требующими привлечения таких нарушителей к ответственности;
- **обеспечивать верховенство совместимых и безопасных технических стандартов, вырабатываемых техническими экспертами.** Разработка международных добровольных, основанных на консенсусе стандартов, относящихся к киберпространству, и создание продуктов, процессов и услуг на основе таких стандартов являются фундаментом интероперабельной, безопасной и устойчивой глобальной инфраструктуры. Государственный и частный секторы должны работать рука об руку над разработкой, поддержанием и внедрением этих стандартов, равно как и поддерживать разработку международных стандартов и процедур оценки соответствия, которые бы устраняли барьеры для международной торговли и коммерции. Международная стандартизация киберпространства и добровольные, основанные на принципе консенсуса процедуры служат общим интересам. Они поощряют инновации, облегчают взаимную функциональную совместимость, повышают безопасность и устойчивость, доверие к транзакциям, осуществляемым через Интернет, стимулируют конкуренцию на глобальных рынках. Соединенные

Штаты будут укреплять сотрудничество между государственным и частным секторами в поддержку распространения требований к продукции и услугам, основанных на международных стандартах;

Защита наших сетей: повышение безопасности, надежности и устойчивости

Поскольку надежная кибербезопасность критически важна для понимаемой более широко экономической и национальной безопасности, мы:

- **будем стимулировать сотрудничество по вопросам киберпространства, в частности, в области норм поведения государств в киберпространстве - в двухстороннем порядке и в рамках целого ряда многосторонних организаций и многонационального партнерства**. Все большее число международных организаций вовлекаются в решение вопросов кибербезопасности и киберпространства вообще, и Соединенные Штаты продолжат содействие этой важной работе так, чтобы формируемое киберпространство отвечало потребностям тех организаций, в которых мы участвуем. США приложили усилия для включения насущных вопросов киберпространства в повестку заседаний Организации американских государств (OAS), Регионального форума Ассоциации государств Юго-Восточной Азии (ASEAN), Организации Тихоокеанского экономического сотрудничества (APEC), Организации по безопасности и сотрудничеству в Европе (OSCE), Африканского союза (AU), Организации экономического сотрудничества и развития (OECD), «Большой восьмерки» (G-8), Европейского союза, ООН и Совета Европы и для обеспечения того, чтобы такая работа поддерживалась эффективными институциональными структурами. На указанных выше и других форумах Соединенные Штаты продолжат усилия по консолидации регионального и международного консенсуса по ключевым видам деятельности, связанной с киберпространством (в том числе по вопросу норм). Кроме того, мы с надеждой смотрим в сторону форумов, где реально осуществляется многостороннее сотрудничество и продвижение к консенсусу и где могут вырабатываться те принципы дальнейшего развития Интернета, которые обсуждаются в этом документе. Мы приветствуем расширение такой работы на географические регионы, в настоящее время недостаточно представленные в диалоге (прежде всего, это Африка и Ближний Восток), для продвижения нашего интереса к наращиванию соответствующего потенциала по всему миру;

- **будем бороться за уменьшение числа вторжений в сети США и срывов их работы.** Несанкционированный доступ в сети создает угрозы целостности экономик и подрывает национальную безопасность. Различные ведомства правительства США сотрудничают между собой и с частным сектором в сфере защиты инноваций от промышленного шпионажа, защиты федеральных сетей, сетей штатов и местных государственных сетей, защиты военных операций в условиях нарушенной операционной среды, сбережения критически важной инфраструктуры от вторжений и атак (прежде всего, объектов энергетических, транспортных и финансовых систем) и защиты промышленной базы. Соединенные Штаты будут по-прежнему добиваться широкого международного согласия государств, признающих важность уважения к собственности и устойчивости сетей, и будут поддерживать такую точку зрения с учетом нашей готовности и готовности наших партнеров к защите сетей от действий, создающих для них угрозу;
- **обеспечим оперативное реагирование на инциденты, устойчивость и возможности восстановления информационной инфраструктуры.** Во взаимосвязанной глобальной среде низкий уровень безопасности систем одной страны создает риск для других. Ни одна из стран не сможет получить полного ознакомления с системами всего мира. У нас имеется обязательство делиться информацией о наших собственных сетях и сотрудничать с другими странами в ситуациях, когда те или иные события могут угрожать нам всем. Так как мы продолжаем наращивать и укреплять наши возможности в плане реагирования, мы будем работать сообща с другими странами над расширением международных сетей, поддерживающих повышение уровня глобальной ситуационной осведомленности и реагирования на инциденты (включая сотрудничество между правительством и отраслью). Правительство США активно участвует в контроле, предупреждении инцидентов и реагировании на таковые посредством обмена информацией с надежными сетями международных партнеров. Мы будем и дальше наращивать эти возможности в рамках международного сотрудничества для повышения общего уровня устойчивости. Кроме того, Соединенные Штаты будут прилагать усилия по международному участию в учениях, посвященных безопасности в киберпространстве, по повышению качества и усилению существующих оперативных процедур вместе с нашими партнерами;
- **повысим надежность высокотехнологичной цепочки поставок, в консультациях с отраслью.** Работа критически важных сетей и информационных инфраструктур зависит от гарантированной эксплуатационной готовности надежного аппаратного и программного обеспечения. Уязвимости в логистических цепочках могут открыть

возможности для атак на целостность, готовность или конфиденциальность сетей и содержащихся там данных. Использование этих уязвимых мест снижает экономическую эффективность и ослабляет национальную безопасность. Соединенные Штаты продолжат сотрудничество с отраслевыми и международными партнерами в том, что касается разработки передовых практических методов защиты целостности информационных систем и критически важной инфраструктуры. Таким образом мы значительно повысим безопасность глобализированных логистических цепочек, от которых зависит свободная открытая торговля;

Правоприменение: расширение сотрудничества и верховенство закона

Для повышения доверия к киберпространству и преследования тех, кто допускает злоупотребления в онлайн-системах, мы будем:

- **принимать полноценное участие в развитии международной политики по вопросам киберпреступности.** Соединенные Штаты обязуются активно участвовать в обсуждениях по вопросам выработки международных норм и мер по киберпреступности в рамках двусторонних и многосторонних контактов, на форумах, доказавших свою компетентность и имеющих достижения в плане продвижения эффективных принципов борьбы с такой преступностью. Обсуждения подобного рода будут включать текущие усилия, например, по расширению области влияния таких институтов, как Будапештская конвенция. США будут базировать эти усилия на успешном партнерстве между национальными правоохранительными органами и на плодотворных политических диалогах, которые мы в настоящее время ведем, развивая чувство ответственности у государств, вовлекаемых в такую работу;
- **гармонизировать законы о киберпреступности на международном уровне, расширяя число стран, присоединившихся к Будапештской конвенции.** Соединенные Штаты и наши союзники зачастую оказываются поставленными в зависимость от сотрудничества с другими странами и их содействия при расследовании киберпреступлений и привлечении нарушителей к ответственности. Такое сотрудничество наиболее эффективно и содержательно, когда страны имеют схожие законы о преступлениях в киберпространстве, что облегчает совместное использование улик, экстрадицию и другие формы скоординированных действий. Будапештская конвенция по борьбе с преступлениями в киберпространстве дает

странам модель для выработки проектов таких законов и внесения изменений в соответствующее законодательство, и доказала свою эффективность в качестве механизма углубления международного сотрудничества при расследовании киберпреступлений. Соединенные Штаты продолжат поощрение других стран к присоединению к Конвенции и оказание содействие пока не присоединившимся к использованию Конвенции в качестве основы для разработки собственных законов. В краткосрочной перспективе это позволит облегчить двустороннее сотрудничество, а в долгосрочной – подготовит такие страны к присоединению к Конвенции;

- **делать акцент в законах о киберпреступности на борьбе с нелегальной деятельностью, а не на ограничении доступа в Интернет.** Действия преступников в киберпространстве должны наталкиваться на эффективную правоприменительную практику. Здесь нельзя сводить все к политике ограничения законного доступа к Интернету или находящемуся там контенту. Для достижения этой цели правительство Соединенных Штатов работает в рамках двусторонних и многосторонних контактов для обеспечения понимания другими странами того, что акцент в борьбе против онлайн-преступлений должен быть сделан на предупреждении таких деяний, поимке и наказании нарушителей, а не на неизбирательном ограничении доступа к Интернету, поскольку широкое ограничение доступа затрагивает невинных пользователей. В условиях, когда Соединенные Штаты и наши партнеры вовлечены в диалог и содействуют упрочению потенциала в сфере правоприменения по всему миру, мы намерены интегрировать этот подход, объединив защиту неприкосновенности частной жизни, основных свобод и инноваций с сотрудничеством в сфере борьбы с преступлениями в киберпространстве;
- **стремиться лишить террористов и прочих преступников возможности использовать Интернет для планирования операций, их финансирования или проведения атак.** Соединенные Штаты обладают разнообразными международными программами по наращиванию потенциала и обучению по вопросам противодействия киберпреступности. Он могут быть использованы правоохранительными органами и законодателями для разработки эффективных правовых норм и получения компетенций для расследования и преследования лиц, использующих Интернет для террористических или иных преступных целей. Лишение террористов возможностей (тем более их расширения) для найма хакеров и использования организованных преступных инструментов представляет собой важный приоритет для международного сообщества, и решение этой проблемы потребует эффективных законов по киберпреступности. Соединенные Штаты исполнены решимости выявлять и пресекать

работу сетей финансирования террористов и киберпреступников, используя для этого технический инструментарий и структуры международного сотрудничества (к примеру, Международную группу по борьбе с финансовыми злоупотреблениями (FATF).

Военные аспекты: подготовка к решению проблем безопасности XXI века

В силу нашего обязательства по защите наших граждан, союзников и интересов в любой точке, где они окажутся под угрозой, мы:

- **будем учитывать растущие потребности военных в надежных и безопасных сетях, и приспосабливаться к этим потребностям.** Мы осознаем, что наши вооруженные силы во все большей степени зависят от сетей, поддерживающих их работу, и намерены работать над обеспечением того, чтобы наши военные оставались в полной мере оснащенными для проведения операций даже в такой среде, где другие силы могут попытаться нарушить работу систем или иной инфраструктуры, жизненно важных для национальной обороны. Как и все страны, Соединенные Штаты имеют непреходящий интерес в сфере защиты наших жизненно важных активов, равно как и наших базовых принципов и ценностей, и мы обязуемся защищаться от тех, кто попытается ослабить наши возможности в этой области;
- **создадим и усовершенствуем существующие военные союзы для противостояния возможным угрозам в киберпространстве.** Безопасность в киберпространстве не может быть достигнута одной страной в отрыве от других, и потребуется серьезное международное сотрудничество для противодействия лицам, стремящимся нарушить работу наших сетей или использовать их в ненадлежащих целях. Работа в этом направлении начинается с признания того факта, что связанные между собой сетевые системы наших ближайших союзников (к примеру, системы НАТО и стран-членов НАТО) создают как возможности, так и новые риски. Продолжая движение вперед, Соединенные Штаты будут и дальше сотрудничать с военными и гражданскими коллегами наших союзников и партнеров для расширения ситуационной осведомленности и совместного использования систем предупреждения, укрепления наших возможностей для сотрудничества в мирное время и во время кризисов, разработки средств и методов коллективной самообороны в киберпространстве. Такие военные союзы и партнерства будут усиливать наши коллективные возможности в

части сдерживания, равно как и наши возможности в плане защиты Соединенных Штатов от действий со стороны других государств или иных лиц;

- **расширим сотрудничество с союзниками и партнерами в киберпространстве с целью повышения общей безопасности.** Вызовы в сфере киберпространства создают также возможности для совместной работы в новых направлениях с военными союзниками и партнерами. Развивая общее понимание стандартных операционных процедур, наши вооруженные силы способны повышать уровень безопасности посредством координации усилий и более широкого обмена информацией. Эти контакты снижают вероятность ошибочного восприятия оборонной деятельности и возможности для эскалационного поведения. Диалог и обмен передовыми практическими подходами как способ усиления партнерских возможностей (к примеру, цифровые методы судебной экспертизы, развитие персонала, тестирование защиты от несанкционированного доступа в сеть и устойчивости сети) представляются важными в этом плане. Соединенные Штаты будут работать в тесном партнерстве с государствами-единомышленниками для максимально полезного использования всех возможностей, снижения коллективных рисков, содействия многосторонним инициативам с целью сдерживания злоупотреблений в киберпространстве.

Управление Интернетом: продвижение эффективных и всесторонних структур

Для продвижения структур управления Интернетом, эффективно удовлетворяющих нужды всех пользователей Интернета, мы:

- **сделаем упор на открытость и инновации в Интернете.** Возможности для эффективного распространения информации по Интернету лежат в основе современной экономической, политической, научной и образовательной деятельности, а также активности потребителей. Правительства по всему миру признают ценность Интернета, и однако же многие из них накладывают произвольные ограничения на свободные потоки информации или используют подобные меры для подавления деятельности инакомыслящих или оппозиции. В разных странах применяются самые разные методы и формы реализации таких ограничений, равно как и обоснования для этих мер, но мы не должны допустить внесение изменений в структуру управления или технической архитектуры Интернета, если это может упростить осуществление решений, нарушающих основные свободы или излишне затрудняющих инновации.

Эффективное и всестороннее управление Интернетом может помочь в обеспечении того, чтобы действия, грубо нарушающие международные нормы допустимого управления сетями, не облегчались технической структурой или структурой управления. Сохранение, облегчение и расширение доступа к открытому глобальному Интернету являются отчетливым политическим приоритетом. Соединенные Штаты продолжат движение к этим целям в рамках разнообразных контактов, включая работу в соответствующих многосторонних институтах и организациях, а также межправительственных и неправительственных организациях;

- **сохраним безопасность и стабильность глобальной сети, в том числе систему доменных имен (DNS).** Учитывая важность Интернета для мировой экономики, представляется существенным, чтобы эта «Сеть сетей» и лежащая в ее основе инфраструктура (DNS) оставались стабильными и безопасными. Для сохранения и поддержания стабильности и безопасности совершенно необходимо, чтобы США и остальные страны мира и дальше признавали вклад всего спектра заинтересованных сторон, в первую очередь тех организаций и технических экспертов, чья работа жизненно важна для функционирования Интернета. Соединенные Штаты осознают, что эффективная координация этих ресурсов способствовала успеху Интернета, и продолжат поддерживать указанные эффективные многосторонние процессы;

- **будем создавать площадки для многосторонних дискуссий по вопросам управления Интернетом и содействовать работе этих площадок.** Сама архитектура Интернета являет собой модель социальной и технической организации – децентрализованной, скоординированной и многоуровневой. Каждая из этих характеристик фундаментальна с точки зрения преимуществ и выгод Интернета. Такая архитектура питает свободу инноваций, содействующую экономическому росту. Она питает свободу слова и объединений, которые способствуют социальному и политическому развитию и функционированию демократических обществ по всему миру. Соединенные Штаты по-прежнему убеждены в том, что, если международное сообщество проводит заседания с целью обсуждения целого спектра вопросов, связанных с управлением Интернетом, то такие дискуссии должны проводиться с привлечением многих сторон. Мы и дальше будем оказывать поддержку эффективным площадкам, например, Форуму по управлению Интернетом (IGF), который отражает открытую и всестороннюю природу самого Интернета, давая возможность участникам,

не представляющим государства, вносить свой вклад в обсуждение наряду с представителями государств.

Международное развитие: потенциал, безопасность и процветание

Для глобального продвижения преимуществ сетевых технологий, повышения надежности сетей общего пользования и формирования сообщества ответственных участников в киберпространстве мы будем:

- **обеспечивать страны, желающие создать технический потенциал и потенциал в сфере кибербезопасности, необходимыми знаниями, обучением и прочими ресурсами.** Преимущества взаимосвязанного мира не должны ограничиваться национальными границами. Более десяти лет США способствовали ликвидации этого разрыва посредством поддержки разнообразных программ с целью оказания помощи другим странам в получении ресурсов и навыков для формирования базового потенциала в сфере технологий и кибербезопасности. Наша цель – поделиться с другими странами свои опытом, в частности, «встроить» кибербезопасность в общую канву их национального технического развития. С учетом многообразия потребностей, диапазон наших программ варьируется от поддержки национальных возможностей в сфере управления инцидентами и формирования государственно-частного партнерства до повышения уровня безопасности систем управления, выработки проектов эффективных законов расследования киберпреступлений и наказания виновных, а также разработки и осуществления программ по повышению уровня осведомленности и воспитанию культуры в сфере кибербезопасности. Такая работа велась в рамках двусторонних контактов, через программы помощи другим странам, а также через партнерство с инновационными государственно-частными инициативами (к примеру, на базе Американского института повышения квалификации в сфере телекоммуникаций (USTTI)). В последние годы мы сумели сделать эту работу приоритетной для таких форумов, как Организация американских государств (OAS), Организация Тихоокеанского экономического сотрудничества (APEC) и ООН. В ближайшие годы Соединенные Штаты намерены расширять это сотрудничество, работать внутри страны в поддержку инвестиций частного сектора в укрепление потенциала, привлекать внимание к этой исключительно важной потребности и искать новые варианты сотрудничества;

- **неуклонно развивать передовые практические подходы в области международной кибербезопасности и регулярно делиться такими наработками.** В настоящее время странам больше не нужно наращивать потенциал в области кибербезопасности исключительно методом проб и ошибок. Мы располагаем опытом работы с другими странами и множеством многосторонних организаций по разработке и совместному использованию передовых практических подходов, позволяющих государствам делать более взвешенные инвестиции и вырабатывать более эффективные стратегии. Соединенные Штаты продолжат усилия по определению, разработке и усовершенствованию передовых подходов и технических стандартов в сотрудничестве и тесном партнерстве с отраслью. Более того, мы расширим наши усилия для повышения уровня осведомленности и облегчения доступа к таким подходам и стандартам. Мы и дальше будем поддерживать совместные научные исследования и технические разработки с целью совершенствования инструментария и средств для обеспечения кибербезопасности.
- **укреплять возможности государств в плане борьбы с киберпреступностью, в том числе путем обучения правоохранительных органов, судебных специалистов, юристов и законодателей.** Поскольку уголовные дела, касающиеся компьютерных сетей, зачастую связаны с уликами и целями, находящимися по другую сторону океана, правительства регулярно зависят друг от друга в том, что касается технического и следственного содействия (зачастую обширного) по вопросам, затрагивающим национальную безопасность и совершение серьезных преступлений. Угрозы со стороны преступников могут исходить из любой страны, подключенной к Сети, и многие государства нуждаются в существенной помощи в части развития следственного потенциала, необходимого для сотрудничества в рамках указанных выше расследований. Предоставляя обучение по этим вопросам, мы развиваем весьма важные контакты и помогаем овладевать техническими аспектами правоприменительной практики. Такое вовлечение улучшает перспективы эффективного сотрудничества и взаимопомощи в области обеспечения соблюдения законности. Соединенные Штаты продолжат движение к этой цели, предоставляя обучение во многих регионах мира, включая нашу работу в Африке и сотрудничество с Организацией Тихоокеанского экономического сотрудничества, Ассоциацией государств Юго-Восточной Азии, «Большой восьмеркой» и Организацией американских государств;
- **налаживать отношения с лицами, принимающими политические решения, с целью наращивания технического потенциала, обеспечивая постоянные и**

продолжительные контакты с экспертами и их коллегами из правительства Соединенных Штатов. В последние несколько лет развивающееся международное сообщество лиц, принимающих политические решения, вовлеченное в решение вопросов киберпространства, предложило новые направления для диалога, запустило новые инициативы в сфере развития и безопасности и укрепило многочисленные двусторонние контакты. Осуществляя инвестиции в долгосрочное будущее развивающихся стран посредством наращивания технического потенциала и потенциала в сфере кибербезопасности, Соединенные Штаты нацелены на укрепление таких контактов по оказанию помощи до уровня более тесных партнерств по вопросам, представляющим общий интерес. Мы взяли на себя ведущую роль в созыве таких форумов, как, например, Меридианальная конференция, где обсуждаются ключевые вопросы защиты информационной инфраструктуры. США приветствуют тот факт, что все большее число государств присоединяется к диалогу, так как это означает повышение уровня их озабоченности проблемами будущего киберпространства, и мы продолжим работу по укреплению связей между экспертами и лицами, принимающими ключевые решения.

Свобода Интернета: поддержка основных свобод и частной жизни

Для защиты основных свобод и неприкосновенности частной жизни в киберпространстве, мы:

- **будем поддерживать представителей гражданского общества в создании надежных, защищенных и безопасных платформ для свободы слова и объединений.** Мы поощряем использование людьми по всему миру цифровых средств для выражения мнений, распространения информации, контроля выборов, обличения коррупции, организации социальных и политических движений и осуждаем тех, что преследует лиц, применяющих такие технологии, безосновательно арестовывает их, угрожает им или совершает в их отношении акты насилия. Подобная «культура страха» отбивает у других членов сообщества охоту к использованию новых технологий для распространения информации, создания организаций или обмена мыслями. Такие же защитные меры должны распространяться на Интернет-провайдеров и других провайдеров услуг связи, которые точно так же зачастую становятся жертвами правовых норм об опосредованной ответственности, когда

переносят роль цензоров на компании. Соединенные Штаты являются неутомимым поборником основных свобод слова и объединений, осуществляемых, в том числе, через киберпространство. Наша страна будет работать над обеспечением прав деятелей гражданского общества, правозащитников и журналистов на использование цифровых сред. Мы продолжим стимулировать правительства к противодействию угрозам в киберпространстве вместо возложения на компании ответственности с неприемлемым ограничением либо свободы слова, либо свободы информационных потоков;

- **вместе с гражданским обществом и неправительственными организациями, будем работать над мерами по защите их Интернет-активности от незаконных цифровых вторжений.** Повышение кибербезопасности в гражданском обществе и среди неправительственных организаций содействует обеспечению более широкого распространения свободы слова и свободы объединений в цифровую эпоху. Безопасность в киберпространстве особенно важна для активистов, адвокатов и журналистов, находящихся в первых рядах тех, кто может выражать непопулярные мысли и мнения и кто часто становится жертвой взломов ящиков электронной почты, веб-сайтов, мобильных телефонов и систем хранения данных. США поддерживают усилия, направленные на то, чтобы дать таким пользователям возможности защиты, обеспечить им возможность осуществления прав на свободу слова и объединений с использованием новых технологий 21-го века;
- **будем поощрять международное сотрудничество с целью эффективной защиты коммерческих данных.** Защита неприкосновенности частной жизни имеет существенное значение с точки зрения доверия, на котором базируется использование Интернета для экономических и социальных целей. Соединенные Штаты обладают большим опытом применения законов о неприкосновенности частной жизни, равно как и опытом стимулирования выработки политик с участием многих сторон. Мы продолжаем укреплять правовые нормы США о защите коммерческой информации для того, чтобы не отстать от стремительного прогресса сетевых технологий. Мы признаем значимость применения основных принципов неприкосновенности частной жизни в коммерческом контексте при поддержании гибкости, необходимой для инноваций. Соединенные Штаты продолжат усилия для продвижения к общему признанию законов, имеющих одни цели и стимулирующих сотрудничество в сфере правоприменения для защиты частной жизни и поощрения инноваций;
- **обеспечим сквозную совместимость для всеобщей доступности Интернета.** Пользователи должны быть уверенными в том, что информация, которую они

передают в Интернете, будет получена в том виде, как это задумано, причем в любой точке мира. Не менее важным является ожидание, что при нормальных обстоятельствах данные смогут свободно пересекать границы (вне зависимости от происхождения и адресата). Обеспечение целостности информации, передаваемой по Интернету, наполняет пользователей доверием к сети и сохраняет Сеть в качестве открытой платформы для инноваций, питающей рост мировой экономики и стимулирующей обмен идеями между людьми всего мира. Соединенные Штаты продолжат разъяснение преимуществ Интернета, глобального по своей природе, и противодействие расщеплению Всемирной паутины на национальные интрасети, что лишит граждан доступа к контенту из-за рубежа.

IV. Движение вперед

Преимущества и выгоды сетевых технологий не должны оставаться уделом нескольких привилегированных стран или привилегированных слоев населения в этих странах. Однако возможность подключения не слишком ценна сама по себе: она должна поддерживаться киберпространством, открытым для инноваций, обеспечивающим взаимодействие по всему миру, достаточно безопасным для завоевания доверия пользователей и достаточно надежным для поддержания функционирования Сети.

Тридцать лет назад лишь немногие понимали, что нечто под названием «Интернет» совершит революцию, перевернувшую нашу жизнь и работу. За этот короткий срок возникла ситуация, когда средства к существованию (и даже сами жизни) миллионов людей зависят от прогресса сетевых технологий. Еще для миллиарда жителей Земли с Интернетом связаны повседневные формы социального взаимодействия. Эта технология двигает развитие общества вперед, и сейчас стали возможными вещи, о которых предыдущие поколения не могли и помыслить. С нашей стороны, Соединенные Штаты продолжат пробуждать потенциал созидания и творческую фантазию наших людей и граждан других стран мира. Мы не в состоянии предугадать, какой будет следующая великая инновация, но обязуемся содействовать реализации мира, в котором такая инновация могла бы сформироваться и проявить себя во всем блеске.

Настоящая стратегия намечает ориентиры, в соответствии с которыми министерства и ведомства Соединенных Штатов смогут лучше определить и

скоординировать свое место и роль в нашей международной политике в сфере киберпространства, с тем, что бы выбрать конкретный путь движения вперед и спланировать его реализацию. Это призыв к частному сектору, гражданскому обществу и пользователям для умножения усилий через партнерство, повышение осведомленности и конкретные действия. Что еще более важно, это приглашение другим государствам и народам присоединиться к нам в реализации представленного видения процветания, безопасности и открытости нашего сетевого мира. Эти идеалы являются краеугольными для сохранения того киберпространства, которое мы знаем, и для достижения совместными усилиями того будущего, которого мы хотим достичь.

Приложение 2.

Национальная Киберстратегия США 2018 года

НАЦИОНАЛЬНАЯ КИБЕРСТРАТЕГИЯ

Соединенных Штатов Америки

(С е н т я б р ь 2018)9.

БЕЛЫЙ ДОМ
Вашингтон, Округ Колумбия

Мои соотечественники:

Защита национальной безопасности Америки и содействие процветанию американского народа - это мои главные приоритеты. Обеспечение безопасности киберпространства имеет основополагающее значение для обоих направлений. Киберпространство является неотъемлемым компонентом всех сфер жизни Америки, включая нашу экономику и безопасность. При этом наши частные и государственные организации по-прежнему борются за безопасность своих систем, а противники увеличивают частоту и изощренность своей вредоносной кибердеятельности. Америка создала интернет и поделилась им с миром. В настоящее время мы должны приложить все силы для того, чтобы обеспечить безопасность и сохранить киберпространство для будущих поколений.

В течение последних 18 месяцев моя Администрация принимала меры для устранения киберугроз. Мы применили санкции к злостным лицам, действующим в киберпространстве. Мы отдали под суд тех, кто совершил киберпреступления. Мы в публичной форме отнесли это на счет злонамеренной деятельности противоборствующей стороны и опубликовали подробную информацию относительно применяемых при этом инструментов. Мы потребовали, чтобы департаменты и агентства удалили программное обеспечение, уязвимое для различных рисков безопасности. Мы приняли меры к тому, чтобы руководители департаментов и агентств отвечали за управление рисками кибербезопасности в отношении систем, которые они контролируют, одновременно расширяя их права и возможности обеспечивать надлежащую безопасность. Кроме того, в

9 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

прошлом году я подписал Административное распоряжение Президента США (*Executive Order, EO*) 13800 «Об усилении кибербезопасности Федеральных сетей и критической инфраструктуры» («*Strengthening of Federal Networks and Critical Infrastructure*»). Выполненная работа и отчеты, подготовленные в соответствии с этим Приказом, заложили основу для настоящей Национальной Кибер Стратегии (*National Cyber Strategy*).

С опубликованием настоящей Национальной Киберстратегии, Соединенные Штаты теперь имеют свою первую в полной мере четко сформулированную киберстратегию на 15 лет. Настоящая Стратегия объясняет, как моя Администрация будет:

• Защищать Родину, оберегая сети, системы, функциональные элементы и данные;

• Содействовать американскому благоденствию посредством содействия безопасной, процветающей цифровой экономики и стимулирования сильных внутристрановых инноваций;

• Сохранять мир и безопасность посредством укрепления способности Соединенных Штатов – во взаимодействии с союзниками и партнерами – сдерживать и, в случае необходимости, наказывать тех, кто использует кибер-инструменты в злонамеренных целях;

• Увеличивать американское влияние за рубежом с тем, чтобы расширить основополагающие принципы открытого, функционально совместимого, интероперабельного, надежного и безопасного интернета.

Национальная Киберстратегия свидетельствует о моей приверженности укреплению потенциала кибербезопасности Америки и обеспечению защиты Америки от киберугроз. Это призыв к действию для всех американцев и наших великих компаний предпринять необходимые шаги для повышения нашей национальной кибербезопасности. Мы продолжим вести мир в направлении обеспечения процветающего кибер-будущего.

С уважением,
(подпись)
Президент Дональд Дж. Трамп

Белый дом
Сентябрь 2018

Введение

Процветание и безопасность и Америки зависит от того как мы ответим на потенциальные возможности и вызовы в киберпространстве. Критическая инфраструктура, национальная оборона и ежедневная жизнь американцев зависит от компьютерных и взаимосвязанных информационных технологий. В то время, когда все аспекты американской жизни стали более зависимы от защищенного киберпространства, ранее не существовавшие уязвимые стороны стали выявляться, а также новые угрозы не прекращают заявлять о себе. Используя в качестве основы Стратегию Национальной Безопасности, а также успешность деятельности Администрации течение ее первых 18 месяцев, Национальная Киберстратегия обобщенно очерчивает каким образом Соединенные Штаты будут обеспечивать американцам сохранение преимуществ безопасного киберпространства, которое отражает наши принципы, защищает нашу безопасность, а также способствует нашему процветанию.

Как мы оказались в этой ситуации?

Рост влияния интернета и рост первостепенного значения киберпространства в отношении всех аспектов современного мира соответствует росту влияния Соединенных Штатов как единственной сверхдержавы. За последние четверть века изобретательность американцев приводила к дальнейшему развитию киберпространства, что позволило приумножить богатство Соединенных Штатов и, в свою очередь, киберпространство стало фундаментальным для американского повышения благосостояния и инноваций. Киберпространство является неотъемлемым компонентом американской финансовой, социальной, государственной и политической жизни. В то же самое время американцы подчас принимали как данность, что доминирующее положение Соединенных Штатов в киберпространстве остается бесспорным, а также что американское восприятие открытого, функционально совместимого, надежного и безопасного интернета неминуемо станет реальностью.

Американцы считали, что рост интернета повлечет за собой всеобщее стремление к свободе слова и свободе личности во всем мире. Американцы предполагали, что возможности расширения коммуникаций, торговой деятельности и свободного обмена идеями были бы само собой разумеющимися. Значительная часть мира приняла

американское видение совместно используемого и открытого киберпространства для взаимной выгоды всех.

Наши соперники и противники, при этом, приняли противоположный подход. Они извлекают выгоду из открытого интернета, и между тем ограничивают и контролируют доступ своего населения к нему, а также активно подрывают принципы открытого интернета на международных форумах. Они прикрываются понятием суверенитета, несмотря на то, что безответственно нарушают право других государств, участвуя в пагубном экономическом шпионаже и злостной кибердеятельности, причиняя значительный экономический ущерб и вред отдельным лицам, коммерческим и некоммерческим интересам, а также правительствам по всему миру. Они рассматривают киберпространство как арену, где решающая военная, экономическая и политическая сила Соединеных Штатов могла бы быть нейтрализована, а также где Соединеные Штаты и их союзники являются уязвимыми.

Россия, Иран и Северная Корея проводили безответственные кибератаки, которые нанесли ущерб американскому и международному бизнесу, а также нашим союзникам и партнерам без возмещения издержек, способных с большей вероятностью сдержать последующую кибер-агрессию. Китай занимался кибер-поддержкой экономического шпионажа и кражей триллион-долларовой интеллектуальной собственности. Негосударственные акторы, – в том числе террористы и преступники, – использовали киберпространство для получения прибыли, вербовки, пропаганды и нападения на Соединенные Штаты и их союзников и партнеров, причем их деятельность часто находится под защитой недружественных государств. Государственные и частные субъекты всячески пытаются защитить свои системы, поскольку злоумышленники увеличивают частоту и изощренность своей вредоносной кибердеятельности. Организации (хозяйствующие субъекты) на территории Соединенных Штатов сталкиваются с проблемами кибербезопасности в части эффективности соединения, защиты и обеспечения устойчивости своих сетей, систем, функций и данных, также как и с проблемами обнаружения, реагирования и восстановления последствий инцидентов.

Пути дальнейшего развития

Новые угрозы и новая эра стратегической конкуренции требуют новой кибер-стратегии, которая отвечает новым реалиям, ослабляет уязвимости, сдерживает противников и гарантирует возможности для процветания американского народа. Защита киберпространства является фундаментальной для нашей стратегии и требует

технического совершенствования и административной эффективности на уровне всего федерального Правительства и частного сектора. Администрация также признает, что чисто технократический подход к киберпространству недостаточен для решения сути новых проблем, которыми мы противостоим. Соединенные Штаты должны также обладать выбором средств воздействия для того, чтобы заставить платить по счетам, если они надеются противодействовать злонамеренным кибер-субъектам, а также предотвратить дальнейшую эскалацию. Администрация уже предпринимает действия для активного противодействия таким угрозам и приспосабливается к новым реалиям. Соединенные Штаты применили санкции к злостным кибер субъектам, а также предъявили обвинения тем, кто совершил киберпреступления. Мы публично отнесли это на счет злонамеренной деятельности противоборствующей стороны, а также опубликовали подробную информацию об инструментах и инфраструктуре, которые они использовали. Нам нужны отделы и агентства, чтобы удалять программное обеспечение уязвимое для различных рисков безопасности. Мы приняли меры по привлечению руководителей департаментов и учреждений к ответственному управлению рисками кибербезопасности в отношении контролируемых ими систем, при этом наделив их полномочиями по обеспечению надлежащей безопасности.

Подход Администрации к киберпространству основывается на непреходящих американских ценностях, таких как вера в силу свободы личности, свободу слова, свободу рынка и конфиденциальность. Мы сохраняем нашу приверженность увеличению потенциала открытого, функционально совместимого, надежного и безопасного интернета для укрепления и расширения наших ценностных ориентиров, а также для защиты и обеспечения экономической безопасности американских работников и компаний. Будущее, к которому мы стремимся, не придет без обновленных американских целенаправленных усилий в продвижении наших интересов в пределах киберпространства.

Администрация признает, что Соединенные Штаты ведут постоянную конкуренцию со стратегическими противниками, государствами, не признающими международных норм, террористическими и криминальными сетями. Россия, Китай, Иран и Северная Корея всецело используют киберпространство как средство для создания реальной угрозы Соединенным Штатам, их союзникам и партнерам, часто с безрассудством, которое они никогда не проявляли бы в других сферах деятельности. Эти противоборствующие стороны используют кибер-инструменты, чтобы подорвать нашу экономику и демократию, украсть нашу интеллектуальную собственность и посеять раздор в наших демократических процессах. Мы уязвимы перед кибератаками в мирное

время на критическую инфраструктуру, а также растет риск того, что эти страны будут проводить кибератаки против Соединенных Штатов во время кризиса, близкого к войне. Эти противоборствующие стороны постоянно разрабатывают новое и более эффективное кибер-оружие.

Настоящая Национальная Киберстратегия очерчивает в общих чертах, как мы будем (1) защищать Родину посредством защиты сетей, систем, функций и данных; (2) содействовать американскому процветанию стимулируя безопасную, успешно развивающуюся цифровую экономику, а также поддерживать прочные внутренние инновации; (3) сохранять мир и безопасность посредством укрепления способности Соединенных Штатов – совместно с союзниками и партнерами – сдерживать и, если необходимо, привлекать к ответственности тех, кто использует кибер-инструменты в злонамеренных целях; и (4) расширять американское влияние в целом, для того, чтобы распространить основополагающие принципы открытого, функционально совместимого, надежного и безопасного интернета.

Успех Стратегии будет реализован, в том случае, если уязвимости кибербезопасности будут эффективно устраняться путем идентификации и защиты сетей, систем, функций и данных, также как и выявлением, обеспечением устойчивости, реагирования и восстановления после инцидентов; деструктивная и разрушительная или иным образом дестабилизирующая злонамеренная кибер-деятельность, направленная против интересов Соединенных Штатов будет сокращена или предотвращена; деятельность, которая противоречит ответственному поведению в киберпространстве будет сдерживаться возложением дополнительных издержек посредством кибер и не-кибер-средств; а также если Соединенные Штаты сориентируют использование кибер-возможностей для достижения целей национальной безопасности.

Формулирование Национальной Киберстратегии подготовлено в соответствии с основополагающими элементами Стратегии Национальной Безопасности (*National Security Strategy*). Штатные сотрудники Совета национальной безопасности (*National Security Council*) будут взаимодействовать с департаментами, агентствами, а также Административно-бюджетным Управление [при Президенте США] (*Office of Management and Budget, OMB*) в отношении соответствующего плана распределения ресурсов для реализации настоящей Стратегии. Департаменты и агентства будут осуществлять свои главные цели деятельности основываясь на нижеследующих стратегических директивных положениях.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ I

Защищать американский народ, Отечество и американский образ жизни

Защита американского народа, американского образа жизни и американских интересов является приоритетной задачей Стратегии Национальной Безопасности (*National Security Strategy*). Защита американских информационных сетей, будь то государственные, или частные является жизненно важным для достижения этой цели. Это требует ряда скоординированных действий, направленных на защиту правительственных сетей, защиту критической инфраструктуры, а также на борьбу с киберпреступностью. Правительство Соединенных Штатов, частный сектор и общественность каждый должны предпринять немедленные и решительные действия для укрепления кибербезопасности, при этом каждый, работая на обеспечение безопасности сетей находящихся под их контролем, при необходимости, поддерживает друг друга.

ЦЕЛЬ: Управлять рисками кибербезопасности для повышения защиты и устойчивости информации граждан США и информационных систем.

Обеспечивать безопасность Федеральных сетей и информации

Ответственность за безопасность федеральных сетей, – в том числе федеральные информационные системы и системы национальной безопасности, – полностью ложится на федеральное Правительство. Администрация уточнит соответствующие ведомства, сферы ответственности, функциональные обязанности и подотчетность внутри и между департаментами и агентствами для обеспечения безопасности федеральных информационных систем, одновременно установив стандарт эффективного управления рисками кибербезопасности. В рамках этих усилий Администрация сосредоточит некоторые полномочные органы в системе федерального Правительства, обеспечит лучшую межведомственную прозрачность, улучшит управление нашей федеральной цепочкой поставок, а также повысит безопасность системы подрядчиков Правительства США.

Приоритетные Действия

ДАЛЬНЕЙШАЯ ЦЕНТРАЛИЗАЦИЯ УПРАВЛЕНИЯ И НАДЗОР ЗА ФЕДЕРАЛЬНОЙ ГРАЖДАНСКОЙ КИБЕРБЕЗОПАСНОСТЬЮ: Администрация будет действовать с тем, чтобы в дальнейшем Министерство внутренней безопасности (*Department of Homeland Security, DHS*) могло обеспечить безопасность сетей

федеральных департаментов и агентств, за исключением систем национальной безопасности и систем Министерства обороны *(Department of Defense, DOD*), а также разведывательных ведомств (*Intelligence Community,IC*). Это включает обеспечение соовтетствующего доступа Министерства внутренней безопасности, DHS, к информационным системам агентства в целях кибербезопасности, а также принятие и бысрое реагирование для защиты систем от разнообразных рисков. Под надзором Административно-бюджетного Управления, OMB, Администрация расширит работу, начатую в соответствии с Административным распоряжением Президента США, EO, 13800, чтобы уделить первоочередное внимание переходу учреждений к распределению услуг и инфраструктуры. Министерство внутренней безопасности, DHS, будет иметь надлежащую доступность для осмотра этих услуг и инфраструктуры для улучшения состояния кибербезопасности Соединеных Штатов. Мы будем продолжать развертывать возможности, централизации, инструменты и услуги посредством Министерства внутренней безопасности, DHS, когда это целесообразно, а также улучшать надзор и соблюдение применимого права, политики, стандартов и директив. Это, вероятно, потребует новой политики и архитектуры, которые позволят Правительству улучшить уровень использования инноваций. Министерство обороны, DOD, а также разведывательные ведомства, IC, рассмотрят такие ти действия, поскольку они работают для того, чтобы лучше защитить системы национальной безопасности, системы Министерства обороны, DOD, а также системы разведывательных ведомств, IC, в зависимости от ситуации.

СОГЛАСОВЫВАТЬ УПРАВЛЕНИЕ РИСКАМИ И ДЕЯТЕЛЬНОСТЬЮ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: Административное распоряжение, EO, 13833 Усиление эффективности работы главных сотрудников информационной службы агентства (*Agency Chief Information Officers*) наделяет полномочиями главных сотрудников информационной службы (*Chief Information Officers, CIOs*) более эффективно задействовать технологии для осуществления главных задач агентства, сократить дублирование, а также сделать инвестиций в информационные технологии (IT) более эффективными. Руководители департаментов и агентств будут наделять полномочиями и возлагать на своих Главных сотрудников информационной службы, CIOs, ответственность за согласование решений по системе управления рисками, а также решений по IT-бюджетированию и поставкам. Администрация через Административно-бюджетное Управление, OMB, и Министерство внутренней безопасности, DHS, будет продолжать руководить и направлять действия по управлению рисками Федеральных

гражданских департаментов и агентств, а Главные сотрудники информационной службы, CIOs, будут наделены полномочиями играть ведущую инициативную роль в обеспечении того, чтобы решения по IT-поставкам придавали надлежащий приоритет защите сетей и данных.

СОВЕРШЕНСТВОВАТЬ УПРАВЛЕНИЕ РИСКАМИ ФЕДЕРАЛЬНОЙ СИСТЕМЫ СНАБЖЕНЧЕСКИХ ЦЕПОЧЕК: Администрация объединит управление рисками снабженческих цепочек в службу закупок и процесса управления рисками в соответствии с федеральными требованиями, которые соответствует лучшими отраслевым практикам, чтобы лучше обеспечить безопасность и надежность технологий, которые федеральные Правительство разворачивает. Это охватывает обеспечение лучшего обмена информацией между департаментами и агентствами для того, чтобы повысить осведомленность относительно угроз снабженческих цепочек и сократить дублирование действий в снабженческих цепочках в Правительстве Соединеных Штатов, в том числе созданием совместной службы оценки рисков снабженческих цепочек. Это также охватывает устранение недостатков в федеральной системе государственных закупок, таких как предоставление более упорядоченных полномочий для исключения рискованных поставщиков, продуктов и услуг, в тех случаях, когда это оправдано. Эти усилия будут синхронизированы с усилиями по управлению рисками снабженческих цепочек в инфраструктуре США.

УСИЛИВАТЬ КИБЕРБЕЗОПАСНОСТЬ ФЕДЕРАЛЬНОГО ПОДРЯДЧИКА: Соединенные Штаты не могут позволить себе обладать информацией, составляющей государственную тайну или системы, ненадлежащим образом защищенные подрядчиками. Федеральные подрядчики предоставляют важные услуги Правительству Соединенных Штатов и должны надлежащий образом защищать системы, с помощью которых они предоставляют такие услуги. В перспективе Правительство сможет оценить защищенность их данных посредством проверки практик управления рисками подрядчика, а также адекватного тестирования, поиска, обнаружения и реагирования на инциденты в системах подрядчиков. Контракты с федеральными департаментами и агентствами разработаны для того, чтобы санкционировать такого рода деятельность в целях усиления кибербезопасности. Среди критических проблемных вопросов в этой области находятся те поставщики оборонно-промышленной базы, ответственные за исследования и разработку ключевых систем, принимаемых на вооружение Министерством обороны, DOD. В свою очередь, как рекомендовано в Административном распоряжении Президента США, EO, 13800, *Доклада Президенту по Федеральной IT*

модернизации, Администрация будет поддерживать принятие согласованных стратегий государственных закупок

для улучшения кибербезопасности и сокращения накладных расходов, связанных с использованием несовместимых контрактных условий через Федеральное Правительство. Она будет также обеспечивать, когда это необходимо, чтобы федеральные подрядчики получали и использовали всю соответствующую и совместно используемую информацию угроз и уязвимостей для того, чтобы усилить свое состояние защищености.

ОБЕСПЕЧИВАТЬ ЛИДИРУЮЩИЕ ПОЗИЦИИ ПРАВИТЕЛЬСТВА ПО ЛУЧШИМ И ИННОВАЦИОННЫМ ПРАКТИКАМ: Федеральное Правительство обеспечит соответствие систем и операций, которыми она владеет и управляет, стандартам и лучшим практикам кибербезопасности, которые рекомендованы отрасли. Проекты, которые получают федеральное финансирование, должны также соответствовать таким стандартам. Федеральное правительство будет использовать свою покупательную способность для того, чтобы управлять общесекторальным усовершенствованием продуктов и услуг. Федеральное Правительство будет также лидером в разработке и внедрении стандартов и лучших практик в новых и развивающихся областях. К примеру, криптография с открытым ключом является основополагающей для безопасной работы нашей инфраструктуры. Для защиты от потенциальной угрозы того, что квантовые компьютеры могут взломать современную криптографию с открытым ключом, Министерство торговли (*Department of Commerce*) через Национальный институт стандартов и технологий (*National Institute of Standards and Technology,* NIST) будет продолжать запрашивать, оценивать и стандартизировать открытый ключ квантово-устойчивых криптографических алгоритмов. Соединенные Штаты должны быть на переднем крае защиты коммуникаций, поддерживая быстрое принятие таких будущих стандартов Национального института стандартов и технологий, NIST, в рамках Правительственной инфраструктуры, а также содействуя нашей стране делать то же самое.

Защищать Критическую Инфраструктуру

Обязанность обеспечить безопасность критической инфраструктуры США и управлять своим риском кибербезопасности является общей для частного сектора и Федерального Правительства. Мы будем параллельно использовать подход, ориентированный на последствия, для того, чтобы расставить приоритеты в действиях, которые сокращают вероятность того, что самые продвинутые противоборствующие

стороны могут вызвать крупномасштабную или долговременную дестабилизацию критической инфраструктуры. Мы будем также сдерживать злонамеренных кибер-субъектов, возлагая на них и их спонсоров издержки, посредством максимального использования целого ряда инструментов, включая, но не ограничиваясь, судебное преследование и экономические санкции, как часть более широкой стратегии сдерживания.

Приоритетные Действия

СОВЕРШЕНСТВОВАТЬ РАСПРЕДЕЛЕНИЕ ФУНКЦИЙ И СФЕР ОТВЕТСТВЕННОСТИ: Администрация уточнит распределение функций и сфер ответственности Федеральных агентств и ожидания частного сектора в отношении управления рисками кибербезопасности и реагирования на инциденты. Уточнение позволит действовать на опережение в управлении рисками, которое исчерпывающим образом решит вопросы угроз, уязвимостей и последствий. Это также выявит и устранит существующие пробелы в обязанностях и взаимодействии между Федеральными и не-федеральными усилиями реагирования на инциденты, а также будет способствовать более регулярным тренировкам, учениям и координации.

РАССТАВИТЬ ПРИОРИТЕТЫ ДЕЙСТВИЙ В ЗАВИСИМОСТИ ОТ ХАРАКТЕРА ИДЕНТИФИЦИРОВАННЫХ НАЦИОНАЛЬНЫХ РИСКОВ: Федеральное Правительство будет работать с частным сектором для того, чтобы управлять рисками в критической инфраструктуре наибольших рисков. Администрация разработает комплексное понимание национального риска посредством определения национальных критических функции и будет совершенствовать наших предложения и обязательства по кибербезопасности для того, чтобы более эффективно управлять такими национальными рисками. Администрация буде придавать первостепенное значение деятельности по снижению степени риска в семи ключевых сферах: национальная безопасность, энергетика и электроэнергетика, банковское дело и финансы, охрана труда и здравоохранения, коммуникации, информационные технологии и транспорт.

ПРИВЛЕКАТЬ ПРОВАЙДЕРОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАК ПОСРЕДНИКОВ КИБЕРБЕЗОПАСНОСТИ: Информационные и коммуникационные технологии (ИКТ) положены в основу каждого сектора в Америке. Провайдеры ИКТ обладают уникальной возможностью выявлять, предотвращать и снижать риски до того, как они повлияют на их клиентов, и Федеральное Правительство должно работать с такими провайдерами, чтобы

повышать безопасность и устойчивость ИКТ целенаправленным и эффективным способом, защищая при этом конфиденциальность и гражданские свободы. Правительство Соединенных Штатов увеличит усилия по обмену информацией с провайдерами ИКТ, чтобы они могли реагировать и устранять известную вредоносную кибер-деятельность на сетевом уровне. Это будет охватывать обмен систематизированными угрозами и сведениями об уязвимостях с проверенными ИКТ операторами, а также понизить статус информации до несекретного уровня насколько это возможно. Мы будем продвигать адаптируемые, долгосрочные и защищенные технологические снабженческих цепочки которые поддерживают безопасность на основе лучших практик и стандартов. Правительство Соединенных Штатов соберет заинтересованные стороны для разработки межотраслевых решений проблем на уровне сети, устройств и шлюзов, а также мы будем поощрять отраслевые режимы сертификации, которые гарантируют, что решения могут адаптироваться к быстро меняющемуся рынку и ландшафту угроз.

ЗАЩИТЩАТЬ НАШУ ДЕМОКРАТИЮ: Обеспечение наших демократических процессов имеет первостепенное значение для Соединенных Штатов и наших демократических союзников. Федерация и чиновники штатов владеют и управляют разнообразной избирательной инфраструктурой в пределах Соединенных Штатов. Соответственно по запросу мы будем предоставлять технические услуги и услуги по управлению рисками, поддерживать обучение и тренировки, поддерживать ситуационную осведомленность относительно угроз в этом секторе, а также улучшать обмен разведданных об угрозах безопасности угрозах этими должностными лицами, чтобы лучше подготовить и защитить инфраструктуру выборов. Федеральное Правительство будет продолжать координировать разработку стандартов и руководящих положений по кибербезопасности для защиты избирательного процесса и инструментов, обеспечивающих защиту системы. В случае значительного кибер-инцидента Федеральное Правительство проявляет готовность обеспечить отражение угроз и средства ответа на восстановление избирательной инфраструктуры.

СОЗДАВАТЬ БЛАГОПРИЯТНЫЕ УСЛОВИЯ ДЛЯ ИНВЕСТИЦИЙ В КИБЕРБЕЗОПАСНОСТЬ: Большинство рисков кибербезопасности для критической инфраструктуры обусловлены использованием общепризнанных уязвимостей. Правительство Соединенных Штатов будет работать с субъекты частного и государственного сектора для того, чтобы способствовать пониманию риска кибербезопасности, с тем, чтобы они принимали более обоснованные решения по

управлению рисками, инвестировали средства в соответствующие меры безопасности и получали выгоды от таких инвестиций.

РАССТАВИТЬ ПРИОРИТЕТЫ НАЦИОНАЛЬНЫХ ИССЛЕДОВАНИЙ И РАЗВИТИЯ ИНВЕСТИЦИЙ: Федеральное Правительство обновит Национальный план исследований и разработок в сфере безопасности и устойчивости критической инфраструктуры, (*National Critical Infrastructure Security and Resilience Research and Development Plan*) для того, чтобы определить устранения рисков кибербезопасности для критической инфраструктуры. Департаменты и агентства будут согласовывать свои инвестиции с приоритетами, сфокусированные на создании новых подходов кибербезопасности, которые используют новые технологии, улучшая обмен информацией и управление рисками, относящиеся к межотраслевой взаимозависимости и повышая устойчивость при крупномасштабной или длительной дестабилизации.

УЛУЧШАТЬ ТРАНСПОРТНУЮ И МОРСКУЮ КИБЕРБЕЗОПАСНОСТЬ: Экономическая и национальная безопасность Америки строится на глобальной торговле и транспорте. Наша способность гарантировать бесплатно и своевременно движение товаров, открытых морских и воздушных линий коммуникаций, доступ к нефти и природному газу, и наличие связанных критических инфраструктур жизненно важн*о* для нашей экономической и национальной безопасности. По мере модернизации этих секторов они также становятся более уязвимыми для кибер-использования или атак. Морская кибербезопасность вызывает особую озабоченность, потому что потерянные или задержанные поставки могут привести к стратегическим сбоям в экономике и потенциальному побочному эффекту для потребительских отраслей. Принимая во внимание критичность морских перевозок в Соединенные Штаты и мировую экономику, а также минимальные инвестиции в снижение рисков для защиты от кибер-эксплуатации, сделанные до сих пор, Соединенные Штаты быстро перейдут к тому, чтобы уточнить роли и ответственности морской кибербезопасности; содействовать укреплению механизмов международного взаимодействия и обмена информацией; и ускорят развитие кибер-устойчивой морской инфраструктуры нового поколения. Соединенные Штаты будут обеспечивать бесперебойную перевозку грузов перед лицом всех угроз, которые могут подвергать эту, по своей сути международную инфраструктуру, в опасности с помощью кибер-средств.

УЛУЧШАТЬ КОСМИЧЕСКУЮ КИБЕРБЕЗОПАСНОСТЬ: Соединенные Штаты считают, что беспрепятственный доступ и свобода действий в космосе имеют

жизненно важное значение для развития безопасности, экономического процветания и научных знаний нашей страны. Администрация обеспокоена растущими кибер-угрозами, относящимися к космическим активам и поддерживающей инфраструктуре, поскольку такие активы имеют решающее значение для таких функций, как определение местоположения, навигация и синхронизация (*positioning, navigation, and timing*, PNT); разведка, наблюдение и разведка (*intelligence, surveillance, and reconnaissance* ISR); спутниковая связь; и мониторинг погоды. Администрация будет наращивать усилия по защите наших космических активов и вспомогательной инфраструктуры от развивающихся киберугроз, и мы будем работать с отраслевыми и международными партнерами для повышения киберзащищенности существующих и будущих космических систем.

Бороться с киберпреступностью и улучшать отчетности об инцидентах

Федеральные департаменты и агентства, в сотрудничестве с государством, местными, этническими и территориальными государственными органами играют важную роль в обнаружении, предотвращении, устранении и расследовании киберугроз для нашей страны. Соединенные Штаты регулярно становятся жертвами злонамеренной кибер-активности, совершаемой преступными субъектами, в том числе государственными и негосударственными субъектами, а также их доверенными лицами и террористами, использующими сетевую инфраструктуру в Соединенных Штатах и за рубежом. Федеральные правоохранительные органы занимаются задержанием и судебным преследованием правонарушителей, отключением криминальной инфраструктуры, ограничением распространения и использования безнравственных кибер-возможностей, предотвращением киберпреступников и их спонсоров от получения прибыли от их незаконной деятельности и захватом их активов. Администрация будет стремиться к тому, чтобы наши Федеральные департаменты и агентства имели необходимые юридические полномочия и ресурсы для борьбы с транснациональной киберпреступностью, включая выявление и демонтаж ботнетов, черных рынков и другой инфраструктуры, используемой для обеспечения киберпреступности, и борьбу с экономическим шпионажем. Для того, чтобы эффективно сдерживать, выявлять и предотвращать киберугрозы, правоохранительные органы будут работать с частным сектором, чтобы противостоять вызовам, связанным с технологическими барьерами, такими как технологии анонимизации и шифрования, для получения чувствительных ко времени доказательств согласно надлежащему юридическому процессу. Действия правоохранительных органов

по борьбе с преступной кибер-активностью служат инструментом национальной власти, среди прочего, посредством сдерживания такой деятельности.

Приоритетные Действия

УЛУЧШАТЬ ОТЧЕТНОСТЬ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ: Правительство Соединенных Штатов продолжит поощрять сообщения о вторжениях и кражах данных всех жертв, особенно партнеров критической инфраструктуры. Оперативное информирование Федерального Правительства о кибер-инцидентах имеет важное значение для эффективного реагирования, установления связи между соответствующими инцидентами, установления личности преступников, а также предотвращения будущих инцидентов.

УЛУЧШИТЬ ЭЛЕКТРОННЫЙ НАДЗОР И ПРАВО О КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЯХ: Администрация будет работать с Конгрессом над обновлением свода законов об электронном наблюдения и компьютерных преступлениях с тем, чтобы расширить возможности правоохранительных органов по правомерному сбору необходимых доказательств преступленной деятельности, разрушать криминальную инфраструктуру посредством гражданских судебных запретов и возложения соответствующих мер воздействия для злостных кибер-субъектов.

СНИЖАТЬ УГРОЗЫ ОТ ТРАНСНАЦИОНАЛЬНЫХ ПРЕСТУПНЫХ ОРГАНИЗАЦИЙ В КИБЕРПРОСТРАНСТВЕ: Компьютерный взлом ведущийся транснациональными криминальными группировками представляет значительную угрозу для нашей национальной безопасности. Располагая значительными средствами, организованные преступные группировки действуют за рубежом используя сложное вредоносное программное обеспечение, фишинговые кампании и иные хакерские инструменты — некоторые из которых конкурируют с национальными государствами в изощренности — для того, чтобы взламывать чувствительные финансовые системы, осуществлять массовые нарушения данных, распространять вирусы-вымогатели, атаковать критическую инфраструктуру и красть интеллектуальную собственность. Администрация будет добиваться того, чтобы правоохранительные органы располагали эффективными правовыми инструментами для расследования и судебного преследования таких группировок, а также совершенствовать свод законов об организованной преступности для его использования против такой угрозы.

УЛУЧШАТЬ ЗАДЕРЖАНИЕ ПРЕСТУПНИКОВ, НАХОДЯЩИХСЯ ЗА РУБЕЖОМ: Сдерживание киберпреступности требует достоверной вероятности того, что преступники будут выявлены, задержаны и привлечены к ответственности. Однако, некоторые иностранные государства предпочитают не сотрудничать с запросами об экстрадиции, налагать необоснованные ограничения или активно вмешиваться в такие усилия. Соединенные Штаты будут продолжать выявлять пробелы и потенциальные механизмы привлечения к суду иностранных киберпреступников. Правительство Соединенных Штатов также активизирует дипломатические и иные усилия со странами по продвижению сотрудничества по законным запросам об экстрадиции. Мы будем настаивать на том, чтобы другие страны ускорили свою помощь в проведении расследований и выполняли любые двусторонние или многосторонние соглашения или обязательства.

УКРЕПЛЯТЬ ПОТЕНЦИАЛ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ СТРАН-ПАРТНЕРОВ В БОРЬБЕ С ПРЕСТУПНОЙ КИБЕР-ДЕЯТЕЛЬНОСТЬЮ: Соединенные Штаты также должны помочь странам-партнерам укрепить свой потенциал в борьбе с преступной кибер-деятельностью. Безграничная природа киберпреступности, в том числе спонсируемой государством, и террористическая деятельность, требует прочного международного правоприменительного сотрудничества. Такое сотрудничество требует требует, чтобы иностранные правоохранительные органы располагали техническим потенциалом для оказания эффективной помощи правоохранительным органам Соединенных Штатов в случае поступления соответствующего запроса. Это, следовательно, в интересах национальной безопасности Соединенных Штатов продолжать наращивать потенциал борьбы с киберпреступностью, способствующий укреплению международного сотрудничества в правоохранительной сфере.

Соединенные Штаты будут стремиться к улучшению международного сотрудничества в расследовании злонамеренной кибер-деятельности,в том числе разработку решений потенциальных барьеров для сбора и обмена доказательствами. Соединенные Штаты будут также возглавлять разработки совместимых и взаимовыгодных систем для поощрения эффективного трансграничного обмена информацией в правоохранительных целях и снятия барьеров для координации. Администрация будет призывать к эффективному использованию международных инструментов, таких как Конвенция Организации Объединенных Наций против транснациональной организованной преступности (*United Nations Convention Against*

Transnational Organized Crime) и Сетевые Контактные Пункты G7 24/7 (*Network Points of Contact G7 24/7*). Наконец, мы будем работать над расширением международного консенсуса в пользу Конвенции о киберпреступности Совета Европы (Будапештская конвенция), в том числе путем поддержки более широкого участия в этой Конвенции.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ II

Содействовать американскому процветанию

Интернет принес гигантские преимущества выгоды как внутри страны, так и за рубежом, и это помогает продвигать американские ценности свободы, безопасности и процветания. Наряду с его расширением появились вызовы, которые угрожают нашей национальной безопасности. Соединенные Штаты будут демонстрировать последовательный и всеобъемлющий подход к решению этих и других задач по защите американских национальных интересов в этом все более оцифрованном мире.

Интернет породил огромные преимущества внутри страны и широкий, и это помогает продвигать американские ценности свободы, безопасности и процветания. Наряду с его расширением появились проблемы, которые угрожают нашей национальной безопасности.

ЦЕЛЬ: Сохранить влияние Соединенных Штатов в технологической экосистеме и развивать киберпространство как открытого двигателя экономического роста, инноваций и эффективности.

Способствовать развитию жизнеспособной и устойчивой цифровой экономике

Экономическая безопасность неразрывно связана с нашей национальной безопасностью. По мере того как основы нашей экономики все в большей степени основываются на цифровых технологиях, Правительство Соединенных Штатов будет разрабатывать и продвигать стандарты, которые защищают нашу экономическую безопасность и укрепляют жизнеспособность американского рынка и американских инноваций.

Приоритетные Действия

СТИМУЛИРОВАТЬ ГИБКУЮ И ЗАЩИЩЕННУЮ ТЕХНОЛОГИЧЕСКУЮ ТОРГОВУЮ ПЛОЩАДКУ: Для повышения устойчивости киберпространства Администрация ожидает, что технологические площадки будут поддерживать и поощрять непрерывное развитие, внедрение и эволюцию инновационных технологий и процессов безопасности. Администрация будет работать с группами стейкхолдеров/заинтересованных сторон, включая частный сектор и гражданское общество, в целях пропаганды лучших практик и разработки стратегий для преодоления рыночных барьеров на пути внедрения безопасных технологий. Администрация улучшит

осведомленность и транспарентность практики кибербезопасности для создания рыночного спроса на более безопасные продукты и услуги. Наконец, Администрация будет сотрудничать с международными партнерами в целях содействия открытым отраслевым стандартам с государственной поддержкой, в соответствующих случаях, а также основываясь на риск-ориентированных подходах при решении вызовов кибербезопасности, включая основания и подходы управления услуг, которые снижают барьеры защиты практики внедрения в масштабах всей экосистемы.

ОПРЕДЕЛЯТЬ ПРИОРИТЕТ ИННОВАЦИЙ: Правительство Соединенных Штатов будет содействовать внедрению и постоянному обновлению стандартов и лучших практик, которые сдерживают и предотвращают существующие и развивающиеся угрозы и опасности во всех сферах кибер-экосистемы. Такие стандарты и практики должны быть ориентированы на результат, а также основываться в большей мере на надежных технологических принципах, а не на нынешние спецификации компании. Администрация будет устранять политические барьеры, которые мешают устойчивой индустрии кибербезопасности развивать, обмениваться и создавать инновационные возможности для снижения киберугроз.

ИНВЕСТИРОВАТЬ В ИНФРАСТРУКТУРУ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ: Администрация будет способствовать ускоренной разработке и внедрению следующего поколения телекоммуникационной и информационно-коммуникационной инфраструктуре здесь, в Соединенных Штатах, используя покупательную способность, Федеральное Правительство должно стимулировать переход к более безопасным снабженческим цепочкам. Правительство Соединенных Штатов будет сотрудничать с частным сектором в целях содействия развитию и безопасности 5G, изучения технологических и спектрально-основанных решений, а также создания основы для инноваций, выходящих за рамки достижений следующего поколения. Правительство Соединенных Штатов Америки изучит использование новейших технологий, таких как искусственный интеллект и квантовые вычисления, при решении проблем рисков, присущих их использованию и применению. Мы будем сотрудничать с частным сектором и гражданскими обществом, чтобы понять тенденции в технологии прогресса для поддержания Соединенных Штатов технологического преимущества в связанных технологиях, и обеспечивать принятие безопасных методов изначально.

СОДЕЙСТВОВАТЬ СВОБОДНОМУ ДВИЖЕНИЮ ПОТОКА ДАННЫХ ЧЕРЕЗ ГРАНИЦЫ: Страны все чаще предусматривают ограничительные положения о

локализации данных и нормативные акты в качестве оправдания для цифрового протекционизма подводя под категорию национальной безопасности. Такие действия отрицательно сказываются на конкурентоспособности Компании Штатов. Соединенные Штаты будут и впредь подавать пример и бороться с неоправданными барьерами на пути свободного потока данных и цифровой торговли. Администрация будет продолжать сотрудничать с международными партнерами в целях поощрения открытых отраслевых стандартов, инновационных продуктов и подходов, основанных на учете факторов риска, которые позволяют осуществлять глобальные инновации и свободный поток данных при одновременном удовлетворении законных потребностей Соединенных Штатов в сфере безопасности.

ПОДДЕРЖИВАТЬ ЛИДЕРСТВО СОЕДИНЕННЫХ ШТАТОВ В ПЕРЕДОВЫХ ТЕХНОЛОГИЯХ: Влияние Соединеных Штатов в киберпространстве связано с нашим технологическим лидерством. Соответственно, Правительство Соединенных Штатов предпримет согласованные усилия для защиты передовых технологий, в том числе от кражи со стороны наших противников, будет поддерживать полное развитие таких технологий и, где это возможно, уменьшит барьеры для выхода американских компаний на рынки. Соединенные Штаты будут продвигать инновации Соединенных Штатов в области кибербезопасности во всем мире посредством вовлечения в торговую деятельность, повышения осведомленности об инновационных американских инструментах и услугах в области кибербезопасности, разоблачения и противодействия репрессивным режимам, использующим такие инструменты и услуги для подрыва прав человека, и сокращения и барьеров на пути устойчивого глобального рынка кибербезопасности.

СОДЕЙСТВОВАТЬ ПОЛНОМУ ЖИЗНЕННОМУ ЦИКЛУ КИБЕРБЕЗОПАСНОСТИ: Правительство Соединеных Штатов будет содействовать полному жизненному циклу кибербезопасности, настаивая на сильных настройках безопасности по умолчанию, адаптируемых, обновляемых продуктах и иных лучших практиках, присущих периоду поставки продукта. Мы наметим четкий путь к адаптируемому, устойчивому и безопасному технологическому рынку, поощряя производителей дифференцировать продукты в зависимости от качества их функций безопасности. Правительство Соединенных Штатов будет поощрять основополагающую инженерную практику в целях снижения системной нестабильности системы и разрабатывать проекты, которые при успешном нападении приводят к деградации, но и эффективно восстанавливаются. Правительство Соединенных Штатов будет также

содействовать регулярному тестированию и проверке кибербезопасности и устойчивости продуктов и систем во время разработки с использованием лучших практик, ориентированных на передовые отрасли. Это охватывает содействие и использование скоординированного раскрытия уязвимостей, краудсорсинга, тестирования и иных инновационных оценок, которые повышают устойчивость перед эксплуатацией или атакой. Правительство Соединенных Штатов также оценит, как улучшить сквозной жизненный цикл управления цифровыми идентификационными данными, включая чрезмерную зависимость от номеров социального страхования.

Поощрять и обеспечивать изобретательность Соединенных Штатов

Поощрение и защита американской изобретательности и инноваций имеют решающее значение для поддержания стратегического преимущества Штатов в киберпространстве. Правительство Соединенных Штатов будет поощрять инновации, продвигая институты и программы, которые стимулируют конкурентоспособность Соединенных Штатов. Правительство Соединенных Штатов будет бороться с захватническими слияниями и поглощениями, а также против кражи интеллектуальной собственности. Мы также будем стимулировать лидерство Соединенных Штатов в новых технологиях и содействовать правительственной идентификации и поддержке этих технологий, которые охватывают искусственный интеллект, квантовую информационную науку и следующее поколение телекоммуникационной инфраструктуры.

Приоритетные Действия

ОБНОВЛЯТЬ МЕХАНИЗМЫ ОБЗОРА ИНОСТРАННЫХ ИНВЕСТИЦИИ И ДЕЯТЕЛЬНОСТИ В СОЕДИНЕННЫХ ШТАТАХ: Конфиденциальность, целостность и доступность телекоммуникационных сетей Соединенных Штатов имеют важное значение для нашей экономики и национальной безопасности. Мы должны быть бдительными, чтобы защищать телекоммуникационные сети, от которых мы зависим в нашей повседневной жизни, чтобы они не могли быть использованы или скомпрометированы иностранным противником, чтобы нанести ущерб Соединенным Штатам. Правительство Соединенных Штатов будет уравновешивать эти цели, формализуя и упорядочивая рассмотрение обращений Федеральной Комиссии по коммуникациям (*Federal Communications Commission*) для рекомендаций лицензий по телекоммуникациям. Правительство США будет содействовать транспарентному процессу повышения эффективности такого обзора.

ПОДДЕРЖИВАТЬ СИЛЬНУЮ И СБАЛАНСИРОВАННУЮ СИСТЕМУ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ: Надежная защита интеллектуальной собственности обеспечивает непрерывный экономический рост и инновации в эпоху цифровых технологий. Правительство Соединенных Штатов способствовало и будет продолжать содействовать развитию глобального системе прав интеллектуальной собственности, которая обеспечивает стимулы для инноваций посредством охраны и защиты прав интеллектуальной собственности, таких как патенты, товарные знаки и авторские права. Правительство Соединенных Штатов будет также содействовать защите чувствительных новых технологий и коммерческой тайны, и мы будем работать над тем, чтобы не допустить получения противоборствующими государствами несправедливого преимущества в ущерб американским исследованиям и разработкам.

ЗАЩИЩАТЬ КОНФИДЕНЦИАЛЬНОСТЬ И ЦЕЛОСТНОСТЬ АМЕРИКАНСКИХ ИДЕЙ: Уже более десяти лет злоумышленники совершают кибер-вторжения в коммерческие сети Соединенных Штатов, нацеленные на конфиденциальную деловую информацию, которой владеют американские фирмы. Вредоносные кибер-субъекты из других стран похищают несметное число торговых секретов, технических данных и конфиденциальные частные внутренние сообщения. Правительство Соединенных Штатов будет бороться с незаконным присвоением технологий и технических знаний в государственном и частном секторах иностранными конкурентами, сохраняя при этом благоприятный инвестиционный климат.

Создавать высококлассный штат сотрудников кибербезопасности

Высококвалифицированный штат рабочей силы кибербезопасности является стратегическим преимуществом национальной безопасности. Соединенные Штаты будут в полной мере развивать обширный американский кадровый резерв, одновременно привлекая лучших и самых ярких людей из-за рубежа, разделяющих наши ценности.

Приоритетные Действия

СОЗДАВАТЬ И ПОДДЕРЖИВАТЬ КАДРОВЫЙ РЕЗЕРВ: Наши коллеги-партнеры по рынку реализуют программы развития рабочей силы, которые обладают возможностью повредить в долгосрочной перспективе конкурентным позициям Соединенных Штатов сфере кибербезопасности. Правительство Соединенных Штатов будет продолжать инвестировать и расширять программы, которые строят отечественный

перспективный пул кадрового резерва, от начального до продолженного среднего образования. Администрация будет максимально использовать предложенные Президентом реформы в отношении иммиграции базирующиеся на основе заслугах, для обеспечения того, чтобы в Соединенных Штатах был наиболее конкурентоспособный технологический сектор. Эти усилия могут потребовать дополнительной нормотворческой деятельности для достижения искомых целей.

РАСШИРЯТЬ ВОЗМОЖНОСТИ ДЛЯ ПЕРЕПОДГОТОВКИ И ОБРАЗОВАНИЯ ДЛЯ АМЕРИКАНСКИХ СЛУЖАЩИХ И РАБОЧИХ: Администрация будет работать с Конгрессом, чтобы продвигать и укреплять возможности образования и обучение для того, чтобы развивать полноценные трудовые ресурсы в сфере кибербезопасности. Это охватывает расширение подбора и расстановки кадров на Федеральном уровне, обучение, переподготовка людей из самых разных слоев общества и предоставление им возможности повышения квалификации для карьеры в сфере кибербезопасности.

УВЕЛИЧИВАТЬ КАДРОВЫЙ ПЕРСОНАЛ КИБЕРБЕЗОПАСНОСТИ ФЕДЕРАЛЬНОГО УРОВНЯ: Для того, чтобы улучшить комплектование и привлечение высококвалифицированных профессионалов в сере кибербезопасности в Федеральное Правительство, Администрация будет продолжать использовать организационную основу Национальной образовательной инициативы по кибербезопасности (*National Initiative for Cybersecurity Education,* NICE Framework) для поддержки политику, допускающей стандартизированный подход для определения, найма, развития и сохранения талантливого рабочего персонала в сфере кибербезопасности. Кроме того, Администрация будет изучать соответствующие возможности для создания распределенной системы штата служащих по кибербезопасности под управлением Министерства внутренней безопасности, DHS, с тем, чтобы контролировать развитие, управление, и комплектования персонала кибербезопасности в Федеральные департаменты, исключая Министерство обороны, DOD, а также разведывательные ведомства, IC. Администрация будет поощрять надлежащую финансовую компенсацию для рабочей персонала Правительства Соединенных Штатов, также как и уникальные возможности профессиональной подготовки и оперативного потенциала по эффективному привлечению и сохранению критически важных кадровых ресурсов в сфере кибербезопасности с учетом конкурентной среды частного сектора.

ИСПОЛЬЗОВАТЬ ИСПОЛНИТЕЛЬНЫЕ ОРГАНЫ ДЛЯ ВЫЯВЛЕНИЯ И ПООЩРЕНИЯ ТАЛАНТЛИВЫХ КАДРОВ: Правительство Соединенных Штатов будет поощрять и приумножать высокие достижения, посредством выдвижения преподавателей и профессионалов по кибербезопасности. Правительство Соединенных Штатов будет также задействовать систему возможностей частно-государственного партнерства для развития и распространения организационной основы Национальной образовательной инициативы по кибербезопасности, NICE Framework, которая обеспечивает

стандартизированный подход к выявлению пробелов в кадровом персонале в сфере кибербезопасности, при этом реализовывая меры по подготовке, росту и поддержанию рабочих кадров, которые могут защищать и поддерживать американскую критическую инфраструктуру и основу инноваций.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ III

Сохранить Мир посредством силы

Вызовы безопасности и экономическим интересам США, со стороны национальных государств и иных групп, которые долгое время существуют в офлайн-мире, сегодня все чаще возникают в киберпространстве. Такая ныне устойчивая вовлеченность в киберпространство уже меняет стратегический баланс сил. Настоящая Администрация будет проводить преобразующую политику, отражающую сегодняшнюю новую реальность, и направит Правительство Соединенных Штатов по пути достижения стратегических результатов, которые защитят американский народ и наш образ жизни. Киберпространство больше не будет расцениваться как отдельная категория политики или деятельности отделенная от иных элементов потенциала мощи государства. Соединенные Штаты будут интегрировать использование кибер-возможностей во всех элементах потенциала мощи государства.

ЦЕЛЬ: Выявлять, противодействовать, пресекать, ослаблять интенсивность и сдерживать действия в киберпространстве, которые дестабилизирует и противоречат национальным интересам, сохраняя при этом превосходство Соединенных Штатов в киберпространстве и посредством него.

Повышать киберстабильность посредством норм ответственного поведения государств

Соединенные Штаты будут содействовать созданию основополагающих рамок ответственного поведения государств в киберпространстве разработанные на основе международного права, приверженности добровольного соблюдения юридически не обязывающих норм ответственного поведения государств, которые применяются в мирное время, а также рассмотрению практических мер по укреплению доверия для снижения риска конфликта, связанного с вредоносной кибер-деятельностью. Такие принципы должны формировать ответ на совокупность запросов по противодействию безответственным действиям государств, несовместимых с такими основополагающими рамками.

Приоритетные Действия

ПООЩРЯТЬ ВСЕОБЩУЮ ПРИВЕРЖЕННОСТЬ К КИБЕР НОРМАМ: Международное право и необязательные нормы ответственного поведения государств в киберпространстве обеспечивают стабилизирующие, повышающие безопасность стандарты, которые определяют допустимое поведение для всех государств, а также способствуют большей предсказуемости и стабильности в киберпространстве. Соединенные Штаты будут поощрять другие страны публично подтвердить эти принципы и позиции посредством информационного продвижения и совместной работы на многосторонних форумах. Увеличение публичного подтверждения со стороны Соединенных Штатов и других Правительств приведет к общепринятому ожидаемому результату поведения государств и, таким образом, будет способствовать большей предсказуемости и стабильности в киберпространстве.

Атрибуты и сдерживание неприемлемого поведения в киберпространстве.

Поскольку Соединенные Штаты продолжают продвигать консенсус в отношении того, что представляет собой ответственное поведение государств в киберпространстве, мы должны также работать для подтверждения существования последствий безответственного поведения, которое вредит Соединенным Штатам и нашим партнерам. Все инструменты потенциала мощи государства являются доступными для того, чтобы предотвращать, реагировать и сдерживать злонамеренную кибер-деятельность против Соединенных Штатов. Это охватывает дипломатические, информационные, военные (одновременно и кинетические, и кибер), финансовые, разведывательные, публичные атрибуты, а также возможности правоприменения.

Приоритетные Действия

Соединенные Штаты официально определят и выработают определенную практику как они будут сотрудничать с партнерами-единомышленниками, для того, чтобы определить атрибуты и сдерживать вредоносную кибер-деятельность комплексными стратегиями, которые вводят быстрые, затратные и транспарентные последствия, когда злонамеренные субъекты наносят вред Соединенным Штатам или нашим партнерам.

РУКОВОДСТВОВАТЬСЯ ЦЕЛЯМИ, ВЗАИМОДЕЙСТВОВАТЬ С РАЗВЕДЫВАТЕЛЬНЫМИ ОРГАНАМИ: Разведывательные ведомства, IC, будут и впредь занимать ведущее положение в мире в использовании всех источников кибер-разведданных для выявления и определения характерных признаков вредоносной кибер-деятельности, которая угрожает национальным интересам Соединенных Штатов. Объекты и достоверные разведданные будут совместно использоваться Правительством Соединенных Штатов и ключевыми партнерами для выявления враждебно настроенных иностранных государств, а также не государственных кибер-программ, намерений, возможностей, исследований и разработок, тактической и оперативной деятельности, которые будут оказывать влияние на обще-правительственную ответную реакцию для защиты американских интересов в отечестве и за рубежом.

ВОЗЛАГАТЬ МЕРЫ ЗА ПОСЛЕДСТВИЯ: Соединенны Штаты будут расширять незамедлительно и транспарентно последствия, которые мы будем возлагать в соответствии с нашими обязательствами и обязанностями для того, чтобы предотвращать дальнейшее преднамеренное ненадлежащее поведение. Администрация будет проводить межведомственное планирование политики в течении периода времени, перед, во время, а также после возложения последствий, с тем, чтобы обеспечить своевременный и последовательный процесс реагирования и предотвращения злонамеренных кибер-действий. Соединенные Штаты будут сотрудничать с партнерами, когда это целесообразно, чтобы возлагать последствия вредоносным кибер-субъектам в ответ на их действия против нашего отечества и интересов.

СОЗДАВАТЬ КИБЕР-СДЕРЖИВАЮЩИЕ ИНИЦИАТИВЫ: Возложение последствий будет обладать большей силой воздействия и даст решительное понимание если они проводится совместно с более широкой коалицией

государств-единомышленников. Соединенные Штаты приступят к реализации международную Инициативы по кибер-сдерживанию (*Cyber Deterrence Initiative*), для того, чтобы создать такую коалицию, а также разработать индивидуальные стратегии, позволяющие противникам понять последствия своего злонамеренного кибер-поведения.

Соединенные Штаты будут сотрудничать с государствами-единомышленниками, взаимодействовать и поддерживать ответную реакцию друг друга

на существенные злонамеренные кибер-инциденты, в том числе

посредством обмена разведданными, консолидирования заявлений о характерных признаках [кибер-инцидента], публичных заявлений о поддержке

предпринятые ответные действий, а также совместное возложение последствий против злостных субъектов.

ПРОТИВОДЕЙСТВОВАТЬ ВРЕДОНОСНОМУ КИБЕР-ВЛИЯНИЮ И ИНФОРМАЦИОННЫМ ОПЕРАЦИЯМ: Соединенные Штаты будут будут использовать все соответствующие инструменты национальной потенциала государства, чтобы разоблачать и противостоять потоку злонамеренного он-лайн влияния и информационных кампаний, а также негосударственной пропаганды и дезинформации. Это охватывает работу с Правительствами иностранных партнеров, а также с частным сектором, научными кругами и гражданским обществом для выявления, противодействия и предотвращения использования цифровых платформ для злонамеренных операций иностранного влияния при соблюдении гражданских прав и свобод.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ IV

Усиление американского влияния

Мир смотрит на Соединенные Штаты, где значительная часть инноваций для современного интернета берут свои начала, с точки зрения лидирующей роли по широкому спектру транснациональных киберпроблем. Соединенные Штаты сохранят активную позицию международного лидера, чтобы усилить американское влияние и противостоять растущему ряду угроз и вызовов своим интересам в киберпространстве. Сотрудничество с союзниками и партнерами является существенным., также чтобы мы могли продолжать

извлекать преимущества из трансграничной коммуникации, создания контента и коммерции, генерируемых открытой, функционально совместимой архитектуры интернета.

ЦЕЛЬ: Сохранять долгосрочную открытость, функциональную совместимость, безопасность и надежность интернета, который поддерживается и усиливается интересами Соединенных Штатов.

Способствовать открытому функционально совместимому, надежному и безопасному интернету.

Глобальный интернет вызвал ряд самых больших достижений со времен промышленной революции, обеспечивая большие успехи в торговле, здравоохранении, коммуникации и иной национальной инфраструктуре. В то же время многовековые сражения за права человека и основные свободы в настоящее время разворачиваются в онлайн среде. Свобода выражения мнений, мирных собраний и ассоциаций, а также права на неприкосновенность частной жизни находятся под угрозой. Несмотря на беспрецедентный рост, экономический и социальный потенциал интернета по-прежнему подрывается цензурой и репрессиями в интернете. Соединенные Штаты твердо придерживаются своих принципов защиты и продвижения открытого, функционально совместимого, надежного и безопасного интернета. Мы будем работать над тем, чтобы наш подход к открытому интернету представлял собой международный стандарт. Мы будем также работать над тем, чтобы авторитарные государства, которые рассматривают открытый интернет как политическую угрозу, не превратили свободный и открытый интернет в авторитарный интернет, находящийся под их контролем, под предлогом безопасности или противодействия терроризму.

Приоритетные Действия

ЗАЩИЩАТЬ И СОДЕЙСТВОВАТЬ СВОБОДЕ ИНТЕРНЕТА: Правительство Соединенных Штатов смоделирует концепцию онлайнового осуществления прав человека и основных свобод — таких, как свобода выражения мнений, ассоциации, мирных собраний, религии или убеждений, а также права на неприкосновенность частной жизни в интернете — независимо от границ или среды. В более широком смысле свобода интернета также поддерживает свободный поток информации в интернете, что способствует развитию международной торговли и коммерции, стимулирует инновации и укрепляет как национальную, так и международную безопасность. Сами по себе, как таковые, принципы свободы интернета в Соединенных Штатах неразрывно связаны с нашей национальной безопасностью. Свобода Интернета также является ключевым руководящим принципом в отношении других вопросов внешней политики США, таких как киберпреступность и борьба с терроризмом. Учитывая его важность, Соединенные Штаты будут поощрять другие страны к продвижению свободы Интернета с помощью таких площадок, как Коалиция свободы в он-лайн среде (*Freedom Online Coalition*), одним из основателей которой являются Соединенные Штаты.

СОТРУДНИЧАТЬ СО СТРАНАМИ-ЕДИНОМЫШЛЕННИКАМИ, ПРОМЫШЛЕННОСТЬЮ, АКАДЕМИЧЕСКИМ И ГРАЖДАНСКИМ СООБЩЕСТВОМ: Соединенные Штаты будут продолжать работать со странами-единомышленниками, промышленностью, гражданским обществом и иными заинтересованными сторонами/стейкхолдерами для того, чтобы содействовать правам человека и свободе интернета во всем мире, а также противостоять авторитарным усилиям в цензуре и авторитарным влияниям на развитие интернета. Правительство Соединенных Штатов будет и впредь оказывать поддержку гражданскому обществу посредством комплексной поддержки развития технологий, обучения в области цифровой безопасности, информационно-разъяснительно работы и исследований. Такие программы направлены на повышение способности отдельных граждан, активистов, правозащитников, независимых журналистов, организаций гражданского общества и маргинальных групп населения безопасно получать доступ к интернету без цензуры, а также содействовать свободе интернета на локальном, региональном, национальном и международном уровнях.

СОДЕЙСТВИЕ МНОГОСТОРОННЕЙ МОДЕЛИ УПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА: Соединенные Штаты будут и впредь принимать

активное участие в глобальных усилиях по обеспечению того, чтобы многосторонняя модель управления использования интернета с участием всех заинтересованных сторон, т.е. мультистейкхолдерская модель, преобладала против попыток создания государственно-центристских структурных рамок, которые подорвали бы открытость и свободу, препятствовали бы инновациям и поставили бы под угрозу функциональность интернета. Многосторонняя модель управления использования интернета характеризуется транспарентностыми, демократично-коллегиальными, консенсус-ориентированными процессами, что позволяет Правительствам, частному сектору, гражданскому

общество, научным кругам и техническому сообществу участвовать на равных. Правительство Соединенных Штатов будет защищать открытую, функционально совместимую природу интернета на многосторонних и международных форумах посредством активного взаимодействия с ключевыми организациями, такими как Корпорация интернета по присвоению имен и номеров (*Internet Corporation for Assigned Names and Numbers*), Форум по управлению интернетом (*Internet Governance Forum*), Организация Объединенных Наций и Международный Союз электросвязи.

СОДЕЙСТВОВАТЬ ФУНКЦИОНАЛЬНО СОВМЕСТИМОЙ НАДЕЖНОЙ КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЕ И ПОДКЛЮЧЕНИЯ К ИНТЕРНЕТУ: Соединенные Штаты будут содействовать развитию инфраструктуры коммуникаций и подключения к интернету, которая будет открытой, функционально совместимой, надежной и безопасной. Такие инвестиции предоставят американским фирмам громадные возможности для конкуренции, при этом противодействуя влиянию нерыночных, административно-командных мер государственного вмешательства в области стратегической конкуренции. Это также защитит американскую безопасность икоммерческие интересы за счет укрепления конкурентоспособности промышленности Соединенных Штатов США в глобальной цифровой экономике. Администрация также будет поддерживать и продвигать открытые отраслевые стандарты деятельности, основанные на надежных технологических принципах.

СОДЕЙСТВОВАТЬ И ПОДДЕРЖИВАТЬ РЫНКИ В ОТНОШЕНИИ ИЗОБРЕТАТЕЛЬНОСТИ СОЕДИНЕННЫХ ШТАТОВ ПО ВСЕМУ МИРУ: Американские субъекты инновационной деятельности и специалисты в области безопасности внесли значительный вклад в разработку продуктов и услуг, которые улучшают наши возможности коммуникаций и взаимодействия на глобальном уровне, а также которые защищают инфраструктуру коммуникаций, данные и устройства по всему

миру. Соединенные Штаты будут продолжать содействовать рынкам в отношении американской изобретательности за рубежом, в том числе для новых технологий, которые могут снизить стоимостные издержки безопасности. Соединенные Штаты будут также консультировать по вопросам развертывания инфраструктуры, инноваций, управления рисками, политики и стандартов для дальнейшего глобального расширения зон доступа к интернету и обеспечения функциональной совместимости, безопасности и стабильности. Наконец, Соединенные Штаты будут работать с международными партнерами, Правительством, промышленностью, гражданским обществом, техническими специалистами и учеными, чтобы улучшить внедрение и осведомленность о лучших практиках кибербезопасности во всем мире.

Создавать международный кибер-потенциал.

Наращивание потенциала позволяет партнерам защищать самих себя, а также помогать Соединенным Штатам в устранении угроз, направленных на взаимные интересы, одновременно выполнять свои функции в широких дипломатических, экономических целях и целях безопасности. Посредством инициатив по наращиванию кибер-потенциала Соединенные Штаты создают стратегические партнерства, способствующие распространению лучших практик в сфере кибербезопасности, посредством общего видения открытого, функционально совместимого, надежного и безопасного интернета, который стимулирует инвестиции и открывает новые экономические рынки. Кроме того, наращивание потенциала предоставляет дополнительные возможности для обмена информацией о киберугрозах, что позволяет Правительству Соединенных Штатов и нашим партнерам лучше защищать отечественную критическую инфраструктуру и глобальные снабженческие цепочки, а также сконцентрировать внимание на межправительственном взаимодействии в киберпространстве. Наше лидерство в создании партнерского потенциала кибербезопасности имеет решающее значение для поддержания американского влияния на глобальных конкурентов. Создание партнерского кибер-потенциала позволит международным партнерам реализовывать политику и практику, которые позволят им стать эффективными партнерами в рамках возглавляемой Соединенными Штатами Инициативы по кибер-сдерживанию (*Cyber Deterrence Initiative*).

Приоритетные Действия

УЛУЧШАТЬ КИБЕР-МОБИЛИЗУЮЩИЕ МЕРЫ: Многие союзники и партнеры Соединенных Штатов обладают уникальными кибер-возможностями, которые

могут дополнять наши собственные. Соединенные Штаты будут работать над укреплением потенциала и функциональной совместимости таких союзников и партнеров с целью повышения нашей способности оптимизировать наши совместные навыки, ресурсы, возможности и перспективы против общих угроз. Партнеры могут также помогать обнаруживать, сдерживать и разрушать эти общие угрозы в киберпространстве. Для того чтобы международные партнеры могли эффективно защищать свою цифровую инфраструктуру и бороться с общими угрозами, в то же время осознавая экономические и социальные выгоды, извлекаемые из интернета и ИКТ, Соединенные Штаты будут продолжать заниматься вопросами создания структурных элементов для организации национальных усилий по кибербезопасности. Мы также будем активно наращивать усилия по обмену автоматизированной и действенной информацией о киберугрозах, расширять координацию в области кибербезопасности, а также способствовать аналитическим и техническим

обменам. К тому же, Соединенные Штаты будут работать над уменьшением воздействия и влияния транснациональной киберпреступности и террористической деятельности посредством установления партнерских отношений и укрепления потенциала наших партнеров в сфере безопасности и правоприменения для наращивания их кибер-потенциала.