СТРАТЕГИЯ НАЦИОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ СОЕДИНЕННЫХ ШТАТОВ АМЕРИКИ

Сентябрь 2018 года

БЕЛЫЙ ДОМ, Вашингтон, округ Колумбия

Соотечественники!

Защита национальной безопасности Америки и обеспечение процветания американского народа являются основными приоритетами моей администрации. Обеспечение безопасности киберпространства является жизненно важным для их реализации. Безопасность киберпространства является неотъемлемой частью любой отрасли и сферы жизни Америки, в том числе ее экономики и обороны. Тем не менее, наши коммерческие и государственные компании и учреждения все еще с трудом обеспечивают безопасность своих рабочих систем, ведь количество и сложность хакерских атак со стороны наших недоброжелателей возросли многократно. Америка создала интернет и поделилась им со всем миром. Теперь мы должны обеспечить безопасность киберпространства для будущих поколений.

За последние восемнадцать месяцев моя администрация предприняла целый комплекс мер по борьбе с киберугрозами. Мы наложили на опасных внешних злоумышленников соответствующие санкции. Мы привлекли лица, совершившие киберпреступления, к уголовной ответственности. Мы поименно назвали наших противников, осуществлявших подрывную деятельность, и опубликовали информацию о совершенных действиях, а также используемых ими инструментах и методах. Мы обязали государственные органы и ведомства заменить программное обеспечение, имеющее критические уязвимости для обеспечения безопасности. Мы возложили на руководителей государственных структур и ведомств обязательства по управлению рисками в области кибербезопасности в контексте систем, находящихся под их управлением, а также предоставили им дополнительные полномочия, позволяющие им обеспечить надлежащий уровень безопасности. Кроме того, в прошлом году я подписал Указ №13800 *«Усиление кибербезопасности федеральных сетей и критически важной инфраструктуры»*. Результаты проведенной работы и соответствующая отчетность, составленная на основании этого Указа, были взяты за основу настоящей Стратегии национальной кибербезопасности.

После опубликования настоящего документа у Соединенных Штатов Америки впервые за последние пятнадцать лет появилась четко определенная и полноценная стратегия кибербезопасности. В настоящей стратегии излагаются методы, с помощью которых моя администрация будет:

• обеспечивать безопасность Америки путем защиты сетей, систем, программных функций и данных;

• обеспечивать процветание Америки путем построения безопасной, успешной цифровой экономики и стимулирования развития инноваций на национальном уровне;

• обеспечивать мир и безопасность путем увеличения возможностей Соединенных Штатов Америки совместно с их союзниками и партнерами по сдерживанию, а, при необходимости, и по наказанию лиц и государств, использующих цифровые инструменты в злонамеренных целях;

• расширять американское влияние за рубежом с целью более широкого внедрения основных принципов открытого, функционально совместимого, надежного и безопасного интернета.

Настоящая Стратегия национальной кибербезопасности является подтверждением моей приверженности усилению практических возможностей Америки по обеспечению кибербезопасности и защиты от киберугроз. Настоящий документ – это призыв ко всем американцам и нашим крупным компаниям принять необходимые меры по усилению нашей национальной кибербезопасности. Америка останется мировым лидером в области создания безопасного киберпространства.

С уважением,

(подпись)

Президент Дональд Джон Трамп

Белый дом

Сентябрь 2018 года

Содержание

Введение

Процветание и безопасность Америки зависят от использования имеющихся возможностей и надлежащего реагирования на возникающие угрозы в киберпространстве. Критически важная инфраструктура, национальная оборона и повседневная жизнь граждан США зависят от компьютерных и взаимосвязанных информационных технологий. Все сферы жизни простого американца стали намного более зависимы от безопасного киберпространства; определяются новые уязвимые места и растет количество новых угроз. Настоящая Стратегия национальной кибербезопасности основана на стратегии национальной безопасности и практических результатах деятельности администрации президента США за первые 18 месяцев работы, и описывает то, каким образом Соединенные Штаты продолжат предоставлять своим гражданам возможность пользоваться безопасным киберпространством, которое отражает принятые нами принципы, обеспечивает нашу безопасность и ведет нас к процветанию.

Анализ текущей ситуации

Появление интернета и увеличение влияния киберпространства на все сферы жизни современного мира совпали со становлением Соединенных Штатов Америки в качестве единственной сверхдержавы во всем мире. За последнюю четверть века изобретательность американского народа стала залогом успешного развития киберпространства. В свою очередь, киберпространство стало источником американского богатства и инноваций. Киберпространство – неотъемлемая часть финансовой, социальной, государственной и политической жизни Америки. Американцы зачастую принимали превосходство Соединенных Штатов в киберпространстве как само собой разумеющееся явление и считали, что такое положение навсегда останется неоспоримым, а также рассчитывали на то, что американское видение открытого, функционально совместимого, надежного и безопасного интернета неизбежно станет реальностью. Американцы искренне считали, что развитие интернета позволит реализовать фундаментальные права на свободу слова и личную свободу во всем мире; они предполагали, что возможности по расширению коммуникации, ведению коммерческой деятельности, а также свободному обмену идеями будут очевидными. Множество стран приняли американское видение общего и открытого киберпространства, что привело к получению взаимной выгоды всеми сторонами.

Тем не менее, наши конкуренты и противники придерживаются противоположной точки зрения. Они пользуются преимуществами открытого интернета, при этом ограничивая и контролируя доступ к нему для своих граждан; более того, они активно подрывают принципы свободного интернета на международных форумах. Прикрываясь понятием суверенитета, они безответственно нарушают законодательство других государств, осуществляя акты экономического шпионажа и хакерские атаки, нанося значительный вред экономикам, интересам физических лиц, интересам коммерческого и некоммерческого характера, а также правительствам по всему миру. Они рассматривают киберпространство в качестве площадки, которая позволяет нейтрализовать

превосходящую военную, экономическую и политическую мощь Соединенных Штатов; площадки, где Соединенные Штаты, их союзники и партнеры уязвимы.

Россия, Иран и Северная Корея провели ряд хакерских атак, которые нанесли ощутимый ущерб американским и транснациональным компаниям, нашим союзникам и партнерам и не понесли соответственного наказания, что могло бы стать сдерживающим фактором от осуществления подобных хакерских атак в будущем. Китай использует киберпространство для осуществления экономического шпионажа и кражи объектов интеллектуальной собственности, стоимость которой измеряется триллионами долларов. Негосударственные структуры, в том числе террористические и преступные группировки, используют киберпространство для получения прибыли, вербовки новых участников, популяризации своих идей и нападения на Соединенные Штаты, наших союзников и партнеров. При этом, их преступная деятельность часто покрывается враждебными нам государствами. Государственные и частные компании прикладывают множество усилий к обеспечению безопасности своих компьютерных и информационных систем, поскольку наши противники непрерывно увеличивают частоту и изощренность своих хакерских атак. Предприятия и организации, ведущие деятельность на территории Соединенных Штатов, столкнулись с проблемами кибербезопасности в процессе эффективного выявления, защиты от хакерских атак и обеспечения устойчивости функционирования своих сетей, систем, функций и данных, а также выявления, реагирования на произошедшие инциденты, а также последующее восстановление.

«Америка останется мировым лидером в области создания безопасного киберпространства».
Дональд Джон Трамп
Сентябрь 2018 года

Стратегия развития

Новые угрозы и новый этап стратегической конкуренции требуют новой стратегии по обеспечению безопасности киберпространства, которая должна отвечать новым реалиям, уменьшать выявленные уязвимости, служить фактором сдерживания для противников и обеспечивать возможности процветания американского народа. Обеспечение безопасности киберпространства имеет основополагающее значение для реализации нашей стратегии и требует внедрения последних достижений технического прогресса, а также административной эффективности федерального правительства и частного сектора. Нынешняя администрация признает, что исключительно технократического подхода в отношении киберпространства недостаточно для решения появляющихся проблем. Соединенные Штаты также должны обладать широким инструментарием эффективных мер принуждения, которые обеспечат сдерживание структур, осуществляющих хакерские атаки, и позволят предотвратить дальнейшую эскалацию.

Нынешняя администрация уже приняла ряд мер по активному устранению этих угроз и адаптации к новым реалиям. Мы наложили на опасных внешних злоумышленников соответствующие санкции. Мы привлекли лица, совершившие киберпреступления, к

уголовной ответственности. Мы поименно назвали наших противников, осуществлявших подрывную деятельность, и опубликовали информацию о совершенных действиях, а также используемых ими инструментах и методах. Мы обязали государственные органы и ведомства заменить программное обеспечение, имеющее критические уязвимости для обеспечения безопасности. Мы возложили на руководителей государственных структур и ведомств обязательства по управлению рисками в области кибербезопасности в контексте систем, находящихся под их управлением, а также предоставили им дополнительные полномочия, позволяющие им обеспечить надлежащий уровень безопасности.

Подход нынешней администрации к регулированию киберпространства основан на американских ценностях, а именно, на личной свободе, свободе слова, свободных рынках и неприкосновенности личной жизни. Мы будем строго соблюдать принятые на себя обязательства по обеспечению открытого, функционально совместимого, надежного и безопасного интернета в целях усиления привлекательности и распространения наших ценностей, а также защиты и обеспечения экономической безопасности американских рабочих и компаний. Желаемое будущее не наступит без подтверждения приверженности Америки к продвижению своих интересов в киберпространстве.

Нынешняя администрация признает тот факт, что Соединенные Штаты ведут непрерывную конкурентную борьбу с нашими стратегическими противниками, угрожающими международной безопасности государствами, терроризмом и организованной преступностью. Россия, Китай, Иран и Северная Корея используют киберпространство в качестве площадки, где они могут бросить вызов Соединенным Штатам, нашим союзникам и партнерам. Такие вызовы зачастую характеризуются безрассудством, которое немыслимо в других сферах. Наши противники используют инструменты киберпространства для подрыва нашей экономики и демократии, кражи нашей интеллектуальной собственности и нарушения механизмов наших демократических процессов. В мирное время мы уязвимы для хакерских атак на критически важную инфраструктуру, следовательно, увеличивается риск того, что перечисленные выше страны будут осуществлять хакерские атаки на Соединенные Штаты в течение кризисов, не связанных с войной. Эти наши противники непрерывно разрабатывают новое и более эффективное кибероружие.

В настоящей Стратегии национальной кибербезопасности представлены методы: (1) защиты нашей родины путем обеспечения безопасности наших сетей, систем, функций и данных; (2) обеспечения благополучия Америки путем создания безопасной, процветающей цифровой экономики, а также условий для изобретения и внедрения инноваций на национальном уровне; (3) сохранения мира и безопасности путем усиления возможностей Соединенных Штатов совместно с нашими союзниками и партнерами по сдерживанию, а, при необходимости, и наказанию тех лиц и структур, которые используют киберинструменты в злонамеренных целях; (4) расширения американского влияния в целях реализации основных принципов открытого, функционально совместимого, надежного и безопасного интернета.

Настоящая стратегия будет считаться реализованной после успешного устранения

уязвимостей в структуре кибербезопасности путем их выявления и последующей защиты от них сетей, систем, функций и данных; выявления инцидентов, обеспечение устойчивости к их воздействию, реагирования и последующего восстановления; снижения ущерба от деструктивной, вредоносной и подрывной хакерской деятельности, направленной против интересов Соединенных штатов, или ее предотвращение; сдерживания деятельности, противоречащей ответственному поведению в киберпространстве при помощи мер принуждения, сетевого и иного характера; Соединенные Штаты могут использовать кибервозможности для достижения целей национальной безопасности.

Структура Стратегии национальной кибербезопасности составлена в соответствии с Принципами Стратегии национальной безопасности. Сотрудники Совета по национальной безопасности согласуют с министерствами и ведомствами, Службой управления и бюджета (OMB) соответственный план по ресурсному обеспечению в целях реализации настоящей Стратегии. Министерства и ведомства будут выполнять свои функции в соответствии со стратегическим руководством.

ПРИНЦИП I

Защита американского народа, Америки и американского образа жизни

Защита американского народа, американского образа жизни и интересов США является основной задачей Стратегии национальной кибербезопасности. Защита американских государственных или частных информационных сетей является жизненно важной составляющей этой цели. Достижение этой задачи потребует выполнения скоординированных действий, нацеленных на защиту государственных сетей, критически важной инфраструктуры и борьбу с киберпреступностью. Правительство Соединенных Штатов, частные предприятия, и общественность обязаны незамедлительно принимать необходимые меры по укреплению кибербезопасности, в контексте сетей, находящихся под их управлением, а также оказывать поддержку друг другу по мере необходимости.

ЦЕЛЬ: Обеспечение надлежащего управления рисками в области кибербезопасности с целью повышения безопасности и защищенности информационных систем и информации, имеющей государственную важность.

Обеспечение безопасности федеральных сетей и информации

Ответственность по обеспечению безопасности федеральных сетей, в том числе федеральных информационных систем и систем национальной безопасности, возлагается на федеральное правительство. Нынешняя администрация представит перечень соответственных прав и обязанностей, а также вертикаль подотчетности внутри и между министерствами и ведомствами в области обеспечения безопасности федеральных информационных систем, а также установит стандарт эффективного управления рисками в области кибербезопасности.

В целях выполнения данной задачи администрация президента проведет централизацию отдельных полномочий в рамках структуры федерального правительства, обеспечит большую межведомственную прозрачность, улучшит управление цепочкой поставок для нужд федерального правительства, а также усилит безопасность систем подрядчиков правительства Соединенных Штатов.

Приоритеты

ПРОДВИЖЕНИЕ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ И НАДЗОРА ЗА ОБЕСПЕЧЕНИЕМ КИБЕРБЕЗОПАСНОСТИ ГРАЖДАНСКОГО СЕКТОРА НА ФЕДЕРАЛЬНОМ УРОВНЕ:

Нынешняя администрация предоставит Министерству национальной безопасности (DHS) полномочия по обеспечению безопасности сетей федеральных министерств и ведомств за исключением систем национальной безопасности и систем Министерства обороны (DOD) и разведывательного сообщества (IC). Такие полномочия охватывают предоставление DHS соответственного доступа к министерским и ведомственным информационным системам в целях обеспечения кибербезопасности, а также полномочий по

осуществлению непосредственной защиты систем от целого ряда рисков. Под надзором Административно-бюджетного Управления (OMB) нынешняя администрация продолжит выполнять ряд задач в соответствии с предписаниями Указа №13800 в рамках первостепенной приоритетности перехода министерств и ведомств к межведомственным услугам и инфраструктуре. DHS будет иметь возможность контроля таких услуг и инфраструктуры с целью улучшения положения Соединенных Штатов в контексте кибербезопасности. При необходимости, DHS будет внедрять централизованные инструменты, услуги и средства, а также совершенствовать механизм надзора и обеспечивать соблюдение действующих законов, политик, стандартов и директив. Вполне вероятно, что это потребует внедрения новых политик и архитектур, которые позволят правительству лучше использовать инновации. При необходимости, DOD и IC проведут анализ результативности описанных мероприятий по мере их внедрения с целью обеспечения более высокого уровня безопасности национальных систем безопасности, систем DOD и IC.

СООТВЕТСТВИЕ УПРАВЛЕНИЯ РИСКАМИ ХАРАКТЕРИСТИКАМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ:

Указ №13833 «Повышение эффективности руководителей информационных управлений министерств и ведомств» наделяет руководителей информационных управлений (CIO) полномочиями по более эффективному использованию технологий для выполнения задач агентств и ведомств, устранения дублирующих процессов, а также повышения эффективности инвестиций в информационные технологии (IT). Руководители информационных управлений подотчетны руководителям министерств и ведомств по вопросам соответствия решений по управлению рисками в области кибербезопасности и финансирования решений в области информационных технологий и осуществляемыми закупками. Администрация, привлекая OMB и DHS, будет осуществлять руководство и проводить мероприятия по управлению рисками в федеральных гражданских ведомствах, а CIO будут уполномочены играть активную роль в обеспечении соответствия закупок IT-решений приоритетам по обеспечению безопасности сетей и данных.

УЛУЧШЕНИЕ УПРАВЛЕНИЯ РИСКАМИ ЦЕПОЧКИ ПОСТАВОК ДЛЯ НУЖД ФЕДЕРАЛЬНОГО ПРАВИТЕЛЬСТВА:

Администрация выступает за объединение управления рисками материального снабжения с министерскими процедурами закупок и управлением рисками в соответствии с федеральными требованиями, которые соответствуют передовым отраслевым методам с целью обеспечения безопасности и надежности технологий, используемых федеральным правительством. Сюда относится повышение качества обмена информацией между министерствами и ведомствами с целью повышения осведомленности об угрозах цепочке поставок и снижения количества дублирующих действий по материальному обеспечению Правительства Соединенных Штатов, в том числе, путем создания общего сервиса по оценке рисков материального обеспечения. Настоящее мероприятие также предусматривает устранение недостатков федеральной системы закупок, например, путем предоставления конкретных полномочий по обоснованному исключению рискованных поставщиков, продукции, услуг. Эта инициатива будет синхронизирована с усилиями по

управлению рисками цепочки поставок в рамках национальной инфраструктуры.

УСИЛЕНИЕ КИБЕРБЕЗОПАСНОСТИ ФЕДЕРАЛЬНЫХ ПОДРЯДЧИКОВ:

Для Соединенных Штатов непозволительной роскошью является недостаточная защищенность информации, составляющей государственную тайну, а также систем подрядчиков. Федеральные подрядчики предоставляют важные услуги правительству Соединенных Штатов и обязуются надлежащим образом обезопасить системы, при помощи которых они предоставляют такие услуги. В дальнейшем, федеральное правительство сможет оценивать безопасность своих данных путем проведения проверок механизмов управления рисками подрядчиков, а также соответственных тестирований, мониторинга, контроля и реагирования на инциденты, используя системы подрядчиков. Контракты с федеральными министерствами и ведомствами будут разрабатываться с учетом предоставления разрешений на осуществление таких действий в целях улучшения кибербезопасности. Особую озабоченность в этой области вызывают промышленные подрядчики, отвечающие за исследования и разработку базовых систем для нужд DOD. Кроме того, в соответствии с Указом №13800 «Отчетность перед президентом по вопросам модернизации федеральных информационных технологий», администрация поддержит принятие единых стратегий закупок с целью улучшения кибербезопасности и сокращения накладных расходов, связанных с использованием несогласованных условий контрактов в рамках структуры федерального правительства. При необходимости, администрация также предпримет меры по обеспечению получения и использования федеральными подрядчиками всей необходимой и доступной информации об угрозах и уязвимостях с целью улучшения своей позиции с точки зрения безопасности.

ОБЕСПЕЧЕНИЕ ВЕДУЩЕЙ РОЛИ ГОСУДАРСТВА В КОНТЕКСТЕ ПЕРЕДОВОЙ И ИННОВАЦИОННОЙ ПРАКТИКИ:

Федеральное правительство обязуется обеспечить соответствие собственных или используемых систем требованиям стандартов и передовой практики в области кибербезопасности, рекомендуемой для промышленности. Проекты, получающие федеральное финансирование, также должны соответствовать этим стандартам. Федеральное правительство намерено использовать свою покупательную способность для улучшения качества продуктов и услуг для нужд отрасли. Федеральное правительство также намерено быть лидером по разработке и внедрению стандартов и передовой практики в новых и зарождающихся секторах. Например, криптография с открытым ключом является краеугольным камнем для безопасного функционирования нашей инфраструктуры. Министерство торговли в целях защиты от потенциальной угрозы со стороны квантовых компьютеров, способных взломать современные криптографические механизмы с открытым ключом, основываясь на опыте Национального института стандартов и технологий (NIST), продолжит работу по сбору информации, оценке и стандартизации криптографических алгоритмов с открытым ключом, устойчивых к квантовому воздействию. Соединенные Штаты должны стать лидером в области защиты средств и каналов связи, оказывая поддержку быстрому принятию таких будущих стандартов NIST в отношении всей правительственной инфраструктуры, а также поощряя граждан США последовать собственному примеру.

Обеспечение безопасности критически важной инфраструктуры

Федеральное правительство и частный сектор несут солидарную ответственность по обеспечению безопасности национальной критически важной инфраструктуры и управлению рисками в области кибербезопасности. В рамках тесного сотрудничества с представителями частного сектора, используя методы управления рисками, мы сможем снизить количество присутствующих уязвимостей и поднять базовый уровень кибербезопасности всей критически важной инфраструктуры. Одновременное использование причинно-следственного подхода с целью определения приоритетов в отношении действий, уменьшающих возможности наиболее продвинутых противников организовать широкомасштабные и долгосрочные сбои в работе критической инфраструктуры. Нами также будет внедрен комплекс мер по сдерживанию злоумышленников и их спонсоров в виде мер принуждения, в том числе, но, не ограничиваясь, уголовным преследованием и экономическими санкциями в рамках более широкой стратегии сдерживания.

Приоритеты

АДАПТАЦИЯ ФУНКЦИЙ И ОБЯЗАННОСТЕЙ:

Нынешняя администрация четко распределит функции и обязанности федеральных министерств и ведомств, а также представит свои ожидания в отношении частного сектора в контексте управления рисками в области кибербезопасности и реагирования на инциденты. Четкое размежевание функций и обязанностей позволит обеспечить активное управление рисками, позволяющее осуществлять комплексное управление угрозами, уязвимостями и последствиями. Такой подход также позволит выявить и устранить существующие пробелы в рамках перечня обязанностей и порядке координации действий между федеральными и нефедеральными структурами по реагированию на инциденты и будет способствовать созданию более отлаженной системы обучения, подготовки и координации действий.

РАССТАНОВКА ПРИОРИТЕТОВ В СООТВЕТСТВИИ С ВЫЯВЛЕННЫМИ РИСКАМИ ДЛЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ:

Федеральное правительство будет взаимодействовать с представителями частного сектора по вопросам управления рисками критически важной инфраструктуры с наибольшим уровнем риска. Администрация разработает всестороннее понимание рисков на национальном уровне путем определения национальных критически важных функций, тем самым заложив твердое основание наших предложений по обеспечению кибербезопасности и обеспечению лучшего понимания таких национальных рисков. Администрация считает приоритетными действия по снижению рисков в семи ключевых отраслях: национальная безопасность, энергетика, банковский сектор и финансы, охрана здоровья и безопасность, связь, информационные технологии и транспорт.

ИНФОРМАЦИЯ ПОВЫШЕННОЙ ВАЖНОСТИ И ПОСТАВЩИКИ КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В КАЧЕСТВЕ НЕОБХОДИМЫХ УСЛОВИЙ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ:

Основу любой отрасли народного хозяйства Америки составляют информационно-коммуникационные технологии (ИКТ). Поставщики ИКТ имеют уникальные возможности по обнаружению, предотвращению и смягчению рисов до того, как они нанесут какой-либо ущерб потребителям их услуг. Федеральное правительство обязано целенаправленно и эффективно сотрудничать с такими поставщиками с целью улучшения безопасности и устойчивости ИКТ, одновременно обеспечивая защиту неприкосновенности личной информации и гражданских свобод. Правительство Соединенных Штатов нацелено на активизацию взаимодействия с поставщиками ИКТ по обмену информацией с целью реагирования и предотвращения известных видов хакерских угроз на сетевом уровне. Такое взаимодействие будет охватывать обмен секретной информацией об угрозах и уязвимостях с проверенными операторами ИКТ, а также снижение степени секретности или полного снятия грифов секретности в пределах возможного. Нынешняя администрация стремится продвигать адаптируемую, устойчивую и безопасную цепочку поставок технологий, обеспечивающую безопасность на основании передовой практики и стандартов. Правительство Соединенных Штатов планирует собрать ряд заинтересованных сторон для разработки межсекторальных решений для устранения угроз и проблем на уровне устройств, сети и шлюзов. Кроме того, мы будем оказывать содействие созданию отраслевых режимов сертификации, обеспечивающих адаптацию решений на фоне быстро меняющегося рынка и картины угроз.

ЗАЩИТА НАШИХ ДЕМОКРАТИЧЕСКИХ ЦЕННОСТЕЙ:

Защита демократических процедур имеет первостепенное значение для Соединенных Штатов и наших союзников, разделяющих демократические ценности. Государственные и местные органы власти владеют и имеют в своем распоряжении самую разнообразную выборную инфраструктуру на всей территории Соединенных Штатов. Следовательно, по первому требованию правительство предоставит технические услуги и услуги по управлению рисками, обеспечит необходимую подготовку и обучение, поддержит ситуационную осведомленность об угрозах в данном секторе, будет способствовать улучшению обменом информацией об угрозах со служащими государственных и местных органов власти в целях обеспечения лучшей подготовки и защиты выборной инфраструктуры. Федеральное правительство будет и впредь осуществлять координацию разработки стандартов кибербезопасности и рекомендаций по обеспечению безопасности выборов и инструментов, обеспечивающих безопасность систем. В случае значительного нарушения кибербезопасности, федеральное правительство готово соответственно отреагировать на возникшую угрозу, а также предоставить необходимые материальные ресурсы для восстановления избирательной инфраструктуры.

ПООЩРЕНИЕ ИНВЕСТИЦИЙ В СИСТЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ:

Большинство рисков в сфере кибербезопасности, затрагивающих критически важную инфраструктуру, произрастают из известного круга уязвимостей. Правительство

Соединенных Штатов стремится наладить тесное взаимодействие с государственными и частными компаниями и организациями по вопросу продвижения понимания рисков в области кибербезопасности с целью принятия компаниями и организациями более информированных решений по вопросам управления рисками, осуществления инвестиций в соответственные системы безопасности и осознания выгод этих инвестиций.

ПРИОРИТЕТНОСТЬ ИНВЕСТИЦИЙ В НАЦИОНАЛЬНЫЕ ИССЛЕДОВАНИЯ И РАЗВИТИЕ:

Федеральное правительство обновит Национальный план исследований и развития безопасности и устойчивости национальной критической инфраструктуры с целью расстановки приоритетов по устранению рисков для критически важной инфраструктуры в сфере кибербезопасности. Министерства и ведомства обязуются привести свои инвестиции в соответствие с установленными приоритетами, нацеленными на создание новых подходов в сфере кибербезопасности с использованием новейших технологий, улучшением обмена информацией и управления рисками, обусловленными межсекторальными взаимозависимостями и повышением устойчивости к крупномасштабным и долговременным нарушениям функциональности.

УСИЛЕНИЕ КИБЕРБЕЗОПАСНОСТИ НАЗЕМНОГО И МОРСКОГО ТРАНСПОРТА:

Национальная и экономическая безопасность Америки основана на международной торговле и транспортной инфраструктуре. Наша возможность гарантировать свободное и своевременное перемещение товаров, открытое море и воздушные коридоры, доступ к нефти и природному газу, доступность соответствующей критической инфраструктуры имеет первостепенное значение для экономической и национальной безопасности нашего государства. По мере модернизации этих секторов они также стали более уязвимыми для сетевых атак и использования в злоумышленных целях. Кибербезопасность морского транспорта имеет первостепенное значение, поскольку утрата грузов или задержки их доставки могут привести к значительной экономической дезорганизации и побочным эффектам для отраслей последующей обработки. С учетом критической важности морских перевозок для Соединенных Штатов и глобальной экономики, а также уже совершенных минимальных инвестиций в снижение рисков для защиты от несанкционированного использования, Соединенные Штаты в ближайшее время разработают схему разграничения функций и обязанностей в контексте обеспечения кибербезопасности морского транспорта; будут содействовать укреплению механизмов международной координации и обмена информации; будут содействовать развитию устойчивой к хакерским атакам морской инфраструктуры следующего поколения. Соединенные Штаты обязуются обеспечить бесперебойную транспортировку товаров, не смотря на любые угрозы такой международной инфраструктуре, исходящих от киберсредств.

УСИЛЕНИЕ КИБЕРБЕЗОПАСНОСТИ В КОСМИЧЕСКОМ ПРОСТРАНСТВЕ:

Соединенные Штаты считают неограниченный доступ и свободу действия в космическом пространстве чрезвычайно важными для обеспечения безопасности, экономического процветания и научных исследований на благо нашего народа. Нынешняя администрация

обеспокоена ростом киберугроз в отношении систем космического базирования и вспомогательной инфраструктуры, поскольку эти системы являются критически важными для обеспечения таких функций как позиционирование, навигация и синхронизация (PNT); разведка, наблюдение, рекогносцировка (ISR); спутниковая связь; и мониторинг погоды. Нынешняя администрация приложит большие усилия по защите наших систем космического базирования и вспомогательной инфраструктуры от непрерывно эволюционирующих киберугроз, а также будет сотрудничать с представителями промышленности и международными партнерами по укреплению киберустойчивости существующих и будущих космических систем.

Борьба с киберпреступностью и отчетность о происшествиях

Федеральные министерства и ведомства в тесном взаимодействии с региональными, местными, городскими (сельскими) и территориальными органами власти играют критически важную роль в процессе выявления, предотвращения, защиты и расследования киберугроз для граждан США. Соединенные Штаты часто становятся жертвой злоумышленных хакерских атак со стороны преступных элементов, в том числе государственных и негосударственных структур, их доверенных лиц и террористов, использующих сетевую инфраструктуру на территории Соединенных Штатов и заграницей. Федеральные правоохранительные органы тщательно работают над задержанием и уголовным преследованием правонарушителей, выведением из строя преступной инфраструктуры, ограничением распространения и недобросовестного использования возможностей информационных и компьютерных систем, предотвращением получения выгоды киберпреступниками и их государствами-спонсорами от своей незаконной деятельности, арестами и конфискации их активов. Нынешняя администрация обязуется наделить наши федеральные министерства и ведомства необходимыми юридическими полномочиями и ресурсами по борьбе с международной киберпреступностью, в том числе по выявлению и ликвидации бот-сетей, черных рынков и другой инфраструктуры, используемой для совершения киберпреступлений, а также борьбе с экономическим шпионажем. Для эффективного сдерживания, обезвреживания и предотвращения киберугроз правоохранительные органы будут тесно взаимодействовать с частными компаниями в целях противодействия вызовам, которые порождают технологические барьеры, такие как технологии анонимности и шифрования, с целью получения доказательств с ограниченным временем действия для целей соответственного судебного процесса. Деятельность правоохранительных органов по борьбе с киберпреступностью является силовым ресурсом нации, которая, помимо всего прочего, выполняет функцию сдерживающего фактора.

Приоритеты

УЛУЧШЕНИЕ ОТЧЕТНОСТИ О ПРОИСШЕСТВИЯХ И МЕРАХ РЕАГИРОВАНИЯ:

Правительство Соединенных Штатов продолжит политику поощрения сообщений пострадавших о несанкционированном проникновении и хищении данных, особенно

партнерами по критически важной инфраструктуре. Неотложное сообщение о киберинцидентах федеральному правительству имеет первостепенное значение для эффективного реагирования, установления исполнителей и предотвращения подобных инцидентов в будущем.

СОВЕРШЕНСТВОВАНИЕ ЗАКОНОДАТЕЛЬСТВА О СИСТЕМАХ ЭЛЕКТРОННОГО НАБЛЮДЕНИЯ И ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ:

Администрация разработает и подаст в Конгресс на рассмотрение соответственные изменения и дополнения в законодательство о системах электронного наблюдения и преступлений с использованием компьютерной техники с целью расширения возможностей правоохранительных органов по законному сбору необходимых доказательств преступной деятельности, обезвреживания преступной инфраструктуры при помощи гражданско-правовых судебных запретов, а также применения соответственных мер принуждения в отношении злоумышленников, использующих информационные и компьютерные системы.

СНИЖЕНИЕ УРОВНЯ УГРОЗ СО СТОРОНЫ МЕЖДУНАРОДНЫХ ПРЕСТУПНЫХ ОРГАНИЗАЦИЙ В КИБЕРПРОСТРАНСТВЕ:

Хакерские атаки на компьютерные системы со стороны международных преступных групп несут значительную угрозу нашей национальной безопасности. Обладая значительными финансовыми ресурсами, организованные преступные группы, действующие за пределами США, используют сложное вредоносное программное обеспечение, адресный фишинг и другие хакерские инструменты (некоторые из которых по своей изощренности могут конкурировать с национальными государствами) для взлома секретных финансовых систем, организации серьезных утечек данных, распространения программ-вымогателей, атак на критически важную инфраструктуру и кражи интеллектуальной собственности. Нынешняя администрация будет лоббировать предоставление правоохранительным органам эффективных юридических инструментов для проведения расследований и судебного преследования таких организованных групп, а также внесения изменений и дополнений в законодательство по борьбе с организованной преступностью для устранения этой угрозы.

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ЗАДЕРЖАНИЯ ПРЕСТУПНИКОВ ЗАГРАНИЦЕЙ:

Залогом успешного сдерживания совершения новых преступлений с использованием компьютерной техники являются веские основания полагать, что потенциальные преступники будут выявлены, задержаны и привлечены к ответственности. Тем не менее, некоторые иностранные государства отказываются экстрадировать таких лиц по обоснованному требованию, налагают необоснованные ограничения или активно препятствуют таким действиям. Соединенные Штаты приложат все усилия по устранению пробелов в существующих процедурах, а также будут разрабатывать новые действенные механизмы привлечения к уголовной ответственности находящихся за рубежом преступников, совершивших преступления с использованием компьютерной техники. Правительство Соединенных Штатов продолжит прилагать все необходимые

дипломатические и другие усилия по взаимодействию с другими странами в целях обеспечения содействия по вопросам обоснованной экстрадиции. Соединенные Штаты будут побуждать другие страны оказывать необходимое содействие в целях проведения соответственных расследований в максимально сжатые сроки и соблюдать любые двусторонние или многосторонние соглашения или взятые на себя обязательства.

РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ СТРАН-ПАРТНЕРОВ В ЦЕЛЯХ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ:

Соединенные Штаты обязуются оказывать необходимую поддержку заинтересованным странам-партнерам в наращивании потенциала для борьбы с киберпреступностью. Отсутствие ограничений в виде государственных границ для киберпреступности, террористической деятельности, а также деятельности, финансируемой за счет государственного бюджета, требует надежного взаимодействия международных правоохранительных органов. Такое сотрудничество требует наличия у иностранных правоохранительных органов технических возможностей для эффективного оказания помощи правоохранительным органам Соединенных Штатов по первому требованию. Следовательно, Соединенным Штатам в интересах национальной безопасности следует продолжить наращивать потенциал по борьбе с киберпреступностью, что способствует укреплению международного сотрудничества правоохранительных органов.

Соединенные Штаты будут прилагать необходимые усилия по улучшению международного сотрудничества в контексте расследования хакерской деятельности, в том числе разработке решений с учетом потенциальных препятствий для сбора и обмена доказательствами. Соединенные Штаты также будут играть ведущую роль в разработке совместимых и взаимовыгодных систем, обеспечивающих эффективный трансграничный обмен информацией для целей правоохранительных органов и уменьшения количества барьеров для координации действий. Нынешняя администрация настоятельно рекомендует более эффективно использовать действующие международные инструменты, такие как Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Сеть координаторов «Большой семерки», работающих в режиме 24/7. Кроме того, мы будем работать над расширением международного консенсуса в пользу Конвенции по борьбе с киберпреступностью Совета Европы (Будапештская конвенция), в том числе продвигая принятие конвенции большим количеством стран.

ПРИНЦИП II

Обеспечение процветания Америки

Интернет стал средством, приносящим огромные выгоды как внутри страны, так и за рубежом, более того, он позволяет распространять американские ценности – свободу, безопасность и процветание. По мере распространения интернета стали появляться вызовы и проблемы, представляющие угрозу нашей национальной безопасности. Соединенные Штаты будут прилагать последовательные и всесторонние усилия по разрешению появившихся и иных угроз с целью защиты своих национальных интересов во все более оцифрованном мире.

ЦЕЛЬ: Сохранение влияния Соединенных Штатов в рамках технологической опорной инфраструктуры и разработка киберпространства в качестве открытого двигателя экономического роста, инноваций и эффективности.

Содействие развитию динамичной и устойчивой цифровой экономики

Экономическая безопасность неотъемлемо связана с нашей национальной безопасностью. Поскольку основу нашей экономики все больше составляют цифровые технологии, правительство Соединенных Штатов обязуется создавать и продвигать стандарты, которые защищают нашу экономическую безопасность и укрепляют жизнеспособность американского рынка и американские инновации.

Приоритеты

СТИМУЛИРОВАНИЕ РАЗВИТИЯ РЫНКА АДАПТИВНЫХ И БЕЗОПАСНЫХ ТЕХНОЛОГИЙ:

В целях улучшения устойчивости киберпространства нынешняя администрация ожидает, что рынок технологий обеспечит поддержку и вознаграждение усилий по непрерывной разработке, внедрению и развитию инновационных технологий и процессов в области обеспечения безопасности. Нынешняя администрация будет взаимодействовать со всеми заинтересованными группами, включая представителей частного сектора и гражданского общества, для продвижения передовой практики и разработки стратегий преодоления рыночных барьеров с целью внедрения безопасных технологий. Администрация будет повышать осведомленность и прозрачность практик в области обеспечения кибербезопасности с целью создания рыночного спроса на более безопасные продукты и услуги. Более того, нынешняя администрация планирует тесно взаимодействовать с международными партнерами в целях продвижения открытых отраслевых стандартов, поддерживаемых государством (в зависимости от ситуации), риск-ориентированных подходов к решению проблем кибербезопасности для охвата подходов на базе платформ и управляемых услуг, которые уменьшают барьеры по внедрению безопасной практики в рамках всей опорной инфраструктуры.

ПРИОРИТЕТ РАЗРАБОТКИ И ВНЕДРЕНИЯ ИННОВАЦИЙ:

Правительство Соединенных Штатов будет содействовать внедрению и постоянному

обновлению стандартов и передовой практики, которые позволяют сдерживать и предотвращать существующие и зарождающиеся угрозы во всех областях опорной инфраструктуры. Эти стандарты и практика должны быть ориентированы на результат и основаны на надежных технологических принципах, а не на текущих характеристиках компании. Нынешняя администрация будет работать над устранением политических барьеров, препятствующим разработке, совместному использованию и созданию инноваций для снижения опасности киберугроз в рамках построения устойчивой системы кибербезопасности.

ИНВЕСТИЦИИ В ИНФРАСТРУКТУРУ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ:

Нынешняя администрация будет содействовать ускоренному развитию и внедрению инфраструктуры информационно-коммуникационных технологий следующего поколения на территории Соединенных Штатов за счет покупательной способности федерального правительства с целью поощрения перехода к более безопасным цепочкам поставок. Правительство Соединенных Штатов будет взаимодействовать с представителями частного сектора в целях содействия развитию и обеспечения безопасности 5G, изучения технологических и спектральных решений и создания основания для инноваций, выходящих за пределы достижений следующего поколения. Правительство Соединенных Штатов проанализирует возможность использование новых технологий, таких как искусственный интеллект и квантовые вычисления, параллельно устраняя риски, присущие их использованию и применению. Мы будем сотрудничать с представителями частного сектора и гражданским обществом для понимания тенденций развития технологий с целью обеспечения технологического преимущества Соединенных Штатов в области сетевых технологий и обеспечения изначального внедрения практики обеспечения безопасности.

«Национальная стратегия кибербезопасности – это призыв ко всем американцам и нашим крупным компаниям принять необходимые меры по усилению нашей национальной кибербезопасности».
Дональд Джон Трамп
Сентябрь 2018 года

СОДЕЙСТВИЕ СВОБОДНОМУ ТРАНСГРАНИЧНОМУ ДВИЖЕНИЮ ДАННЫХ:

Многие страны все чаще прибегают к различным ограничениям по локализации данных и внедряют соответственные механизмы регулирования в целях реализации политики цифрового протекционизма под предлогом обеспечения национальной безопасности. Эти действия оказывают отрицательное воздействие на конкурентоспособность американских компаний. Соединенные Штаты продолжат вдохновлять другие страны собственным примером и оказывать всяческое противодействие необоснованным барьерам для свободного движения данных и цифровой торговли. Нынешняя администрация продолжит активное сотрудничество с международными партнерами по вопросу продвижения открытых отраслевых стандартов, инновационных продуктов и риск-ориентированных подходов, обеспечивающих создание и внедрение инноваций на международном уровне и свободное движение данных с учетом обеспечения законных интересов Соединенных Штатов в области безопасности.

ОБЕСПЕЧЕНИЕ ЛИДЕРСТВА СОЕДИНЕННЫХ ШТАТОВ АМЕРИКИ В ОБЛАСТИ ПЕРЕДОВЫХ ТЕХНОЛОГИЙ:

Основой влияния Соединенных Штатов в киберпространстве является технологическое преимущество. Соответственно, правительство Соединенных Штатов обеспечит проведение скоординированных действий по защите передовых технологий, в том числе от их кражи нашими противниками, обеспечит поддержку доработки этих технологий и, по возможности, уменьшения барьеров для американских компаний для выхода на рынок. Соединенные Штаты намерены продвигать американские инновации в области кибербезопасности по всему миру следующими методами: 1) использование торговых операций; 2) повышение уровня осведомленности об инновационных инструментах и услугах в области кибербезопасности американского происхождения и производства; 3) разоблачение и противодействие репрессивным режимам, использующим такие инструменты и услуги с целью нарушения прав человека; 4) устранение барьеров по созданию единого глобального рынка кибербезопасности.

ПРОДВИЖЕНИЕ КИБЕРБЕЗОПАСНОСТИ С ПОЛНЫМ ЖИЗНЕННЫМ ЦИКЛОМ:

Правительство Соединенных Штатов выступает за внедрение решений, обеспечивающих кибербезопасность, с полным жизненным циклом, настаивая на внедрении надежных настроек безопасности по умолчанию, адаптируемых, обновляемых продуктов и других передовых практик, созданных на момент поставки продукта. Нашей задачей является определение ясного пути к созданию адаптируемого, устойчивого и безопасного рынка технологий, поощряя производителей к дифференциации продуктов в зависимости от качества их функций безопасности. Правительство Соединенных Штатов будет способствовать внедрению базовых инженерных практик с целью повышения системной устойчивости и разработки проектов, которые выходят из строя и эффективно восстанавливаются при успешной хакерской атаке. Правительство Соединенных Штатов также будет поощрять проведение периодического тестирования и проверок кибербезопасности, устойчивости продуктов и систем во время разработки с использованием передовой практики в перспективных отраслях. Это включает в себя продвижение и использование скоординированного раскрытия уязвимостей, группового тестирования и других инновационных оценок, которые повышают отказоустойчивость перед незаконным использованием или атакой. Правительство Соединенных Штатов намерено провести анализ потенциальных возможностей по улучшению полного (сквозного) жизненного цикла по управлению цифровой идентификацией, в том числе чрезмерной зависимости от номеров социального страхования.

Содействие развитию и защита изобретательских талантов в США

Содействие развитию и защита американских изобретений и инноваций имеет решающее значение для обеспечения стратегического преимущества Соединенных Штатов в киберпространстве. Правительство Соединенных Штатов намерено способствовать созданию инноваций, поощряя учреждения и программы, являющиеся движущей силой конкурентоспособности Соединенных Штатов. Правительство Соединенных Штатов намерено целенаправленно противодействовать неправомерным слияниям и поглощениям, а также бороться с кражей интеллектуальной собственности. Одной из

наших целей является обеспечение лидерства Соединенных Штатов в сфере новых технологий и содействие выявлению и обеспечению поддержки этих технологий со стороны правительства, включая искусственный интеллект, квантовую информатику и телекоммуникационную инфраструктуру следующего поколения.

Приоритеты

СОВЕРШЕНСТВОВАНИЕ МЕХАНИЗМОВ АНАЛИЗА ХАРАКТЕРА ИНВЕСТИЦИЙ И ДЕЯТЕЛЬНОСТИ КОММЕРЧЕСКИХ КОМПАНИЙ НА ТЕРРИТОРИИ США:

Обеспечение конфиденциальности, целостности и доступности телекоммуникационных сетей Соединенных Штатов имеет первостепенное значение для нашей экономики и национальной безопасности. Одной из основных задач является защита телекоммуникационных сетей, от работоспособности которых зависит повседневная жизнь каждого гражданина США. Необходимо обеспечить невозможность их использование или нарушение нормального функционирования иностранным противником с целью нанесения ущерба Соединенным Штатам. Задачей правительства Соединенных Штатов является сбалансирование этих целей путем формализации и упорядочения порядка рассмотрения заявлений на получение лицензий на предоставление услуг связи Федеральной комиссией связи. Правительство Соединенных Штатов будет содействовать повышению прозрачности процедуры получения таких лицензий с целью улучшения ее эффективности.

ОБЕСПЕЧЕНИЕ НАДЕЖНОЙ И СБАЛАНСИРОВАННОЙ СИСТЕМЫ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ:

Надежный механизм защиты интеллектуальной собственности является залогом непрерывного экономического роста и развития инноваций в эпоху цифровых технологий. Правительство Соединенных Штатов продолжит содействовать созданию международной системы прав на интеллектуальную собственность, стимулирующей разработку и внедрение инноваций посредством защиты и обеспечения соблюдения прав интеллектуальной собственности, таких как патенты, товарные знаки и авторские права. Правительство Соединенных Штатов также будет содействовать обеспечению защиты новых секретных технологий и коммерческой тайны, а также противодействовать получению странами-противниками несправедливого преимущества за счет американских исследований и разработок.

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ И ЦЕЛОСТНОСТИ АМЕРИКАНСКИХ ИДЕЙ:

В течение более десяти лет злоумышленники незаконно проникали в коммерческие сети Соединенных Штатов с целью получения конфиденциальной коммерческой информации, принадлежащей американским компаниям. Киберпреступники из других стран украли множество торговых секретов, технических данных и конфиденциальной внутренней информации. Правительство Соединенных Штатов нацелено на противодействие незаконному присвоению технологий и информации технического характера государственного и частного секторов со стороны иностранных конкурентов, сохраняя при этом благоприятный инвестиционный климат.

Повышение качества человеческих ресурсов, обеспечивающих кибербезопасность

Высококвалифицированная рабочая сила в сфере обеспечения кибербезопасности является стратегическим преимуществом для национальной безопасности. Соединенные Штаты нацелены на всестороннее развитие американского кадрового потенциала, одновременно привлекая лучших зарубежных специалистов, разделяющих наши ценности.

Приоритеты

СОЗДАНИЕ И ОБЕСПЕЧЕНИЕ НАДЕЖНОГО КАДРОВОГО РЕЗЕРВА:
Наши конкуренты реализуют программы подготовки трудовых ресурсов, которые могут нанести вред конкурентоспособности Соединенных Штатов в сфере кибербезопасности в долгосрочной перспективе. Правительство Соединенных Штатов продолжит финансировать и расширять программы, которые создают качественный национальный кадровый резерв, как в начальной школе, так и в рамках высших учебных заведений. Нынешняя администрация будет внедрять предложенные Президентом иммиграционные реформы, основанные на заслугах кандидатов, с целью создания в Соединенных Штатах наиболее конкурентоспособного технологического сектора. Достижение таких целей может потребовать принятия нового законодательства или внесения изменений и дополнений в уже существующие законы и подзаконные нормативно-правовые акты.

РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ ДЛЯ ПЕРЕКВАЛИФИКАЦИИ И ПОЛУЧЕНИЯ ОБРАЗОВАНИЯ АМЕРИКАНСКИМИ РАБОЧИМИ:
Нынешняя администрация нацелена на тесное взаимодействие с Конгрессом по вопросам продвижения и активизации образовательных и учебных программ для обучения профессионального кадрового резерва в целях обеспечения кибербезопасности. Такой комплекс мер включает расширение программ подбора кадров, обучения, перепрофилирования на федеральном уровне лиц из самых разных слоев общества и предоставление им возможности прохождения переподготовки для построения карьеры в области обеспечения кибербезопасности.

СОВЕРШЕНСТВОВАНИЕ ПОТЕНЦИАЛА И НАВЫКОВ СОТРУДНИКОВ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ НА ФЕДЕРАЛЬНОМ УРОВНЕ:
В целях улучшения подбора и удержания высококвалифицированных специалистов в области кибербезопасности для нужд федерального правительства, нынешняя администрация продолжит использовать Рамочную программу национальной образовательной инициативы в области кибербезопасности (NICE) для поддержки политики, предусматривающей стандартизованный подход по поиску, найму, обучению и предотвращению утечки высокопрофессиональных специалистов в области кибербезопасности. Кроме того, администрация изучит соответствующие варианты по распределению персонала в области кибербезопасности под руководством DHS в целях надзора за обучением, руководством и распределением персонала в области кибербезопасности по федеральным министерствам и ведомствам, за исключением Министерства обороны и Разведывательного сообщества. Администрация намерена способствовать установлению надлежащего уровня оплаты труда для сотрудников правительства Соединенных Штатов, а также предоставит уникальные образовательные и

карьерные возможности с целью эффективного набора и удержания особо важных специалистов в области кибербезопасности с учетом конкуренции с частными компаниями.

ИСПОЛЬЗОВАНИЕ ИСПОЛНИТЕЛЬНЫХ ПОЛНОМОЧИЙ ДЛЯ ПОИСКА И НАГРАЖДЕНИЯ ТАЛАНТОВ:

Правительство Соединенных Штатов намерено содействовать и повышать уровень профессионализма, уделяя особое внимание обучающему персоналу и высококвалифицированным специалистам в области кибербезопасности. Правительство Соединенных Штатов намерено сотрудничать с представителями частного сектора для разработки и распространения информации о рамочной программе NICE. Такая программа предусматривает единый подход по выявлению дефицита специалистов конкретного направления в области кибербезопасности, а также комплекс мер по подготовке, карьерному росту и удержанию специалистов, которые обладают необходимыми знаниями и навыками по обеспечению защиты и усилению критической инфраструктуры и инновационной базы.

ПРИНЦИП III

Сохранение мира методом принуждения

Угрозы безопасности и экономическим интересам Соединенных Штатов, обусловленные действиями национальных государств и иных групп, которые уже давно существуют за пределами интернета, все чаще находят свое практическое воплощение в киберпространстве. Непрерывные действия и присутствие в киберпространстве стали менять стратегический баланс сил. Нынешняя администрация намерена опубликовать обновленные основополагающие документы, отражающие новую реальность и предоставляющие ориентиры для правительства Соединенных Штатов по достижению стратегических результатов с целью защиты американского народа и нашего образа жизни. Киберпространство больше не будет рассматриваться как отдельное направление политики или какой-либо иной деятельности, не связанной с другими элементами реализации власти на национальном уровне. Соединенные Штаты предусмотрят использование возможностей киберпространства по всем направлениям реализации власти на национальном уровне.

ЦЕЛЬ: выявление, противодействие, обезвреживание, снижение уровня угрозы и сдерживание действий в киберпространстве, которые нарушают или противоречат национальным интересам, с целью обеспечения превосходства Соединенных Штатов в пределах киберпространства.

Обеспечение кибербезопасности при помощи Норм ответственного поведения со стороны государств

Соединенные Штаты намерены продвигать стандарты ответственного поведения государств в киберпространстве с учетом норм международного права, добровольной приверженности факультативным нормам ответственного поведения государств в мирное время, и поставить на рассмотрение практические меры по укреплению доверия с целью снижения риска конфликтов, обусловленных хакерской деятельностью. Эти принципы должны заложить основу для совместного противодействия безответственному поведению государства, несовместимого с требованиями этого механизма.

Приоритеты

ПООЩРЕНИЕ ВСЕОБЩЕГО СОБЛЮДЕНИЯ НОРМ, ОБЕСПЕЧИВАЮЩИХ КИБЕРБЕЗОПАСНОСТЬ:
Международное право и факультативные нормы ответственного поведения государства в киберпространстве содержат стандарты безопасности, определяющие приемлемое поведение для всех государств, и способствуют большей предсказуемости и стабильности в киберпространстве. Соединенные Штаты намерены поощрять другие страны публично подтверждать свою приверженность этим принципам и взглядам путем информационного продвижения и участия в многосторонних форумах. Увеличение общественной поддержки со стороны Соединенных Штатов и других государств будет способствовать формированию общепринятых ожиданий поведения государства, а также большей предсказуемости и стабильности в киберпространстве.

Отличительные признаки неприемлемого поведения в киберпространстве и меры противодействия

Соединенные Штаты нацелены на достижение консенсуса по вопросу определения ответственного поведения государства в киберпространстве, тем не менее, следует также предусмотреть комплекс мер воздействия за безответственное поведение, которое наносит ущерб Соединенным Штатам и нашим партнерам. В нашем распоряжении имеются весь спектр инструментов федеральной власти, позволяющих предотвратить, надлежащим образом отреагировать и сдержать хакерские атаки против Соединенных Штатов. В такой инструментарий входят дипломатические, информационные, военные (кинетические и цифровые), финансовые, разведывательные методы, публичное определение и возможности правоохранительных органов. Соединенные Штаты стремятся оформить в виде официального документа и внедрить в повседневную деятельность достигнутые договоренности с партнерами-единомышленниками в целях определения и сдерживания хакерской деятельности при помощи комплексных стратегий, предполагающих применение быстрых и прозрачных мер воздействия, являющихся чувствительными для злоумышленников, наносящих ущерб Соединенным Штатам или нашим партнерам.

Приоритетны

ЦЕЛЕВОЕ ЛИДЕРСТВО, СОВМЕСТНАЯ ОБРАБОТКА ИНФОРМАЦИИ:
Разведывательное сообщество сохранит свое преимущество использования всех цифровых разведывательных данных, полученных из любых источников, с целью выявления и определения хакерских действий, угрожающих национальным интересам Соединенных Штатов. Объективные и актуальные данные будут передаваться правительству Соединенных Штатов, которое совместно с основными партнерами определит враждебные иностранные государства, негосударственные киберпрограммы, намерения, практические возможности, исследования и разработки, тактику действий и перечень неотложных мер реагирования в целях защиты интересов Америки как внутри страны, так и за рубежом.

ПРИМЕНЕНИЕ МЕР РЕАГИРОВАНИЯ:
Соединенные Штаты разработают перечень неотложных и прозрачных мер реагирования, используемых в соответствии с принятыми на себя обязательствами по сдерживанию неприемлемого поведения в будущем. Нынешняя администрация нацелена проводить межведомственное планирование практических действий на соответственные временные периоды до, во время и после применения мер реагирования с целью обеспечения своевременного и последовательного реагирования и сдерживания хакерских атак. Соединенные Штаты будут совместно с партнерами (при необходимости) осуществлять практические действия по применению мер реагирования в отношении хакеров в ответ на их противоправные действия, наносящие ущерб интересам Америки и граждан США.

СОЗДАНИЕ ИНИЦИАТИВЫ ПО КОМПЛЕКСУ МЕР СДЕРЖИВАНИЯ В КИБЕРПРОСТРАНСТВЕ:
Применение мер реагирования будет более эффективным и оказывать более сильное влияние при совместном их применении более широкой коалицией государств-единомышленников. Соединенные Штаты планируют ввести в действие международную

Инициативу по сдерживанию хакерских атак в целях создания такой коалиции и разработки адаптированных стратегий, позволяющих противникам уяснить последствия своего злонамеренного поведения в киберпространстве. Соединенные Штаты намерены сотрудничать с государствами-единомышленниками по вопросам координации и оказания поддержки применения мер реагирования друг друга в отношении серьезных злоумышленных инцидентов в киберпространстве, в том числе посредством обмена разведывательными данными, подкрепленными источниками, публичными заявлениями о поддержке мер реагирования, а также совместным применением мер реагирования против злоумышленников.

БОРЬБА С ВРЕДОНОСНЫМ ВЛИЯНИЕМ И ИНФОРМАЦИОННЫЕ ОПЕРАЦИИ В КИБЕРПРОСТРАНСТВЕ:

Соединенные Штаты будут использовать все необходимые инструменты, имеющие в распоряжении федеральных органов власти, в целях выявления и противодействия потокам злоумышленного влияния в режиме онлайн и информационных кампаний, а также негосударственной пропаганде и дезинформации. Эти действия охватывают взаимодействие с иностранными государствами-партнерами, представителями частного сектора, научных кругов и гражданского общества в целях выявления, противодействия и предотвращения использования цифровых платформ для проведения злоумышленных информационных компаний иностранными субъектами при условии соблюдения гражданских прав и свобод.

ПРИНЦИП IV

Продвижение американского влияния

Весь мир считает Соединенные Штаты родиной большей части инноваций сегодняшнего интернета, а также лидером, который может решить широкий спектр международных вызовов и проблем, порожденных киберпространством. Соединенные Штаты будут активно обеспечивать свою позицию международного лидера с целью продвижения американского влияния и решения увеличивающегося количества угроз и вызовов ее интересам в киберпространстве. Сотрудничество с союзниками и партнерами играет важную роль для обеспечения использования трансграничных коммуникаций, создания контента и ведения коммерческих операций, осуществление которых возможно при наличии открытой, совместимой интернет архитектуры.

ЦЕЛЬ: Сохранение долгосрочной открытости, совместимости, безопасности и надежности интернета в целях обеспечения интересов Соединенных Штатов.

Продвижение открытого, совместимого, надежного и безопасного интернета

Создание международной сети интернет является одним из самых больших достижений со времен промышленной революции, что стало катализатором значительного прогресса в области торговли, здравоохранения, коммуникаций и создания иной национальной инфраструктуры. В то же время многовековая борьба за права человека и основные свободы теперь стала протекать в режиме онлайн. Свобода слова, мирных собраний и объединений, а также право на неприкосновенность частной жизни находятся под угрозой. Несмотря на беспрецедентный рост, экономический и социальный потенциал интернета по-прежнему ограничивается онлайн-цензурой и иными ограничениями. Соединенные Штаты твердо придерживаются своих принципов по защите и развитию открытого, совместимого, надежного и безопасного интернета. Америка будет продвигать свое видение открытого интернета в качестве международного стандарта. Мы будем всячески противодействовать попыткам авторитарных государств, рассматривающих открытый интернет как политическую угрозу, превратить свободный и открытый интернет в авторитарную сеть с тотальным контролем под видом обеспечения безопасности или борьбы с терроризмом.

Приоритеты

ЗАЩИТА И ОБЕСПЕЧЕНИЕ СВОБОДЫ В ИНТЕРНЕТЕ:
Правительство Соединенных Штатов определяет свободу слова в интернете как реализацию в режиме онлайн прав человека и основных свобод - таких, как свобода слова, объединений, мирных собраний, вероисповеданий или убеждений, а также права на неприкосновенность частной жизни в интернете - независимо от границ или средств передачи информации. Кроме того, свобода слова в интернете также подразумевает свободное распространение информации в режиме онлайн, способствующей развитию международной торговли и коммерции, разработке и внедрению инноваций и укрепляет как национальную, так и международную безопасность. Таким образом, принципы свободы интернета Соединенных Штатов неразрывно связаны с нашей национальной безопасностью. Свобода слова в интернете также является основным руководящим

принципом для других вопросов внешней политики Соединенных Штатов, таких как борьба с киберпреступностью и терроризмом. С учетом важности этого принципа, Соединенные Штаты будут оказывать другим странам содействие по вопросам продвижения свободы слова в интернете при помощи таких площадок, как Коалиция за свободу в интернете (Freedom Online Coalition), членом-основателем которой являются Соединенные Штаты.

СОВМЕСТНАЯ РАБОТА С ЕДИНОМЫШЛЕННИКАМИ - СТРАНАМИ, ПРЕДСТАВИТЕЛЯМИ ПРОМЫШЛЕННОГО СЕКТОРА, НАУЧНЫХ КРУГОВ И ГРАЖДАНСКОГО ОБЩЕСТВА:

Соединенные Штаты продолжат совместную работу с единомышленниками – странами, представителями промышленного сектора и гражданского общества и другими заинтересованными сторонами в целях продвижения прав человека и свободы слова в интернете по всему миру, противодействуя авторитарным действиям по цензуре и оказанию влияния на развитие интернета. Правительство Соединенных Штатов продолжит оказывать поддержку гражданскому обществу, содействуя всестороннему развитию технологий, обучению основам цифровой безопасности, продвижению установленных требований в рамках проводимой политики и исследований. Целью этих программ является повышение возможностей отдельных граждан, активистов, правозащитников, независимых журналистов, организаций гражданского общества и маргинальных групп населения безопасно получать доступ к интернету без цензуры и содействовать свободе слова в интернете на местном, региональном, национальном и международном уровнях.

ПРОДВИЖЕНИЕ МНОГОСТОРОННЕЙ МОДЕЛИ УПРАВЛЕНИЯ ИНТЕРНЕТОМ:

На международной арене Соединенные Штаты будут прилагать усилия по внедрению многосторонней модели управления интернетом и пресекать попытки по созданию государство-ориентированной инфраструктуры, нивелирующей открытость и свободу, препятствующей созданию и внедрению инноваций, а также представляющей угрозу для функциональности интернета. Многосторонняя модель управления интернетом отличается прозрачностью, процедурами управления «снизу-вверх», основанными на консенсусе, и позволяет правительствам, частному сектору, гражданскому обществу, научным кругам и техническому сообществу принимать в ней участие на равных. Правительство Соединенных Штатов будет защищать открытый, функционально совместимый интернет на многосторонних и международных форумах посредством активного участия в основных организациях, таких как Корпорация по присвоению имен и номеров в интернете, Форум по управлению использованием интернета, Организация Объединенных Наций и Международный союз электросвязи.

ПРОДВИЖЕНИЕ ФУНКЦИОНАЛЬНО СОВМЕСТИМОЙ И НАДЕЖНОЙ ИНФРАСТРУКТУРЫ СВЯЗИ И ДОСТУПА К ИНТЕРНЕТУ:

Соединенные Штаты будут способствовать развитию открытой, функционально совместимой, надежной и безопасной инфраструктуры связи и точек доступа к интернету. Такие инвестиции предоставят американским компаниям большие конкурентные преимущества, противодействуя влиянию вертикального вмешательства государства в областях стратегического значения. Такой подход также позволит защищать безопасность

Соединенных Штатов и их коммерческие интересы, укрепляя конкурентоспособность Соединенных Штатов в рамках мировой цифровой экономики. Нынешняя администрация будет оказывать поддержку и продвигать открытые отраслевые стандарты, в основу которых положены проверенные технологические принципы.

ЗАВОЕВАНИЕ И УДЕРЖАНИЕ ПОЗИЦИЙ НА МЕЖДУНАРОДНЫХ РЫНКАХ АМЕРИКАНСКИМИ НОВАЦИЯМИ И РАЗРАБОТКАМИ:

Американские изобретатели и специалисты в области безопасности внесли значительный вклад в разработку продуктов и услуг, которые улучшают возможности для общения и взаимодействия людей по всему миру, защищают инфраструктуру, данные и устройства связи по всему миру. Соединенные Штаты нацелены на завоевание зарубежных рынков американскими разработками, в том числе новыми технологиями, которые могут снизить стоимость обеспечения безопасности. Соединенные Штаты также будут предоставлять консультации по вопросам развертывания инфраструктуры, инноваций, управления рисками, политик и стандартов для расширения проникновения интернета и обеспечения функциональной совместимости, безопасности и стабильности. Кроме того, Соединенные Штаты намерены взаимодействовать с международными партнерами, правительствами стран, представителями промышленных кругов, гражданским обществом, техническими специалистами и учеными с целью расширения областей внедрения, а также повышения осведомленности о передовых практиках в сфере кибербезопасности во всем мире.

Создание международного киберпотенциала

Создание потенциала позволяет партнерам защищать себя и оказывать Соединенным Штатам содействие в устранении угроз, нацеленных против общих интересов, с одновременной реализацией более широких целей дипломатического, экономического характера, а также в области безопасности. Инициативы по наращиванию киберпотенциала позволяют Соединенным Штатам выстраивать стратегические партнерские отношения, которые способствуют продвижению передовой практики в сфере кибербезопасности через призму общего видения открытого, функционально совместимого, надежного и безопасного Интернета, привлекательного для инвестиций и позволяющего открыть новые рынки. Кроме того, создание потенциала открывает дополнительные возможности по обмену информацией о киберугрозах, позволяя правительству Соединенных Штатов и нашим партнерам обеспечить лучшую защиту внутренней критически важной инфраструктуры и международных цепочек поставок, а также концентрировать кибервозможности всех правительственных структур. Американское содействие по наращиванию потенциала партнеров в сфере кибербезопасности имеет решающее значение для поддержания американского влияния в целях противодействия глобальным конкурентам. Создание киберпотенциала позволит международным партнерам вести политику и осуществлять практические действия в качестве эффективных партнеров в рамках Инициативы Кибер (информационного) сдерживания, возглавляемой Соединенными Штатами.

Приоритеты

УВЕЛИЧЕНИЕ УСИЛИЙ ПО НАРАЩИВАНИЮ КИБЕРПОТЕНЦИАЛА:

Многие союзники и партнеры Соединенных Штатов обладают уникальными кибер-возможностями, которые могут дополнять наши возможности. Соединенные Штаты нацелены на работу по укреплению потенциала и функциональной совместимости с такими нашими союзниками и партнерами с целью оптимизации совместных навыков, ресурсов, возможностей и интересов перед лицом общих угроз. Наши партнеры также могут оказать содействие по выявлению, сдерживанию и ликвидации таких общих угроз в киберпространстве. С целью обеспечения эффективной защиты международными партнерами своей цифровой инфраструктурой и борьбы с общими угрозами наряду с получением выгод экономического и социального характера, получаемых от Интернета и ИКТ, Соединенные Штаты продолжать выстраивать национальную систему обеспечения кибербезопасности. Соединенные Штаты активизируют усилия по автоматизированному обмену информацией о киберугрозах, имеющей практическую ценность, будут содействовать укреплению координации в области кибербезопасности и обменов аналитической и технической информацией. Кроме того, Соединенные Штаты намерены снизить наносимый ущерб и влияние транснациональной киберпреступности и террористической деятельности путем налаживания сотрудничества и укрепления возможностей органов безопасности и правоохранительных органов наших партнеров для наращивания необходимого киберпотенциала.

ПРИМЕЧАНИЯ