Мировая политика
Правильная ссылка на статью:
Хуанфу Ч. Национальная стратегия кибербезопасности США и ее глобальное влияние // Мировая политика. 2024. № 4. DOI: 10.25136/2409-8671.2024.4.72317 EDN: JMHOEF URL: https://nbpublish.com/library_read_article.php?id=72317

Национальная стратегия кибербезопасности США и ее глобальное влияние

Хуанфу Чжэнхуэй

кандидат политических наук

аспирант; кафедра международная безопасность; Московский государственный университет им. М. В. Ломоносова

119234, Россия, г. Москва, ул. Ленинские горы, 1

hfstudy@yandex.ru

Статья из рубрики "Информационные войны"

DOI:

10.25136/2409-8671.2024.4.72317

EDN:

JMHOEF

Дата направления статьи в редакцию:

07-11-2024

Дата публикации:

14-11-2024

Аннотация: В условиях все более интенсивной цифровизации кибербезопасность становится ключевым элементом мирового политического дискурса. США, являясь родиной интернета и лидером в области информационных технологий, существенно влияют на формирование мировых стандартов управления кибербезопасностью. Настоящая статья представляет анализ американских официальных документов для оценки изменений в политике кибербезопасности администрации Байдена и их потенциального воздействия на международные отношения и глобальные стандарты управления киберпространством. Анализ начинается с рассмотрения рыночно-ориентированного подхода времён Клинтона, переходит к стратегическому включению кибербезопасности в национальную архитектуру безопасности при младшем Буше, а также касается различий в подходах администраций Обамы и Трампа. Особое внимание

уделено детальному обзору «Национальной стратегии кибербезопасности» администрации Байдена, подчеркивающей инновации в укреплении сетевого регулирования, углублению сотрудничества между государством и частным сектором и реформированию ответственности за кибербезопасность. Статья также исследует, как эти изменения могут повлиять на международные стандарты в сфере кибербезопасности, и анализирует стратегическое значение и глобальные последствия сотрудничества Китая и России в этой области, обосновывая их важность для будущего глобального управления киберпространством. Методология исследования основана на анализе официальных документов и стратегий администрации США в области кибербезопасности. Статья выявляет тенденции и стратегические изменения, оценивая их глобальное воздействие и взаимодействие с частным сектором. Научная новизна данной статьи выражается в тщательном анализе реформирования стратегии кибербезопасности при администрации Байдена, особенно в контексте её влияния на международные отношения и глобальные стандарты управления киберпространством. Исследование выявляет углубление взаимодействия между государством и частным сектором, а также усиление регулятивных механизмов, что отличается от предыдущих подходов, основанных на добровольной основе. Особое внимание уделяется тенденции перехода глобальной сетевой безопасности от единой модели к многоуровневому сотрудничеству и конкуренции. Статья подчеркивает, что внедрение рамок нулевого доверия может спровоцировать глобальные изменения, усиливающие сложность и многообразие международных отношений в области кибербезопасности. Основным выводом работы является признание стратегического значения сотрудничества между Китаем и Россией в кибербезопасности, что существенно влияет на глобальное управление киберпространством и подчеркивает необходимость международной координации в этой сфере.

Ключевые слова:

кибербезопасность, управление кибербезопасностью, Кибербезопасность администрации Байдена, цифровой суверенитет, безопасность информационной эры, Национальная стратегия кибербезопасности, Модель нулевого доверия, Международные киберотношения, Сотрудничество в киберполитике, Глобальное управление кибербезопасностью

Стратегия кибербезопасности США прошла через множество этапов развития с момента зарождения интернета, каждый из которых значительно отражает влияние технологического прогресса, глобальной политической обстановки и внутренних политических дебатов. В период правления Клинтона (1993-2001) политика в области кибербезопасности в основном была не регулируемой и ориентированной на рынок. В 1997 году администрация Клинтона приняла «Основы глобальной электронной коммерции»[1], подчеркнув поддержку свободы технологий и инноваций, что способствовало коммерциализации интернета и быстрому развитию технологий, но также обнажило недостатки в области кибербезопасности.

С началом XXI века значимость кибербезопасности начала постепенно возрастать. После терактов 11 сентября 2001 года администрация младшего Буша немедленно отреагировала, разработав в 2003 году «Национальную стратегию безопасности киберпространства» [2], которая впервые включила кибербезопасность в архитектуру национальной безопасности США, символизируя переход от рыночного управления к

государственному вмешательству. Фактически, это первая стратегическая инициатива, которая определяет необходимость координации и централизации усилий всех федеральных ведомств для защиты национального информационного пространства [3]. Данный документ, а также другие цели указывают на необходимость укрепления координации между Министерством обороны США и национальными разведывательными службами в области противодействия киберугрозам. Несмотря на начало создания более структурированных мер обороны, акцент все еще делался на роли рынка.

Во время президентства Барака Обамы (2009-2017 гг.) не была разработана новая стратегия кибербезопасности в виде формализованного документа, однако администрация активно стремилась укрепить взаимодействие с частным сектором, особенно уделяя внимание обмену информацией о киберугрозах. Это стало частью усилий по созданию гибкой и эффективной системы защиты от кибератак, которые могли бы нанести значительный ущерб экономике и социальной структуре страны [4]. Значимость этих усилий была особенно подчеркнута в результате кибератаки на киностудию Sony Pictures в 2013 году, осуществленной Северной Кореей в ответ на планируемый выпуск фильма, издевательски относящегося к её лидеру. Атака привела к масштабной утечке конфиденциальной информации, включая личные данные сотрудников, внутреннюю переписку и неопубликованные фильмы, что серьёзно ударило по репутации и финансам компании. Кибератака на Sony Pictures выявила значительные уязвимости в системе защиты информационной инфраструктуры крупных корпораций и подтвердила необходимость усиления национальной и корпоративной кибербезопасности [5]. Попытки администрации Обамы ужесточить меры защиты, в том числе путем законодательного введения обязательных стандартов для критически важной инфраструктуры, встретили сопротивление в Конгрессе из-за давления со стороны частного сектора и опасений, связанных с возможными финансовыми затратами и ограничением корпоративной автономии [6]. В ответ на это администрация Обамы сфокусировала свои усилия на развитии добровольных партнерских отношений между государством и частным сектором, продолжая поддерживать инновации в области технологий кибербезопасности и укрепляя координацию мер реагирования на киберугрозы на национальном уровне, в частности, через такие структуры, как Национальный центр кибербезопасности и интеграции коммуникаций (NCCIC) и другие государственные агентства.

Во время администрации Трампа (2017-2021) в своей «Национальной стратегии кибербезопасности» 2018 года был сделан акцент на активной защите и наступательных действиях в киберпространстве, подчеркивая стратегический переход от преимущественно оборонительной позиции к более агрессивной и инициативной роли в кибербезопасности [7]. Этот подход позволял не только реагировать на угрозы, но и предотвращать их, усиливая национальную и международную безопасность через стратегически организованные кибероперации. В рамках администрации Трампа произошли значительные изменения в политике кибербезопасности, включая приостановку диалога по кибербезопасности между Китаем и США, что было связано с обвинениями в адрес Китая в кибершпионаже и недобросовестной конкуренции. Дополнительно, было усилено давление на китайские интернет-компании, включая такие крупные фирмы, как Huawei и ZTE, которые столкнулись с санкциями и ограничениями, основанными на обвинениях в угрозе национальной безопасности. Эти действия привели к определенному отступлению США от ранее занимаемых лидирующих позиций в глобальной системе управления киберпространством. Такой подход способствовал возникновению новых вызовов в киберпространстве для последующей администрации

Байдена, которой предстояло решать проблемы, связанные с восстановлением международного сотрудничества и доверия, а также с реформированием политики кибербезопасности для адаптации к новым глобальным вызовам и угрозам. Администрация Трампа также активно использовала киберпространство для продвижения национальных интересов, что означало применение кибервозможностей не только для защиты, но и для достижения стратегических целей США на международной арене. Это включало использование кибероперации как инструмента политического давления и защиты экономических интересов, подчеркивая роль кибербезопасности как важного элемента национальной стратегии безопасности.

Администрация Байдена (2021-настоящее время) совершила заметный пересмотр политики в области кибербезопасности. В мае 2021 года, в ответ на инцидент с атакой SolarWinds, Microsoft Exchange и с топливопроводом Colonial Pipeline был издан «Административный приказ о кибербезопасности», требующий усиления защиты критически важной инфраструктуры и создание Комиссии по обзору кибербезопасности. В марте 2023 года опубликованная «Национальная стратегия кибербезопасности» впервые включила регулирование в ключевые позиции национальной безопасности, что ознаменовало значительный поворот в американской стратегии кибербезопасности. Эти стратегические корректировки и эволюция политики не только отражают зрелость взглядов США на кибербезопасность, но и демонстрируют глубокое влияние технологического прогресса и международной политико-экономической обстановки на национальную стратегию кибербезопасности.

Новая стратегия кибербезопасности администрации Байдена

В связи с быстрым развитием цифровых технологий и увеличением угроз кибербезопасности, правительство США приняло ряд инновационных мер для противодействия этим вызовам. 12 мая 2021 года президент США Байден подписал указ о кибербезопасности и защите сетей федерального правительства от кибератак [8], который отмечает значимый поворот в стратегии кибербезопасности США. Этот приказ требует от всех поставщиков ИТ-услуг уведомлять правительство о любых потенциальных кибератаках, что обеспечивает своевременный ответ и соответствующие действия со стороны государства. Кроме того, приказ предусматривает создание Комитета по рассмотрению кибербезопасности, состоящего из экспертов из публичного и частного секторов, задача которого — анализировать инциденты сетевых атак и предлагать меры по защите от будущих атак, что направлено на укрепление кибероборонны через коллективные усилия и обмен ресурсами.

После этого приказа, 2 марта 2023 года, администрация Байдена выпустила "Национальную стратегию кибербезопасности" [9], которая дополнительно укрепляет рамки управления кибербезопасностью, отходя от традиционной модели, основанной на добровольном саморегулировании рыночных субъектов и акцентах на сотрудничестве между государственным и частным секторами и обмене информацией. Новая стратегия четко включает "регулирование" в важные аспекты национальной безопасности, подчеркивая ведущую роль правительства в области кибербезопасности, особенно в защите критически важной инфраструктуры и ключевых сфер национального значения. Кроме того, стратегия перераспределяет обязанности по кибербезопасности, уточняя роли и обязанности всех участников в поддержании кибербезопасности, тем самым укрепляя системный фундамент кибербезопасности. Эти политические меры не только изменили способы управления кибербезопасностью внутри США, но и оказали глубокое влияние на правила управления киберпространством на мировом уровне. Путем

введения более строгих регулятивных мер и перераспределения ответственности, США стремятся способствовать созданию более защищенной и оборонительной глобальной сетевой среды. Этот поворот в стратегии является важным дополнением к предыдущему подходу, основанному на решении проблем кибербезопасности силами рынка, и демонстрирует необходимость государственного вмешательства и международного сотрудничества в условиях усложняющихся вызовов кибербезопасности.

Опубликованная администрацией Байдена "Национальная стратегия кибербезопасности" направлена на создание более защищенной и устойчивой цифровой экосистемы. Стратегия усиливает инвестиции в киберинфраструктуру, укрепляет партнерские отношения с частным сектором и повышает контроль за ключевыми секторами, особенно подчеркивая механизмы ответственности для компаний, не исполняющих обязательства по безопасности. Центральная цель стратегии — создать "цифровую экосистему с более высоким уровнем внутренней защиты, устойчивости и соответствующую американским ценностям". В стратегии акцент на "защите" подразумевает усиление мер кибербезопасности на всех этапах проектирования и эксплуатации, что делает стоимость атаки значительно выше, чем стоимость защиты, эффективно перенося контроль от атакующих к защищающимся. "Устойчивость" означает способность сетевых систем быстро восстанавливаться после неудач и предотвращать катастрофические последствия, обеспечивая, чтобы киберинциденты не оказывали системное воздействие на реальный мир. Кроме того, "ценности" в стратегии означают, что цифровая экосистема должна отражать ценности ее создателей и пользователей, с ясным соблюдением основных демократических принципов США в процессе ее создания.

Для достижения этих целей стратегия администрации Байдена фокусируется не только на реформе внутренней политики, но и активно ищет международное сотрудничество, особенно в борьбе против транснациональной киберпреступности и укреплении глобального управления киберпространством. США совместно с союзниками, такими как Европейский союз и НАТО, стремятся к созданию международных стандартов и обмену лучшими практиками. Это направлено на повышение уровня кибербезопасности на глобальном уровне, укрепление сотрудничества с союзниками, продвижение унификации глобальных стандартов кибербезопасности, что позволит совместно противостоять цифровым вызовам и угрозам. Посредством этой всеобъемлющей стратегии администрация Байдена демонстрирует осознание новых вызовов в области кибербезопасности и готовность к их преодолению, стремясь повысить защиту и устойчивость, чтобы обеспечить способность США и их глобальных партнеров справляться с возрастающей сложностью кибератак, поддерживая стабильность национальной и глобальной кибербезопасности.

Переосмысление обязанностей и стимулов в рамках “Национальной стратегии кибербезопасности”

США долгое время опирались на модель управления кибербезопасностью, основанную на рыночных принципах и автономии отраслей, что часто возлагало тяжесть ответственности на конечных пользователей, малый бизнес и местные власти, которые обычно не располагают необходимыми профессиональными навыками и ресурсами, что делает их бессильными перед лицом всё более сложных киберугроз. В связи с этим срочно требуется системная перестройка ролей, обязанностей и ресурсов в киберпространстве.

Правительство Байдена, признавая эту проблему, выпустило "Национальную стратегию кибербезопасности", которая предлагает два фундаментальных изменения. Стратегия

выступает за перераспределение обязанностей по кибербезопасности от индивидуальных пользователей, малого бизнеса и местных властей к менеджерам цифровых экосистем, обладающим наилучшими возможностями, таким как федеральное правительство и интернет-провайдеры. Федеральному правительству особенно поручается защита собственных сетевых систем и критически важной инфраструктуры, а также использование своих ключевых функций, включая дипломатию, разведку, экономические санкции, правоприменение и проведение операций для эффективного противодействия киберугрозам [10]. Владельцы и операторы критической инфраструктуры, производители оборудования, разработчики программного обеспечения, поставщики услуг и другие ключевые участники также будут нести большую ответственность за кибербезопасность.

Стратегия также акцентирует внимание на пересмотре стимулирующих механизмов для поощрения долгосрочных инвестиций. Правительство поощряет защитников сетей к принятию долгосрочных решений, а не к зависимости от временных исправлений, предлагая финансовую поддержку, налоговые льготы и другие формы стимулов, чтобы коренным образом усилить киберзащиту. Эти меры реформируют распределение обязанностей по кибербезопасности и вводят новые стимулирующие механизмы, целью которых является обеспечение стабильности и безопасности киберпространства. Эта стратегия представляет собой современное применение теории "социального контракта" Запада, определяя обязанности и права всех сторон, создавая тем самым более справедливую и эффективную модель управления кибербезопасностью. Ожидается, что такой подход окажет значительное влияние на кибербезопасность в США и во всем мире.

Агентство по кибербезопасности и защите инфраструктур США (CISA) является ключевым элементом национальной архитектуры кибербезопасности, отвечающим за координацию и укрепление кибербезопасности и защиты инфраструктур по всей стране. В дальнейшей реализации "Национальной стратегии кибербезопасности" [11], опубликованной в марте 2023 года, CISA объявило о трёхлетнем "Стратегическом плане по кибербезопасности на 2024-2026 финансовые годы", опубликованном 4 августа 2023 года. Этот план определяет три долгосрочные цели, направленные на улучшение киберзащиты США и продвижение всей национальной сетевой среды в сторону большей безопасности и устойчивости.

В рамках цели "Устранение непосредственных угроз" CISA планирует сотрудничать с внутренними и внешними партнёрами для совместного противодействия сетевым вторжениям и разрушительным действиям, направленным против США. Стратегия включает активное наблюдение и защитные меры, а также преследование и вмешательство в деятельность потенциальных опасных субъектов. Достижение этой цели будет осуществляться через усиление обмена разведданными, повышение скорости и эффективности реагирования на инциденты, а также проведение совместных операций для подавления или устранения угроз для американской сетевой инфраструктуры.

Цель "Укрепление ландшафта" направлена на сокращение возможности разрушительных сетевых вторжений путём продвижения, поддержки и оценки эффективных практик безопасности и устойчивости. CISA будет разрабатывать и продвигать строгие стандарты безопасности и передовые практики, помогая государственным и частным организациям улучшить свои способности киберзащиты. Это включает усиление безопасности критически важной инфраструктуры, укрепление мер по защите данных и повышение способности сетевых систем к реагированию и восстановлению.

Цель "Способствование масштабированию безопасности" рассматривает кибербезопасность как основную проблему безопасности, приоритизируя внедрение мер безопасности на этапе проектирования продуктов. CISA будет сотрудничать с технологическими компаниями, производителями и дизайнерами для интеграции защитных функций и мер в новые продукты и услуги с самого начала. Это направлено на продвижение всей отрасли к более безопасному и надёжному развитию, минимизируя уязвимости и риски на исходном уровне.

Реализация этих стратегических целей позволит CISA активно и ключевым образом участвовать в обеспечении национальной кибербезопасности и повышении устойчивости инфраструктуры. Эти меры помогут США создать более безопасную, устойчивую и адаптивную цифровую среду, обеспечивая твёрдую защиту национальной безопасности.

Реализация модели нулевого доверия и её влияние на международную безопасность

На фоне быстрого развития цифровых технологий, реализация модели нулевого доверия в области кибербезопасности оказывает глубокое влияние на международную обстановку. Эта стратегия играет ключевую роль в увеличении сложности и стоимости стратегических взаимодействий в области военной и сетевой безопасности. Модель нулевого доверия, усиливая аутентификацию и контроль доступа, эффективно защищает ключевые военные связи и данные, обеспечивая защиту передаваемой информации от кражи или искажения, тем самым поддерживая глобальное технологическое превосходство США и их союзников.

"Меморандум для руководителей исполнительных департаментов и ведомств США"[12] от 28 января 2022 года подробно описывает решение правительства США перейти к архитектуре нулевого доверия (ZTA) для усиления кибербезопасности. Как подчеркнул президент Байден в исполнительном указе №14028, "постепенное улучшение не может обеспечить необходимую безопасность; напротив, федеральному правительству нужны смелые изменения и значительные инвестиции для защиты важнейших учреждений, поддерживающих американский образ жизни." Политика перехода федерального правительства к архитектуре нулевого доверия и использование преимуществ облачной инфраструктуры гарантируют, что все федеральные агентства достигнут минимальных стандартов безопасности, установленных правительством. Модель нулевого доверия следует принципу "никогда не доверяй, всегда проверяй", применяя строгие меры аутентификации и авторизации как для внутренних, так и для внешних пользователей, обеспечивая высокий уровень безопасности. Этот подход революционно меняет уровень кибербезопасности, особенно в защите чувствительной военной связи и данных. Отчёт о положении в области кибербезопасности в США[13] за март 2024 года еще раз подчеркивает необходимость для США внедрения модели нулевого доверия для ответа на усиливающиеся киберугрозы. Это стратегическое изменение стимулирует развитие международной системы управления сетями в направлении более строгой и систематизированной организации. Установление новых стандартов кибербезопасности предоставляет международному сообществу модель для подражания, которая может направить усилия международного сообщества на более согласованное и унифицированное управление сетями, особенно в таких областях, как аутентификация, защита данных и трансграничный поток данных.

В то же время, по мере увеличения глобальной зависимости от цифровых технологий, особенно искусственного интеллекта, страны увеличивают инвестиции в кибербезопасность и постепенно формируют уникальные режимы управления.

Европейский союз акцентирует внимание на "цифровом суверенитете" и "защите приватности", регулируя обработку данных и стандарты защиты приватности согласно Общему регламенту по защите данных (GDPR). Китай и Россия рассматривают кибербезопасность как продолжение государственного суверенитета, приоритетно занимаясь информационной безопасностью и контролем правительства над интернетом, внедряя строгую политику цензуры и локализации данных для защиты национальной безопасности и общественной стабильности. США традиционно следуют рыночно-ориентированной модели управления кибербезопасностью, сосредотачиваясь на технологических инновациях и решениях, лидирующих в отрасли, но также постепенно усиливают вмешательство правительства в область кибербезопасности.

В целом, глобальные тенденции в управлении кибербезопасностью переходят от единой модели к многоуровневому сотрудничеству и конкуренции. Реализация модели нулевого доверия, ожидается, вызовет цепную реакцию на глобальном уровне, стимулируя развитие технологий, политики и международных отношений, направляя международную обстановку к большей сложности и разнообразию. Перемены в политике кибербезопасности США направлены на сотрудничество с международным сообществом для создания объединенного фронта против глобальных киберугроз, улучшения кибербезопасности как внутри страны, так и за рубежом, а также на сохранение лидирующих позиций в быстро меняющейся глобальной среде.

Сотрудничество Китая и России в области кибербезопасности: стратегическое дополнение и международное влияние

В условиях современного развития международных отношений, где кооперация и конкуренция образуют неразделимую дихотомию, особенно на фоне углубления цифровизации и глобализации, кибербезопасность становится ключевой сферой на глобальной политической арене, затрагивающей важнейшие аспекты национальной безопасности и международного сотрудничества. Недавно сотрудничество между Китаем и Россией в этой критически важной области углубилось, что демонстрирует стратегическое дополнение двух стран в противостоянии кибервызовам. Как сообщил руководитель Департамента международной информационной безопасности МИД России Артур Лукманов, сотрудничество не ограничивается двусторонним уровнем, но также включает совместные позиции и действия на многосторонних форумах.

Сотрудничество Китая и России в области кибербезопасности охватывает несколько аспектов: во-первых, две страны усиливают свои возможности противодействия киберугрозам через обмен информацией и разведданными о киберугрозах, включая вредоносное ПО, модели кибератак и активности в рамках продвинутых постоянных угроз (APT). Во-вторых, стороны сотрудничают в области технологий и стратегического развития, совместно разрабатывая решения и защитные системы кибербезопасности, что улучшает их способности защищать свои сети, одновременно противостоя определенным технологическим санкциям или ограничениям со стороны западных стран. Кроме того, Китай и Россия продвигают в международном управлении интернетом законы и политики кибербезопасности, отвечающие их интересам, укрепляя государственный контроль над национальным киберпространством, особенно выступая в защиту прав развивающихся стран на автономию в интернете в рамках международных организаций. Также проводятся совместные тренировки и учения, повышающие способность реагировать на киберинциденты и укрепляющие профессиональные навыки и взаимное доверие технических специалистов обеих стран. Наконец, в ответ на стратегии и действия США и их союзников в киберпространстве, Китай и Россия исследуют сотрудничество в области

кибероборонь и контрстратегий, формируя совместный фронт противодействия западному превосходству в сети.

Эти направления сотрудничества не только обеспечивают важную поддержку национальной безопасности обеих стран, но и оказывают глубокое влияние на глобальную кибербезопасную среду. Благодаря этому стратегическому партнерству Китай и Россия укрепляют свои позиции и влияние в глобальном управлении кибербезопасностью, подчеркивая, что в будущем международных отношениях кибербезопасность продолжит оставаться важной сферой сотрудничества и конкуренции. Эта тенденция указывает на то, что управление кибербезопасностью в мире развивается в сторону большего многообразия и сложности, и странам необходимо искать возможности для сотрудничества и взаимной выгоды, защищая при этом собственные интересы.

***

В процессе быстрого перехода от индустриальной эпохи к информационной эре наше общество преобразовывается из "общества на колесах" в "общество в киберпространстве". Это преобразование коренным образом изменяет "правила игры" в нашей социальной жизни, особенно в вопросах баланса между безопасностью и развитием. В этом контексте изменение модели управления кибербезопасностью, предложенное администрацией Байдена, представляет научный и практический интерес. Это не только реакция на вызовы, вызванные быстрым развитием цифровых технологий, но и глубокий пересмотр и инновация на основе опыта управления интернетом за последние тридцать лет.

Национальная стратегия кибербезопасности США показывает, что традиционная модель управления кибербезопасностью, основанная на государственных усилиях по предотвращению и борьбе с кибератаками, больше не соответствует текущим вызовам в области безопасности. Вместо этого, новая стратегия выступает за сотрудничество публичного и частного секторов для создания надежной системы защиты киберпространства, подчеркивая ключевую роль участников рынка в усложнении и удорожании кибератак. Этот пересмотр стратегии не только выделяет надзорные функции государства, например, установление минимальных стандартов безопасности для критически важной инфраструктуры, но и акцентирует внимание на важности использования рыночных стимулов для создания устойчивой системы кибербезопасности. Стратегия дополнительно подчеркивает, что большинство инцидентов кибербезопасности можно предотвратить с помощью эффективных профилактических мер, поэтому кибербезопасность рассматривается как вопрос управления внутренними рисками компаний. Роль государства заключается в исследовании возможностей использования рыночных стимулов для поддержки этих мер предосторожности, а также в разработке защитных механизмов для ответа на серьезные киберриски, которые не могут быть устранены через рынок. Как отмечает специалист по кибербезопасности Брюс Шнайер: "Безопасность никогда не бывает взломана, ее всегда обходят". Это высказывание не только подчеркивает продолжительность и сложность работы по кибербезопасности, но и акцентирует внимание на необходимости постоянного обновления защитных мер для адаптации к новым угрозам.

Библиография

1. The White House. A Framework for Global Electronic Commerce// The White House.1997//URL: https://clintonwhitehouse4.archives.gov/WH/New/Commerce (дата обращения: 20.02.2024).

2. The White House. The National Strategy to Secure Cyberspace// The White House. February 2003//URL: www.us-cert.gov (дата обращения: 20.02.2024).
3. Корсаков Г. Б., Информационное оружие супердержавы // ИМЭМО РАН. 2012. №1 (42). (дата обращения: 20.02.2024).
4. Bleiberg, Joshua; West, Darrell M. Obama Argues for Technology Policy Reforms in State of the Union/ Joshua Bleiberg, Darrell M. West, 20.01.2015. URL: https://www.brookings.edu/articles/obama-argues-for-technology-policy-reforms-in-state-of-the-union (дата обращения: 20.02.2024).
5. Baylon, Caroline. Expert view: Tracking the Sony hackers/ Caroline Baylon//The World Today, 6.02.2015//URL: https://www.chathamhouse.org/2015/02/expert-view-tracking-sony-hackers(дата обращения: 20.02.2024).
6. The White House. The Comprehensive National Cybersecurity Initiative// Обама Белый дом: архивы//URL: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative(дата обращения: 24.02.2024).
7. United States. White House Office. National Cyber Strategy of the United States of America/ United States. President (2017-2021 : Trump); United States. White House Office//Washington D.C. : United States. White House Office, 2018//URL: https://www.whitehouse.gov/(дата обращения: 24.02.2024).
8. The White House. FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks/ The White House, 12.05.2021//URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks(дата обращения: 06.03.2024).
9. The White House. National Cybersecurity Strategy/ The White House. – March 2023//URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf(дата обращения: 06.03.2024).
10. Internet Security Alliance. ISA and Executive Order 13636 – Internet Security Alliance// Internet Security Alliance. – URL: https://isalliance.org/isa-and-executive-order-13636 (дата обращения: 06.03.2024).
11. The White House. FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy// The White House – Briefing Room – Statements and Releases. – March 02, 2023. – URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy (дата обращения: 06.03.2024).
12. Янг, Шаланда Д. М-22-09 Меморандум для руководителей исполнительных департаментов и ведомств. Тема: Переход правительства США к принципам кибербезопасности с нулевым доверием [Текст] //Вашингтон, Округ Колумбия, 26 января 2022 г. – Перевод. ФГБУ «НИИ»Интеграл»».
13. The White House. National Cybersecurity Strategy, March 2023. – URL: https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf, свободный

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в рецензируемой статье выступают национальная стратегия кибербезопасности США и ее глобальное влияние.

Методология исследования базируется на изучении программных документов в области кибербезопасности, а также реакции государственных органов власти на инциденты в сфере кибербезопасности в США за последние десятилетия.

Актуальность работы обусловлена возрастающей значимостью кибербезопасности для защиты национального информационного пространства, ее включением в архитектуру национальной безопасности США и влиянием на глобальные процессы.

Научная новизна работы, по мнению рецензента состоит в обобщении и систематизации опыта управления интернетом за последние тридцать лет в США, сформулированных результатах авторского анализа сложившейся американской модели управления кибербезопасностью.

Структурно в тексте публикации выделены следующие разделы: Новая стратегия кибербезопасности администрации Байдена, Переосмысление обязанностей и стимулов в рамках "Национальной стратегии кибербезопасности", Реализация модели нулевого доверия и её влияние на международную безопасность, Сотрудничество Китая и России в области кибербезопасности: стратегическое дополнение и международное влияние и Библиография.

В публикации рассмотрена эволюция подходов к кибербезопасности в США в новейшей истории – в периоды правления Клинтона (1993-2001 гг.), Барака Обамы (2009-2017 гг.), Трампа (2017-2021 гг.), Байдена (2021-настоящее время); показано, что традиционная модель управления кибербезопасностью, основанная на государственных усилиях по предотвращению и борьбе с кибератаками, больше не соответствует текущим вызовам в области безопасности; отмечено, что новая стратегия выступает за сотрудничество публичного и частного секторов для создания надежной системы защиты киберпространства, подчеркивая ключевую роль участников рынка в усложнении и удорожании кибератак; сказано о том, что кибербезопасность в современных условиях рассматривается как вопрос управления внутренними рисками компаний, а роль государства заключается в исследовании возможностей использования рыночных стимулов для поддержки этих мер предосторожности, а также в разработке защитных механизмов для ответа на серьезные киберриски, которые не могут быть устранены через рынок.

Библиографический список включает 13 источников – интернет-ресурсы, а также научные публикации зарубежных и российских авторов по рассматриваемой теме на английском и русском языках. В тексте публикации имеются адресные отсылки к списку литературы, подтверждающие наличие апелляции к оппонентам.

Из резервов улучшения статьи следует отметить следующие. Во-первых, в тексте статьи не озаглавлены вводная и заключительная части. Во-вторых,

Тема статьи актуальна, материал отражает результаты проведенного авторами исследования, содержит элементы приращения научного знания и ценные для практики итоги исследовательской работы, соответствует тематике журнала «Мировая политика», может вызвать интерес у читателей, рекомендуется к опубликованию.