МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»**

Кафедра международных отношений
и внешней политики России

# Формирование и эволюция современной стратегии кибербезопасности США

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 441 группы
направления 41.03.05 «Международные отношения»
Института истории и международных отношений
Агафоновой Арины Игоревны

Научный руководитель
Профессор, доктор исторических наук _____ С.Ю. Шенин
подпись, дата

Зав. кафедрой
Профессор, доктор исторических наук _____ Ю.Г. Голуб
подпись, дата

Саратов 2022

## Введение

**Актуальность темы исследования.** В современном мире, где все большее внимание уделяется цифровизации и где устанавливаются планы и государственные стратегии по проведению компьютеризации, на передний план выходит аспект кибербезопасности. Распространение глобальной сети Интернет, технологий сотовой связи и иных способов бесконтактной передачи данных посредством формирования информационных сетей сделало акторами в вопросах кибернетической безопасности (или же безопасности информационных пространств) почти всех граждан развитых стран. Это, в свою очередь, преобразовало вопросы информационной безопасности в вопросы государственной безопасности и позволило выделить даже отдельную её отрасль – государственную кибербезопасность.

В данной работе рассматривается американская политика в области кибербезопасности с начала 2000-х годов по настоящее время. Создание и формулирование киберугроз в данном случае являются основополагающими факторами для дальнейшего формирования политики кибербезопасности. Изменения в дискурсе киберугроз позволяют нам проанализировать эволюцию американского подхода к кибербезопасности, так, изменения в документах последовали за изменениями в президентских администрациях, при этом основной акцент на инфраструктуре и сетевой безопасности оставался стабильным.

Однако с развитием и распространением технологий киберугрозы приобрели социальное, а затем и политическое измерение. В середине 2000-х годов появилось международное измерение политики кибербезопасности; стало ясно, что киберпространство измеряется в глобальном смысле, и для безопасного и экономически эффективного использования Интернета необходимо создать международную систему кибербезопасности. Дискурс киберугроз в американских документах претерпел некоторые изменения. Их типология была расширена и детализирована, разнообразие потенциально

опасных субъектов увеличилось, а возможные соперники стали открыто называться на межгосударственном уровне.

Доступность публичной информации посредством сети Интернет поставила вопрос о том, какая информация может быть публичной, и насколько граждане государств и информация стратегического значения защищены от несанкционированных доступа и манипуляций.

**Степень разработанности темы.** В работе важную роль играют труды отечественных и зарубежных специалистов в сферах кибернетики, юриспруденции, международного права и истории. Отечественная историография представлена работами Данельяна[1], Безкоровайного и Татузова[2], Стрельцова[3], Смекаловой[4], Долженкова и Грачевой[5], Казарина и Тарасова[6], Карасева[7], Бородакия, Добродеева, Бутусова[8] и другими. Среди

---

[1] *Данельян, А.А.* Международно-правовое регулирование киберпространства // Образование и право. 2020. №1. [Электронный ресурс]: [сайт]. – URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovoe-regulirovanie-kiberprostranstva (дата обращения: 30.12.2021).

[2] *Безкоровайный, М.М., Татузов, А.Л.* Кибербезопасность подходы к определению понятия. // Вопросы кибербезопасности. 2014. №1 (2). [Электронный ресурс]: [сайт]. – URL: https://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya (дата обращения: 30.11.2021).

[3] *Стрельцов А.* О проблемах адаптации международного права к информационным конфликтам. [Электронный ресурс]: [сайт]. – URL: https://digital.report/problemyi-adaptatsii-mezhdunarodnogoprava-k-informatsionnyim-konfliktam/ (дата обращения: 15.11.2021)

[4] *Смекалова М.В.* Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктуры // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. М., 2019.

[5] *Долженков А.А., Грачева Е.В.* Полиморфные вирусы // Успехи современного естествознания. 2011. [Электронный ресурс]: [журнал]. – URL: https://natural-sciences.ru/ru/article/view?id=27093 (дата обращения: 20.04.2022)

[6] *Казарин О.В., Тарасов А.А.* Современные концепции кибербезопасности ведущих зарубежных государств. // История и архивы. М., 2013.

[7] *Карасев, П.А.* Стратегия информационной кибербезопасности США в XXI веке // Вестник Московского университета. Серия 12. Политические науки. М., 2013. №2.

[8] *Бородакий, Ю.В., Добродеев, А.Ю., Бутусов, И.В.* Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1). М., 2019.

зарубежных исследователей можно выделить Норберта Винера[9], Джона Мочли[10], Томаса Чена и Жан-Марка Робера[11].

**Объектом** исследования стала концепция кибербезопасности США.

**Предметом** являются нормативно-правовые документы в сфере международной кибербезопасности и защиты киберпространства, а также экспертные оценки концепции кибербезопасности США.

**Цель квалификационной работы -** проследить динамику развития стратегии кибернетической безопасности США и выявить разницу в подходах у Демократической и Республиканских партий.

Поставленная цель достигается путем решения ряда конкретных **задач**:

1. Изучить историю компьютеризации общества и государства, выявить основные особенности;
2. Рассмотреть понятие киберпространства и дать ему определение;
3. Проанализировать понятие кибербезопасности и дать ему определение;
4. Рассмотреть основные документы, регулирующие международные отношения в сфере кибербезопасности;
5. Рассмотреть стратегии кибербезопасности и их реализацию при администрациях четырех президентов США и дать им оценку;
6. Выявить сходства и различия в реализации политики кибербезопасности между политическими партиями в США;
7. Определить, на каком уровне находится и в каком направлении развивается стратегия кибербезопасности при администрации Джо Байдена.

---

[9] *Wiener, N.* Cybernetics or Control and Communication in the Animal and the Machine. // Hermann & Cie Editeurs. Paris: The Technology Press, Cambridge: Mass., John Wiley & Sons Inc., New York, 1948.

[10] *Mauchly, J.W.* Amending the ENIAC Story. // Datamation, 1979 [Электронный ресурс]: [сайт]. – URL: https://sites.google.com/a/opgate.com/eniac/Home/john-mauchly (дата обращения: 22.03.2022)

[11] *Chen, T., Robert J-M.* The Evolution of Viruses and Worms. // Wayback Machine. 2004. [Электронный ресурс]: [сайт]. – URL: https://web.archive.org/web/20090517083356/http://vx.netlux.org/lib/atc01.html (дата обращения: 20.04.2022)

**Источниковая база.** Для решения поставленных задач была привлечена источниковая база, включающая в себя группу документов и электронных ресурсов.

Были проанализированы интервью и работы исследователей современных представлений о «киберпространстве»[12], рассмотрены резолюции ООН[13], нормативно-правовые акты и программные документы различных администраций в Соединенных Штатах[14], включая Стратегию национальной информационной безопасности США[15], а также указы президента РФ[16].

Важно так же отметить современные электронные новостные источники, как отечественные, так и зарубежные, которые составляют основу исследования: РИА-новости, The New York Times, Wayback Machine, Washington Post, Infosecurity Magazine; также в этой работе активно использовался официальный сайт компании IBM, которая является одним из крупнейших поставщиков аппаратного и программного обеспечения в мире[17].

**Структура работы.** Работа состоит из введения, трех глав, заключения и списка использованной литературы.

---

[12] *Gibson, W.* Our 1988 Interview SPIN. 1988

[13] Резолюция, принятая Генеральной Ассамблеей 23 декабря 2015 года [по докладу Первого комитета (A/70/455)] 70/237. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. [Электронный ресурс]: [сайт]. – URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/60/PDF/N1545760.pdf?OpenElement (дата обращения: 13.03.2022)

[14] National Security Presidental Directives (NSPD) George W. Bush Administration. // Federation of American Scientists. [Электронный ресурс]: [сайт]. – URL: https://irp.fas.org/offdocs/nspd/index.html (Дата обращения: 20.03.22)

[15] Стратегия национальной кибербезопасности Соединенных Штатов Америки. Сентябрь 2018 г. [Электронный ресурс]: [сайт]. – URL: https://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf. (дата обращения: 16.03.2022)

[16] Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. - 2016. - № 50.- Ст. 7074.

[17] IBM – United States. [Электронный ресурс]: [сайт]. – URL: https://www.ibm.com/us-en/ (дата обращения: 17.05.2022)

## Основное содержание работы

Выпускная квалификационная работа состоит из 3 глав:

- Глава 1. Теоретические и общие представления о кибербезопасности государства.
- Глава 2. Концепция кибербезопасности: взгляд республиканцев.
- Глава 3. Концепция кибербезопасности: взгляд демократов.

В параграфе 1.1 *«Исторический аспект»* затрагиваются историческое развитие компьютеров, их влияние на жизнь общества, угрозы, которые могут стать причиной утечки важных данных, методы борьбы с ними. Исходя из этой информации обозначена точка отсчета новой вехи в истории человечества – 1943 год, которым датируется появление первого в мире компьютера ЭНИАК (или же электронный цифровой вычислитель).

Далее идут деления на декады, каждая из которых была ознаменована различными громкими событиями, касающихся компьютеризации, появления новых, адаптирующихся, угроз, а также появлением первых антивирусов; описано несколько случаев самых громких в истории заражений компьютерной сети, таких как Cascade[18] и Vienna[19].

Параграфы 1.2 *«Определение термина "киберпространство"»* и 1.3 *«Понятие государственной кибербезопасности»* преследуют выполнение общей задачи – на основе данных различными отечественными и зарубежными исследователями определений данных понятий составить свое собственное, собирательное. Таким образом,

а также эволюцию таких понятий, как «киберпространство» и «кибербезопасность». Из множества определений, данных русскими и

---

[18] Die Geschichte der Schadprogramme. // Wayback Machine. Viruslist. [Электронный ресурс]: [сайт]. – URL: https://web.archive.org/web/20120418185324/http://www.viruslist.com/de/viruses/encyclopedia?chapter=153311150 (дата обращения: 20.04.2022)

[19] History of malicious programs. // Securelist. [Электронный ресурс]: [сайт]. – URL: https://translated.turbopages.org/proxy_u/en-ru.ru.d8b0f182-6299b2e5-eb2a3d64-74722d776562/https/web.archive.org/web/20120724073428/http://www.securelist.com/en/threats/detect?chapter=108 (дата обращения: 20.04.2022)

зарубежными исследователями, была сделана попытка выделить свои. Таким образом, **киберпространство** – это пространство, не имеющее материальной проекции, внутри которого информация может храниться, транспортироваться и обрабатываться посредством сети Интернет или иных средств бесконтактной связи, задействующих для коммуникации компьютеры и иные информационно-емкие устройства; а **кибербезопасность** – это реализация мер защиты данных внутри информационных систем общественного и личного пользования от несанкционированного и неправомерного доступа в целях нанесения ущерба гражданам государства и государственным структурам.

Хронология повествования во 2 и 3 главах осознанно нарушена, т.к. помимо задачи рассмотрения деятельности самих президентов необходимо также уделить внимание партиям, к которым они относятся.

Параграф 2.1 *«Деятельность Дж. Буша-младшего в сфере кибербезопасности»* был полностью посвящен первым шагам президента в новой, неизведанной сфере обеспечения кибербезопасности. Он положил начало реализации контроля над киберпространством, обозначил основные участники этого процесса, выделены угрозы и поставлены первые задачи. Это привело к укреплению альянса и международных союзов для борьбы с кибертерроризмом, в следствие чего НАТО должна была быть готова противостоять потенциальным угрозам XXI века. В целом, проекты, разработанные и реализованные при администрации Дж. Буша мл., после тщательного исследования, можно назвать успешными, но, безусловно, нуждающимися в доработке дальнейшими администрациями.

В параграфе 2.2 *«Дональд Трамп и кибербезопасность»* описывается продолжение Дональдом Трампом и его администрацией кибернетической политики со времен Дж. Буша мл. Его новая стратегия кибербезопасности США держалась на совершенно новых принципах ужесточения подходов к противникам американского государства в этих сферах деятельности. Это означало, что теперь у США снова на первом месте было единоличное

отстаивание своих интересов, а с сотрудничеством на международной арене были большие проблемы.

Промежуточный итог гласит, что республиканская партия Соединенных штатов все-таки придерживается политики активной борьбы за доминирование и открытое соперничество, а также единоличное отстаивание своих интересов, что идет в разрез с политикой демократической партии.

В параграфе 3.1 *«Программы кибербезопасности и их реализация при администрации Барака Обамы»* сразу обозначается, что именно на период работы администрации Барака Обамы проблемы, связанные с кибербезопасностью США, начали крайне болезненно сказываться на внешней политике, поэтому неудивительно, что, придя на смену Джорджу Бушу-мл., новый президент сразу же заявил, что обеспечение безопасности киберпространства является одной из важнейших государственных задач. [20]

Поэтому вскоре после вступления в должность президент распорядился провести тщательный обзор федеральных усилий по защите информационной и коммуникационной инфраструктуры США и разработать комплексный подход к обеспечению безопасности цифровой инфраструктуры Америки.

Сотрудничество с другими странами (по крайней мере попытка) – вот характерная черта, которую можно выделить у администрации Обамы. И условно оно началось в 2009 г. с переговоров с Россией и комитетом ООН по контролю над вооружениями, укреплению безопасности в Интернете и ограничению применения ИКТ в военных целях.

Важная встреча состоялась 30–31 мая 2011 г. Делегация американских экспертов по вопросам кибербезопасности, под руководством Центра стратегических и международных исследований (ЦСМИ), встретилась с

[20] *Казарин, О.В., Тарасов, А.А.* Современные концепции кибербезопасности ведущих зарубежных государств. // История и архивы. М., 2013. С.62

представителями китайской стороны в штаб-квартире Китайского института современных международных отношений в Пекине.[21]

Таким образом, можно сказать, что Обама, как в принципе и весь его курс, проводил более глобалистскую политику в сфере кибербезопасности. Значительно большее внимание уделялось международному сотрудничеству и договоренностям в вопросах обеспечения кибербезопасности.

Параграф 3.2 *«Деятельность администрации Джо Байдена»* повествует об основных положениях, которые успела принять действующая администрация президента США в сфере обеспечения кибербезопасности; в данном параграфе рассматриваются указ от мая 2021 года, который устанавливал новые строгие стандарты безопасности любого программного обеспечения, продаваемого федеральному правительству[22], а также выступление Джо Байдена со срочным предупреждением для лидеров американского бизнеса, в котором посоветовал им немедленно усилить киберзащиту своих компаний.[23]

Несмотря на накал ситуации на мировой арене все еще можно рассуждать о том, что, даже несмотря на то, что Байден – демократ, и он традиционно склонен вести более глобалистскую политику, чем республиканец Трамп, нет никаких оснований предполагать, что в ближайшие годы стратегия кибербезопасности США может измениться, потому что соперничество в этой сфере уже стало невероятно принципиальным для всех участников данного конфликта.

---

[21] *Карасев, П.А.* Стратегия информационной кибербезопасности США в XXI веке // Вестник Московского университета. Серия 12. Политические науки. М., 2013. №2. С.100.

[22] *Sanger, D., Barnes, J.* Biden Signs Executive Order to Bolster Federal Government's Cybersecurity. // The New York Times. May 12, 2021. [Электронный ресурс]: [газета]. – URL: https://www.nytimes.com/2021/05/12/us/politics/biden-cybersecurity-executive-order.html (дата обращения: 28.05.2022)

[23] President Biden signs executive order to strengthen U.S. cybersecurity defenses. // Security. May 13, 2021. [Электронный ресурс]: [сайт]. – URL: https://www.securitymagazine.com/articles/95197-president-biden-signs-executive-order-to-strengthen-us-cybersecurity-defenses (дата обращения: 20.03.2022)

Рассмотренная в данной главе демократическая партия США показала, что все свои действия направляла и направляет на сотрудничество и в целом на глобалистскую политику.

## Заключение

За двадцать лет с момента своего зарождения и формирования кибербезопасность превратилась в одну из важнейших составляющих современной государственной и межгосударственной политики. Начав разработку политики обеспечения кибербезопасности на заре XXI в., правительство США приняло десятки документов, регулирующих работу в киберпространстве. По ходу работы прослеживались так же усилия других государств, предпринимаемые в области кибербезопасности, что показывает безусловную неокончательность формирования международной системы всеобщей кибербезопасности на уровне суверенных государств в рамках международного взаимодействия.

Несмотря на активную политическую позицию по этому вопросу, начав работать в этой сфере чуть ли не первыми, США не удалось и, можно предполагать, не удастся полностью обезопасить себя от киберрисков, количество и комплексность которых растут день ото дня.

В первой главе была изучен исторический аспект кибернетической безопасности, были рассмотрены понятия «киберпространство» и «кибербезопасность», а также основные точки зрения на значения терминов. Были предприняты попытки компиляции различных определений для создания оригинальных определений, отвечающих целям и задачам работы.

Во второй и третьей главах был дан анализ действиям администраций 4-х президентов США, начиная с Дж. Буша-мл. и заканчивая нынешней администрацией Джо Байдена. Благодаря ему было рассмотрено формирование современных представлений и концепций кибербезопасности США, были выделены вызовы, с которыми Соединенные Штаты

сталкиваются в сфере государственной кибербезопасности, а также была подчеркнута разница подходов к роли кибербезопасности, формах ее регулирования администрациями разных президентов. Это позволяет проследить отмечаемую некоторыми исследователями политическую составляющую социально-технологических вопросов кибербезопасности государства.

Достаточно хорошо видно, как стратегия национальной кибербезопасности менялась от администрации к администрации. При этом подходы американских властей к политике в сфере кибербезопасности характеризуются значительной адаптивностью, и в большей степени зависят от текущей внешнеполитической ситуации, нежели отражают осознанное и последовательно эволюционирующее понимание путей решения этой насущной проблемы. Во многом, по этой причине, в настоящий момент затруднительно оценить эффективность более двух десятков законодательных инициатив, принятых двумя последними администрациями.[24]

Наконец, можно отметить еще одну тенденцию: проблематика кибербезопасности зачастую рассматривается руководством США не как самостоятельное направление деятельности, а как средство решения более широких внешнеполитических задач, возможность оказания давления на других акторов с целью изменить поведение последних.[25]

Несмотря на проделанные исследования, крайне сложно поместить комплексный анализ столь обширной и динамично развивающейся системы, как система государственной кибербезопасности США, в рамках одной работы, поскольку огромная база исследований и аналитики, поставляемой различными информационными агентствами почти ежечасно, дает все новую

---

[24] *Смекалова, М.В.* Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктуры // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. М., 2019.С. 64-65

[25] Там же.

информацию для размышлений над ней. Это позволяет актуализировать работу и развивать ее идеи в дальнейших исследованиях.