**Эволюция национальной стратегии кибербезопасности США и ее глобальное влияние**

***Хуанфу Чжэнхуэй***

*Аспират*

*Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Москва, Россия*

*E–mail: hfstudy@yandex.ru*

С приходом цифровой эпохи кибербезопасность стала предметом глобального внимания. Соединенные Штаты, являясь местом рождения интернета и лидерами информационно-технологической революции, сыграли ключевую роль в развитии стратегий кибербезопасности, оказав значительное влияние на национальную безопасность и управление киберпространством на мировом уровне.

В 1990-е годы, с прорывом и распространением интернет-технологий, правительство США приняло открытую и свободную политику в отношении сети. Тогдашнее правительство Клинтона считало, что интернет является глобальным общественным пространством без границ, и следует поощрять свободный поток информации и развитие электронной коммерции. В этот период отношение правительства США к интернету в основном заключалось в том, чтобы оставить рыночные силы в качестве ведущих, что было полностью отражено в "Фреймворке глобальной электронной коммерции", опубликованном в 1997 году, где роль правительства в большей степени виделась как содействующая, а не регулирующая.

Однако теракты 11 сентября 2001 года стали поворотным моментом, после которого США значительно усилили внимание к кибербезопасности. Администрация Джорджа Буша-младшего выпустила "Национальную стратегию безопасности киберпространства", включив вопросы кибербезопасности в рамки национальной безопасности, при этом сохраняя преимущественно рыночный подход к управлению интернетом.

Во втором десятилетии XXI века, несмотря на то что администрация Обамы не разработала конкретную стратегию в области кибербезопасности, в ответ на всё более сложную ситуацию в области кибербезопасности, она попыталась усилить управление в этой сфере через законодательство. Хотя эти усилия не увенчались успехом из-за противодействия со стороны Торговой палаты США и отраслевых групп, попытки этого периода отражают углубление понимания правительства необходимости усиления управления кибербезопасностью. Киберпространство начало становиться горячей точкой в отношениях между Китаем и США, в начале правления Трампа был создан механизм "Диалог по правоприменению и кибербезопасности" между Китаем и США, но в конце правления Трампа произошло безосновательное подавление китайских интернет-компаний, что стало выраженной чертой стратегического соперничества между двумя странами.

В период правления администрации Трампа, «Национальная стратегия в области киберпространства» 2018 года отметила, что США начали уделять внимание активной защите и наступательным действиям в области кибербезопасности, что указывает на дальнейшее развитие стратегии США в области кибербезопасности, а именно на увеличение внимания к активной защите при сохранении доминирования рынка. Во время правления администрации Трампа США скорректировали ряд политик в киберпространстве, включая заморозку диалога по кибербезопасности между Китаем и США, усиление давления на китайские интернет-компании, а также относительный упадок лидерства США в глобальной системе управления киберпространством, что создало сложную ситуацию в киберпространстве для администрации Байдена.

В последние годы, на фоне быстрого развития технологий и усложнения глобального киберландшафта, стало очевидно, что для эффективного управления киберпространством требуется более активное государственное вмешательство. Администрация Байдена сделала значительный шаг в этом направлении, выпустив "Исполнительный приказ о кибербезопасности" и "Национальную стратегию кибербезопасности", которые предусматривают усиление государственного регулирования и сотрудничества между государственным и частным секторами в области защиты киберпространства.

В целом, стратегия США в области кибербезопасности с 1990-х годов, когда преобладал либерализм рынка, через множество корректировок и эволюции, постепенно пришла к приданию большего значения регулированию и активной защите, что отражает не только растущую угрозу кибербезопасности, но и изменение роли США в глобальном управлении киберпространством. С дальнейшим развитием технологий и эволюцией глобальных киберугроз стратегия США в области кибербезопасности будет продолжать адаптироваться к новым вызовам, а её влияние на глобальное управление киберпространством будет продолжать углубляться. В эпоху цифровизации этот переход в стратегии США имеет решающее значение не только для их собственной безопасности, но и предоставляет важные ориентиры для глобального управления кибербезопасностью.

**Литература**

1. Бакиров Рамиль Раилевич, Цветкова Наталья Александровна Политика кибербезопасности США - эволюция, угрозы и оппоненты, 1990-2010-е гг. // Международные отношения. 2019. №4. URL: <https://cyberleninka.ru/article/n/politika-kiberbezopasnosti-ssha-evolyutsiya-ugrozy-i-opponenty-1990-2010-e-gg>
2. Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая. Дисс. ... канд. поли. Наук. Москва 2014
3. Стратегия национальной кибербезопасности соединенных штатов Америки. Сентябрь 2018 года <https://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf>
4. National cybersecurity strategy 2023, March 2023 <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>
5. <https://www.state.gov/translations/russian/> (U.S. Department of state)
6. The White House. Fact sheet: Biden-Harris Administration Announces National Cybersecurity Strategy. March 02, 2023 <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>