**Булавинцев Даниил Александрович,** Курсант
Московский университет МВД России имени В.Я. Кикотя,
Москва

**Мачинский Никита Андреевич,** Курсант,
Московский университет МВД России имени В.Я. Кикотя,
Москва

# ФЕНОМЕН КИБЕРВОЙН В СОВРЕМЕННОЙ РЕАЛЬНОСТИ

**Аннотация:** В данной работе рассмотрен мировой феномен 21 века, пришедший в нашу жизнь с развитием цифровизации.

**Ключевые слова:** киберугроза, кибератака, кибервойна, кибершпионаж, мировое сотрудничество.

В современной реальности, когда технический прогресс развивается быстрыми темпами, все станы мира используют новейшие технологии во всех сферах деятельности, развивается феномен кибервойн. Кибервойны – это новое международное явление, которое возникло в связи с растущей зависимостью современного общества от информационных технологий. Кибервойны – это конфликты, которые происходят в киберпространстве, используя компьютерные атаки и другие средства для нарушения работы сетей, захвата данных, попыток уничтожения или кражи информации, а также распространения ложной, направленной на умышленное дезинформированное лиц.

Кибервойны проводятся не только между конкретными странами, зачастую Кибервойны могут проводиться между государствами, группами хакеров, кибертеррористами или даже отдельными людьми, обладающими определенными техническими умениями. Такие войны могут иметь серьезные последствия, такие как нарушение функционирования критически важных систем, таких как системы коммуникации и энергомощности. Кроме того, через кибервойны могут происходить кража интеллектуальной собственности, нарушения прав на конфиденциальную информацию и другие преступления, которые могут оказаться намного более гибкими и трудно определяемыми и идентифицированными чем традиционные виды преступлений.

Применение кибервойн в последнее время стало все более распространенным в мире, вызывая растущее беспокойство в правительствах, компаниях, а также среди обычных пользователей Интернета. Следовательно, защита информации и кибербезопасность являются ключевыми задачами в современном информационном мире, которые невозможно игнорировать. Первые случаи использования компьютерных атак в политических целях зафиксированы еще в 1980-х годах, но особое значение эти атаки получили только в 1990-х годах после распространения Интернета и сетевых технологий в бизнесе и политике. Одним из первых примеров кибервойны можно назвать историю кибератаки, которую совершил канадский подросток Майкл Каллен в 1986 году. Он создал вирус "Brain", который заражал компьютеры во всем мире и затем сообщал авторам о зараженных компьютерах, с требованием выплаты.

В 2007 году Эстония стала первой страной, наиболее пострадавшей от крупномасштабной кибератаки. По сообщению официальных представителей Эстонии, эта кибератака была проведена российскими хакерами в связи с конфликтом между двумя странами на счет переноса

памятника Советскому солдату из Таллина. Также в 2007 году неизвестная иностранная сторона взломала высокотехнологичные и военные агентства в Соединенных Штатах и скачала большое количество засекреченной информации.

В 2009 году сеть кибершпионов под названием «GhostNet» получила доступ к конфиденциальной информации, принадлежащей как государственным, так и частным организациям более чем в 100 странах мира. Сообщается, что GhostNet происходит из Китая, хотя эта страна отрицает свою ответственность. Это доказывает, насколько велика угроза кибервойны. Страны находят новые способы причинить вред другим странам, даже не ступая на их землю, это действительно война нового века. Как указано выше, вы можете видеть, насколько важно для каждой страны иметь политику кибербезопасности, которая поможет защитить их от возможных будущих атак. С 2010 года кибервойны получили более организованный и серьезный характер с появлением программных комплексов, которые были созданы для осуществления широкомасштабных кибератак на критически важные объекты. В 2012 году кибератака на предприятие "Саудовской Арамко" привела к попытке дестабилизации мирового рынка нефти, вызвав панику и колебания на нефтяных рынках. В такой ситуации проблема кибербезопасности стала критически важной и получила мировое внимание, в связи с чем были созданы международные организации, направленные на сотрудничество в области кибербезопасности и совместную борьбу с киберугрозами и кибератаками. Вместе с ростом угрозы кибербезопасности многие страны начали сосредотачивать усилия на защите себя от кибератак. Однако, так как кибербезопасность является глобальной проблемой, страны также понимают необходимость сотрудничества в этой области.

Мировое сотрудничество стран в области кибербезопасности началось еще в девяностых годах, но в последние годы оно значительно усилилось. Давайте рассмотрим некоторые примеры мирового сотрудничества в этой области:

1. Европейский союз

Европейский союз создал различные программы и инициативы по кибербезопасности, в том числе ЕС-щит, который предназначен для защиты инфраструктуры европейских стран от кибератак. Кроме того, ЕС также учреждает совместные учебные и исследовательские проекты в области кибербезопасности.

2. Китай

Китай активно сотрудничает с другими странами в области кибербезопасности. В 2015 году, на встрече с президентом Обамой, президент Китая Си Цзиньпин подписал соглашение о кибербезопасности между двумя странами. Китай также стал участником Универсального международного телеграфного союза (ITU) и активно принимает участие в их инициативах по защите кибербезопасности.

3. США

США также активно сотрудничает со своими союзниками в области кибербезопасности. Они имеют различные соглашения с другими странами, например, США и Канада подписали Совместное соглашение о кибербезопасности, а США и Япония подписали обмен меморандумами по кибербезопасности.

4. NATO

NATO также принимает меры по укреплению кибербезопасности и усилению сотрудничества между странами. Они создали Группу по кибербезопасности, которая занимается выработкой международных стандартов и практик в области кибербезопасности.

5. Международный союз телекоммуникаций

Международный союз телекоммуникаций (ITU) занимается вопросами кибербезопасности и устанавливает международные стандарты в этой области. Они также проводят международные учения по кибербезопасности и участникам предоставляют возможные сценарии кибератак. В целом, мировое сотрудничество по кибербезопасности является важным инструментом в борьбе с угрозами в этой области. Вооруженными силами на протяжении нескольких поколений всегда были армия, флот, военно-воздушные силы, корпус морской пехоты и береговая охрана; однако в постоянно развивающемся цифровом мире представление о том, что космическое пространство станет следующим военным фронтом, быстро заменяется идеей о том, что следующей гонкой вооружений станет киберпространство. В современном технологически развитом мире кибервойны и кибершпионаж, а также киберпреступления в целом становятся все более опасной угрозой, поскольку почти каждое государственное учреждение и физическое лицо так или иначе подвергается воздействию киберпространства. Кибервойна уже является серьезной проблемой во всем мире, и ее не всегда выполняют правительства, но также и негосударственные субъекты и хакеры, что является дополнительной проблемой для правительств, поскольку количество людей, которые знают, как взламывать другие сети, очень велико и растет быстрым темпом. Чему способствует нарастание популярности специалистов IT технологий. А также проблемой кибервойн является то, что интернет и цифровые технологии не имеют границ. Это означает, что кибератаки могут происходить из любой страны в любом месте мира. Таким образом, многие правительства сталкиваются с проблемой идентификации и обвинения истинных исполнителей атак, от ложных.

Кибервойны стали неотъемлемой частью современной реальности, их влияние на мировую политику и экономику нельзя переоценить. Каждый день происходят новые кибератаки, которые угрожают безопасности государств, корпораций и обычных людей. В связи с этим возрастает потребность в разработке эффективных методов защиты от киберугроз.

Однако необходимость борьбы со злоумышленниками не должна приводить к ограничению свободного доступа к информации или нарушению прав человека на конфиденциальность данных. Правительства должны работать над созданием законодательства, которое бы отстаивало интересы граждан при сохранении безопасности стран.

В заключение хочется отметить, что кибервойны – это серьезная проблема, которая продолжает развиваться. В мире происходят ужасные кибернападения, которые наносят ущерб экономике, бизнесу и частным лицам. Интернет стал частью нашей жизни, и мы используем его для нашей работы, учебы, общения и других целей, и поэтому безопасность в сети должна быть приоритетом для всех, кто использует Интернет.

Угрозы, связанные с кибервойнами, могут быть разрушительными для инфраструктуры объединения ресурсов и техник национальной безопасности, что заставляет государства к постоянному улучшению своего киберправа и кибервоенных возможностей. У лидеров и политиков множество причин для заботы насчет безопасности невоенного характера т.е. защиты критически важных объектов в сфере транспорта, энергоснабжения, медицины и многих других. Это особенно важно в сферах, где жизнь и безопасность людей находится под угрозой.

В последние годы наблюдаются новые тенденции в кибервойнах, которые могут привести к еще более серьезным последствиям в будущем. Возможность использования кибератак в качестве альтернативы традиционным формам войны действительно крайне опасна и необходимы новые меры для защиты национальной безопасности.

Для борьбы с кибервойнами международное сообщество принимает широкий спектр мер. Международные организации, такие как ООН и ЕС, разрабатывают международные соглашения и политики по кибербезопасности. Кроме того, правительства и частные компании вкладывают значительные ресурсы в усовершенствование систем безопасности, включая стратегии профилактики и защиты от кибератак, а также обучение специалистов в области кибербезопасности.

В целом, борьба с кибервойнами требует координации и улучшения национального киберправа и кибервоенных возможностей. Способность государств наладить сотрудничество и координацию в этой области станет ключевым фактором в борьбе с кибернападениями. Инвестирование в кибербезопасность должно стать приоритетом для всей международной общественности, чтобы защитить наш мир и обеспечить безопасность в киберпространстве.

*Список литературы:*

1. "What are Cyberwarfare and Cyberweapons?" – статья, опубликованная The Balance, объясняющая основные понятия кибервойны и кибероружия.

2. "Cyberwarfare: How Nations Attack Without Bullets, Bombs and Missiles" – статья от Forbes, рассказывающая о представлении кибервойны и их последствиях.

3. "The Future of War: How Technology is Remaking the Battlefield" – книга Питера У. Сингера, где он рассматривает тему кибервойн и новейших технологий в области военных действий.

4. "The CyberWar Threat Has Been Growing for Years. Why Hasn't the United States Done More to Stop It?" – статья CNN о проблеме отсутствия достаточного решения со стороны правительства США по предотвращению кибервойн.