# ИНФОРМАЦИОННАЯ ВОЙНА И КОНТРОЛЬ В КИБЕРПРОСТРАНСТВЕ - СОВРЕМЕННАЯ УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ.

**Трофимов И.А.**

*Трофимов Иван Александрович – студент магистратуры,*
*Российский технологический университет,*
*г. Москва*

***Аннотация:*** *данная научная статья посвящена анализу современного состояния и характеристикам информационного противоборства в области национальной безопасности. В работе рассматриваются основные формы информационной войны, включая скрытую («холодную») и открытую («горячую») конфронтацию, а также роль современных технологий, таких как разведка и сбор информации, криптография, управление глобальными информационными потоками и тактики и методы проведения кибератак и контрмеры. Особое значение уделяется угрозам, которые находятся в киберпространстве, методам проведения кибератак и контрмер, а также стратегическим аспектам защиты критической инфраструктуры и национальных интересов. Необходимость подчёркивается для государственных органов, специалистов в области информационной безопасности и международных организаций. Они акцентируют внимание на необходимость развития стратегий и методов защиты, чтобы обеспечить безопасность государства и его информационных ресурсов.*
*Необходимость существует для всего общества, государственных институтов, критической инфраструктуры и граждан страны. Группы зависят от обеспечения информационной безопасности для стабильного функционирования, защиты личных и государственных данных, сохранения суверенитета и предотвращения угроз со стороны противников.*
***Ключевые слова:*** *информационная война, информационное оружие, киберпространство, контроль информационных потоков, кибербезопасность, киберугрозы, информационная безопасность, киберпротивоборство, глобальные информационные ресурсы, национальная безопасность.*

# INFORMATION WARFARE AND CONTROL IN CYBERSPACE - A MODERN THREAT TO NATIONAL SECURITY

**Trofimov I.A.**

*Trofimov Ivan Aleksandrovich – master's student,*
*RUSSIAN TECHNOLOGICAL UNIVERSITY,*
*MOSCOW*

***Abstract:*** *this research article analyzes the current state and characteristics of information warfare in the area of national security. The paper examines the main forms of information warfare, including covert ("cold") and overt ("hot") confrontation, as well as the role of modern technologies such as intelligence and information gathering, cryptography, global information flow management, and tactics and methods for conducting cyberattacks and countermeasures. Particular attention is paid to threats in cyberspace, methods for conducting cyberattacks and countermeasures, and the strategic aspects of protecting critical infrastructure and national interests. The importance of this approach is emphasized for government agencies, information security specialists, and international organizations. They emphasize the need to develop strategies and methods of protection to ensure the security of the state and its information resources. This need exists for society as a whole, including government institutions, critical infrastructure, and citizens. These groups depend on information security for stable operation, the protection of personal and government data, the preservation of sovereignty, and the prevention of threats from adversaries.*
***Keywords:*** *information warfare, information weapons, cyberspace, information flow control, cybersecurity, cyber threats, information security, cyber warfare, global information resources, national security.*

**Введение**

В настоящее время одной из главных проблем, активно обсуждаемых в обществе, является информационная война. Информационная война – это целенаправленные действия в киберпространстве, реализованные для достижения информационно-технологического превосходства над оппонентом с целью повреждения его информационной системы при этом обеспечивая защиту собственных информационных ресурсов. Данная война ведётся с помощью специальных средств и технологий, которые при правильном использовании могут стать мощным оружием. При неправильном использовании данного оружия, оно способно нанести серьёзный ущерб главным объектам информационно-технологической инфраструктуры страны. Это может значительно ослабить обороноспособность государства и повлиять на исход будущей вооружённой конфронтации.

**Цель исследования**

Научная новизна представленной работы заключается в том, что в теме систематизированы методы, направления информационного противоборства и объединены в единую концептуальную модель, что позволяет точно определить стратегические направления в обеспечении национальной безопасности в киберпространстве. В работе проведён комплексный анализ современных технологий, тактик, которые применяются в кибервойнах, также предложены подходы к классификации и оценке степени угроз. В работе предложена концептуальная схема взаимодействия различных элементов системы информационной безопасности на основе междисциплинарных подходов, что расширяет возможности стратегического планирования и оперативного реагирования.


*Рис. 1. Показатели статусного уровня глобального доминирования.*

*Атомно-ядерные технологии* - это информационные войны, которые символизируют наличие новых возможностей для проведения кибератак на критическую инфраструктуру противника.

*Создание систем мониторинга* - формирование систем мониторинга определена необходимостью своевременного обнаружения и анализа перспективных угроз, а также обеспечением быстрого реагирования на инциденты информационной безопасности.

*Разведка и сбор информации в цифровой сфере* - это широкий спектр инструментов, направленных на получение, анализ и использование данных, находящихся в цифровых средах.

*Квантовая криптография* - является необходимым ключевым направлением, но в настоящее время она занимает не первостепенное место среди приоритетных мер по обеспечению информационной безопасности.

*Управление глобальными информационными потоками* - это направление относится к информационной войне — контроль над СМИ, социальными сетями и распространением информации становится инструментом манипуляции общественным мнением, дезинформации и политического влияния на мировой арене.

*Тактики и методы проведения кибератак и контрмеры* - это способы, которые используют злоумышленники для получения несанкционированного доступа к информационным системам, кражи данных, нарушения их работы и целостности.

*Технологии кибер разведки и оперативного реагирования* — это набор инструментов, позволяющих выявлять, анализировать и предотвращать киберугрозы, а также быстро реагировать на инциденты в информационных системах.

**Стратегические концепции обеспечения информационной безопасности**

В настоящее время информационные технологии и киберпространство интегрированы в сферу национальной безопасности. Информационная война включает в себя разнообразные способы и приёмы, которые являются главным показателем для достижения политических и экономических целей государств. В связи с появлением новых угроз и прогресса в технологиях квантовые вычисления и средства радиоэлектронной борьбы, возникает потребность в упорядочении и изучении актуальных методов противодействия в информационной среде.

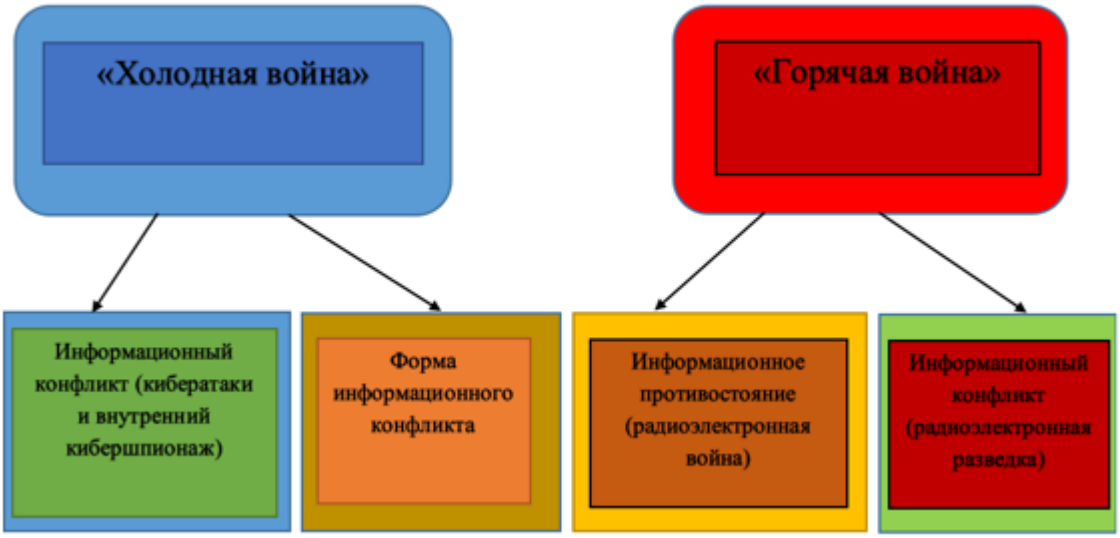


*Рис. 2. Модель информационных противостояний.*

*«Холодная война» — информационный конфликт* это скрытый вид информационного противоборства, который называется информационно-технологическим подавлением — это достижение временного или постоянного снижения эффективности или полного прекращения функционирования информационных систем и технологий противника. Одним из методов такого подавления является внедрение вредоносного программного обеспечения.

*Кибершпионаж и несанкционированный доступ к государственным системам* - это деятельность, при которой взломщики осуществляют несанкционированный доступ в защищённые государственные информационные системы.

*Скрытое внедрение вредоносных программ в критическую инфраструктуру* - взломщики внедряют вредоносное программное обеспечение или в системы, которые управляют важными ресурсами — электросетями, объектами или системами связи.

*Кража интеллектуальной собственности и государственных данных* - злоумышленники осуществляют кражу конфиденциальных данных, таких как технологические разработки, секретные исследования.

*Скрытое манипулирование данными без явных следов атаки* - это деятельность по внедрению ложных или искажённых данных в информационные системы и базы данных без видимых признаков вторжения.

Таким образом, данные методы демонстрируют, что современное информационное противоборство всё чаще приобретает скрытый, изощрённый характер. Они позволяют противнику вести «холодную войну», не вызывая открытых конфликтов и сохраняя скрытность своих действий. Данный стиль позволяет вести борьбу создавая постоянную угрозу для национальной безопасности, экономики и стабильности общества, требуя от государств развития современных средств защиты, разведки и контрмер для своевременного выявления и устранения скрытых угроз.

*«Горячая война»* — агрессивное противоборство. В современном конфликтном пространстве «горячая война» включает в себя не только боевые действия, но и целенаправленные формы информационной и радиотехнической борьбы.

*Массированные кибератаки на критическую инфраструктуру* - одно из основных составляющих являются крупномасштабные кибератаки, нацеленные на жизненно важные объекты инфраструктуры.

*Радиоэлектронное подавление систем управления* — это использование средств электронного подавления, направленных на блокирование или дезориентацию систем связи, навигации и управления.

*Радиоэлектронная разведка (РЭР)* - это главный компонент информационного противостояния в информационном конфликте в условиях горячей войны. РЭР обеспечивает сбор разведданных и электронное подавление, что позволяет сторонам контролировать информационную среду.

Таким образом, данная схема показывает, что информационное противоборство находится в масштабе от скрытых операций к открытому конфликту и переходит в агрессивную стадию. Каждая форма представляет возрастающий уровень угрозы национальной безопасности и требует защитных мер — разведки и контрразведки.

**Заключение**

В данной работе был проведён комплексный анализ современного состояния и характеристик информационного противоборства в сфере национальной безопасности. Исследованы основные формы информационной войны, включая скрытую («холодную») и открытую («горячую») конфронтацию, а также значение современных технологий, например, разведка, сбор информации, криптография, управление глобальными информационными потоками и методы проведения кибератак. Главное место уделяется угрозам, происходящим в киберпространстве в разработке и реализации противодействия для защиты национальных интересов.

В данной работе были систематизированы методы, направления и стратегии информационного противоборства, предложены концептуальные модели взаимодействия элементов системы информационной безопасности, а также рассмотрены потенциальные направления развития технологий, стандартов и межведомственного сотрудничества. Проведён анализ угроз, который относится к киберпреступности, шпионажу и информационной борьбе, оценены средства разведки, мониторинга, защиты и реагирование на киберугрозы.

В работе достигнута цель по комплексному изучению и моделированию современных аспектов информационной и кибербезопасности, сформулированы рекомендации по развитию стратегий защиты и противодействия в условиях глобальной информационной войны. Достигнутые результаты являются базой для развития национальных систем информационной безопасности и усиления стратегической стабильности государства в условиях цифровой среды.

### *Список литературы / References*


1. *Мельников В.П.* Защита информации в компьютерных системах [Текст] / В.П. Мельников. – М.: Финансы и статистика, 2021 – 368 с.
2. *Васильков А.В.* Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков.— Москва : ФОРУМ: ИНФРА-М, 2023.— 368 с.
3. *Жигулин Г.П.* Организационное и правовое обеспечение информационной безопасности / Г.П. Жигулин.— Санкт-Петербург : СПбНИУИТМО, 2024.— 173 с.
4. *Мельников В.В.* Безопасность информации в автоматизированных системах / В.В. Мельников.— Москва : Финансы и статистика, 2023.— 368 с.
5. *Малюк А.А.* Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин.— Москва : Горячая линия — Телеком, 2021.— 148 с.
6. Международный стандарт ITU-T Rec. X.816 — "Модель оценки уровня безопасности".
7. Международный стандарт ITU-T Rec. X.813 — "Модель управления безопасностью".
8. Международный стандарт ITU-T Rec. X.814 — "Модель защиты сети".
9. Международный стандарт ITU-T Rec. X.815 — "Модель оценки уровня безопасности".
10. Международный стандарт ITU-T Rec. X.800 "Рекомендуемые практики по обеспечению безопасности сетей".