

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«**Финансовый университет при Правительстве
Российской Федерации**»
(Финансовый университет)



Факультет информационных технологий и анализа больших данных
Кафедра информационной безопасности

Информационное противоборство в начале XXI века

Подготовил: студент группы УИБ25-1м
Матевосян Гурген Арменович

Преподаватель: доцент, к.п.н.
Цацкина Елена Петровна

17.09.2026



Введение

Информационное противоборство в начале XXI века перестало быть вспомогательным инструментом. Оно превратилось в самостоятельный вид стратегического противоборства, способный достигать политических целей без применения военной силы



Понятие информационного противоборства

Ключевые категории:

- информационное противоборство;
- информационная борьба;
- защита информации;
- поражение информации противника

Информационное противоборство - это соперничество социальных систем в информационно-психологической сфере с целью усиления влияния на определенные сферы социальных отношений и установление контроля над источниками стратегических ресурсов, в результате которого одни участники соперничества получают преимущества, необходимые им для дальнейшего развития, а соответственно другие их утрачивают



Военно-теоретическая основа

Сетецентрическая война — концепция, в рамках которой информационное превосходство рассматривается как фундаментальное условие достижения военного превосходства

Фундаментальная взаимосвязь — средства воздействия на информацию, циркулирующую в системах управления войсками и оружием, становятся ключевым фактором боеспособности



Два поколения информационного противоборства

Первое поколение	Второе поколение
Компонент наряду с другими средствами поражения	Самостоятельный вид стратегического противоборства
Ограничен временными рамками конфликта	Долговременное воздействие (недели, месяцы, годы)
Тактический уровень	Стратегический уровень управления политическими процессами

Концепция strategic information warfare впервые сформулирована специалистами корпорации RAND в конце 1990-х годов



Институционализация в США

Ключевые документы:

- 1992 — Директива МО США TS3600.1 «Информационная война»;
- 1993 — Директива Комитета начальников штабов № 30;
- 1998 — «Объединённая доктрина информационных операций» (Joint Doctrine of Information Operations);
- 1999 — Директива PDD-68, создание International Public Information Group;
- 2006 — обновление доктрины

Доктрина 1998 года официально подтвердила подготовку к наступательным информационным операциям не только в военное, но и в мирное время



Сферы ведения информационного противоборства

Техническая сфера:

- радиоэлектронная борьба;
- воздействие на системы управления войсками и оружием;
- компьютерные атаки, вирусы, «логические бомбы»

Психологическая сфера:

- операции психологического воздействия;
- дезинформация;
- манипулирование общественным мнением



Технические средства поражения информации

Компьютерные вирусы — внедрение в телефонные сети, вывод из строя связи;

Логические бомбы — разрушение электронных устройств управления транспортом, создание предпосылок катастроф;

Электромагнитный импульс (ЭМИ) — неядерные устройства, поражающие компьютерные системы финансовых учреждений;

Передача ложных приказов — дезорганизация управления войсками через информационные системы противника



Концепция «пяти колец»

Цели воздействия в стратегическом информационном противоборстве (по убыванию важности):

- Политическое и военное руководство;
- Системы жизнеобеспечения;
- Инфраструктура;
- Население;
- Вооружённые силы

Воздействие на эти объекты с помощью сетевых технологий получило название «информационно-сетевая война»



Психологические операции: содержание воздействия

Направления дестабилизации:

- создание атмосферы бездуховности и безнравственности;
- манипулирование общественным мнением и политической ориентацией социальных групп;
- дестабилизация отношений между партиями и движениями;
- провоцирование социальных и национальных столкновений;
- подрыв международного авторитета государства;
- инспирирование ошибочных управленческих решений



Практические примеры

- Операция «Буря в пустыне» (1991) — начало системного применения сил информационной войны;
- Югославия / Косово — информационное сопровождение операции НАТО;
- Ирак (2003) — сочетание киберопераций и психологического воздействия;
- Чеченские кампании (1994–1996, 1999–2000-е) — пример информационного проигрыша федеральных властей, что имело трагические последствия для международного престижа России



Уроки чеченской кампании

Проблемы информационной политики России:

- слабый контроль над международными потоками информации;
- неумение работать с прессой;
- «перепрограммирование» общественности: ухудшение отношения к собственной армии;
- цели боевиков становились «ближе и понятнее» населению



Ключевые особенности стратегического информационного противоборства

Согласно Отчёту RAND MR-661-OSD:

- Сравнительно невысокая стоимость средств;
- Отсутствие статуса традиционных государственных границ;
- Сложность обнаружения начала информационной операции;
- Выделение поля операции в общем потоке информации затруднено

Следствие: возможность отказа от использования военной силы при достижении политических целей.



Тенденции развития

Основные направления:

- развитие средств радиоэлектронной борьбы;
- совершенствование средств информационного противоборства в технической сфере;
- развитие способов психологического воздействия;
- интеграция технических и психологических средств

Прогноз: научно-технический прогресс ведёт к постепенному освобождению человека как действующего звена в информационном противоборстве и возложению его функций на вооружение и военную технику



Заключение

- В начале XXI века информационное противоборство институционализировалось как самостоятельный вид стратегического противоборства;
- Ключевой документ — «Объединённая доктрина информационных операций» (1998) — официально закрепил наступательный характер операций не только в военное, но и в мирное время;
- Информационное противоборство ведётся в двух сферах — технической и психологической, — что требует комплексного подхода;
- Пример чеченских кампаний показал, что проигрыш в информационном противоборстве способен свести на нет военные усилия и нанести стратегический ущерб



Спасибо за внимание!