

# Информационные войны и информационное оружие

**Стратегия национальной безопасности относит к основным угрозам безопасности Российской Федерации:**

- усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей;
- появление новых форм противоправной деятельности, в частности, с использованием информационных, коммуникационных и высоких технологий;
- разведывательную и иную деятельность специальных служб и организаций иностранных государств, наносящую ущерб национальным интересам РФ;
- нарушение безопасности и устойчивости функционирования критической информационной инфраструктуры РФ;
- деятельность, связанную с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма.

# Информационные войны и информационное оружие

Указанные положения конкретизируются в **Доктрине информационной безопасности Российской Федерации**. В перечне угроз РФ в информационной сфере мы находим:

- наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях;
- стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве;
- усиление деятельности организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса;
- увеличение в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики РФ;
- увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры;
- нарастание угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности РФ.

# Информационные войны и информационное оружие

**Наиболее острую форму реализация перечисленных угроз приобретает в процессе реализации концепции информационных войн.**

**«Война»** - общественно-политическое явление, связанное с коренной сменой характера отношений между государствами и нациями и переходом противоборствующих сторон от применения ненасильственных форм и способов борьбы (разрешения противоречий) к прямому применению оружия и других насильственных средств для достижения определенных политических и экономических целей.

По основному виду средств вооруженной борьбы различают ядерную войну; неядерную; химическую; биологическую; бактериологическую; геофизическую; информационную и т.д. Другими словами, все виды войн различаются по виду используемых средств вооруженной борьбы (виду оружия).

Поэтому, **термин “информационная война”** означает, что война ведется с помощью информационного оружия в глобальной информационно-технологической инфраструктуре (ИТИ) - киберпространстве.

# Информационные войны и информационное оружие

**Цель информационной войны:** достижение информационного и информационно-технологического превосходства над противником;

Стратегические задачи информационной войны:

- нанесение ущерба информационной инфраструктуре противника;
- одновременная защита собственной информационной инфраструктуры.

**Информационная война** - это любая атака против информационной инфраструктуры, независимо от применяемых средств. Вывод из строя систем энергоснабжения телецентра - операция информационной войны. То же самое можно сказать и про нарушение алгоритма функционирования программного обеспечения телецентра.

**Население государства противника** – часть информационной инфраструктуры, потому воздействие на массовое сознание – часть информационной войны.

# Информационные войны и информационное оружие

## **Концепция информационной войны.**

Термин «информационная война» появился в середине 80-х г.г. XX века в связи с новыми задачами Вооруженных Сил США после окончания «холодной войны». Начал активно употребляться после проведения операции «Буря в пустыне» в 1991 г., когда новые информационные технологии впервые были использованы как средства ведения войны.

Официально впервые закреплён в директиве Министерства обороны США от 21 декабря 1992 г. и в директиве Комитета начальников штабов Вооруженных Сил США Т9 3600.1 (декабрь 1992 г.). Детально разъяснён в Меморандуме №30 (1993 г.) заместителей министра обороны и председателя Комитета начальников штабов Вооруженных Сил США.

Информационная война - важнейшая составляющая так называемой гибридной войны (войны без вторжения на территорию противника).

# Информационные войны и информационное оружие

**Информационное оружие от обычных средств поражения отличают:**

*универсальность* — его применение не зависит от климатических и географических условий, времени суток, сезонов года и т. п.;

*скрытость* — не требуется проводить мобилизацию, создавать большие группировки войск;

*внезапность применения* — не требуется длительная подготовка;

*экономическая эффективность* — разработка информационного оружия и его применение требуют существенно меньших затрат по сравнению с другими видами оружия;

*масштабность применения* — оно может применяться как для решения задач стратегического, так и тактического уровня;

*эффект «цепной реакции»* — воздействие информационного оружия на отдельный элемент информационной системы информационного ресурса может привести к выводу из строя других элементов системы, а затем и всей системы в целом;

*сложность осуществления контроля за созданием, испытанием, применением и распространением информационного оружия.*

# Информационные войны и информационное оружие

*В соответствии со сферой своего применения* информационное оружие классифицируется на:

- информационно-техническое оружие;
- информационно-психологическое оружие.

*В соответствии со своим целевым назначением* информационное оружие подразделяется на два типа:

- оборонительное информационное оружие;
- наступательное информационное оружие.

*Наиболее распространенные средства наступательного информационного оружия:*

1. Средства воздействия на оборудование объектов информационной инфраструктуры и системы их энергообеспечения;
2. Средства воздействия на информационные ресурсы и программные средства объектов информационной инфраструктуры;
3. Средства воздействия на процесс обмена информации между объектами информационной инфраструктуры;
4. Средства воздействия на массовое, групповое и индивидуальное сознание населения противника.

# Информационные войны и информационное оружие

**Средства воздействия на оборудование объектов информационной инфраструктуры и системы их энергообеспечения могут функционировать:**

## *1. На основе энергетического воздействия:*

- средства силового радиоэлектронного подавления;
- сверхмощные генераторы СВЧ-излучения (гиротроны, рефлектные триоды, релятивистские магнетроны и др.);
- ВМГ, взрывные МГД-генераторы;
- средства силового воздействия через электросеть;
- средства вывода из строя электросетей.

## *2. На основе информационных технологий:*

- программные средства вывода из строя оборудования (резонанс головок жестких дисков, выжигание мониторов и др.);
- программные средства стирания перезаписываемой памяти;
- программные средства воздействия на системы бесперебойного питания и др.



# Информационные войны и информационное оружие

**Средства воздействия на информационные ресурсы и программные средства объектов информационной инфраструктуры** действуют на основе информационных технологий. К ним относятся:

- средства преодоления систем защиты информации;
- средства проникновения в информационные системы противника;
- средства маскировки источников получения информации;
- средства вывода из строя программного обеспечения информационной системы;
- средства скрытого частичного изменения алгоритма функционирования программного обеспечения;
- средства сбора данных, циркулирующих в автоматизированных информационных системах противника;
- средства доставки и внедрения определенных алгоритмов в конкретное место информационной системы;
- средства воздействия на системы охраны объектов.

# Информационные войны и информационное оружие

**Средства воздействия на процесс обмена информации между объектами информационной инфраструктуры действуют:**

*1. На основе энергетического воздействия:*

- средства РЭБ;
- станции помех радиосвязи (в том числе с элементами искусственного интеллекта);
- забрасываемые передатчики помех одноразового использования.

*2. На основе информационных технологий:*

- средства воздействия на протоколы передачи данных систем связи и передачи данных;
- средства воздействия на алгоритмы адресации и маршрутизации;
- средства перехвата и нарушения прохождения информации в технических каналах ее передачи;
- средства вызова перегрузки системы ложными запросами на установление связи.

# Информационные войны и информационное оружие

**Средства воздействия на массовое, групповое и индивидуальное сознание населения противника функционируют на основе информационных технологий:**

- воздействие посредством СМИ; средства пропаганды; средства создания или модификации виртуальной реальности;
- средства имитации голосов операторов систем управления (например, ЛПР) и видеоизображения конкретных людей с их голосом (руководителей государств, лидеров партий и др.);
- средства модификации информации, хранимой в базах данных ИС противника;
- средства ввода в ИС противника ложной информации и данных (целеуказания, мест доставки грузов и др.);
- средства дезинформации;
- средства модификации данных навигационных систем, систем точного времени и др.