«Доктрина информационных операций» США.

По поводу 2 пункта внешних угроз *«стремления ряда стран к доминированию и ущемлению интересов России в мире»*. В США, например, проблемам достижения превосходства в информационных конфликтах, проблемам сохранения национальных интересов в информационном противоборстве, стратегии и тактике применения информационного оружия в конфликтах на различных фазах их развития, судя по источникам информации, уделяется значительное внимание. Так, например, «**Доктрина информационных операций**», разработанная в **США** [*Завадский И .И.* Информационная война - что это такое? Защита информации. - Конфидент, 1996, №4], описывает основные принципы ведения информационной войны, как в условиях вооруженного конфликта, так и в мирный период противоборства двух и более организационных структур.

Вся совокупность информационных операций (ИО), применяемых конфликтующими сторонами, может быть условно разделена на наступательные и оборонительные, причем и те и другие планируются и реализуются совместно и взаимоувязано.

Наступательные информационные операции включают интегрированное использование совокупности возможностей и действий, поддержанных разведанными сведениями и направленных на достижение определенных целей. Другими словами, наступательная ИО представляет собой процесс моделирования поведения противника на основе полученных сведений о нем, модификации этой модели в соответствии с целями нападающей стороны и формировании у противника этой модифицированной модели путем воздействия на него специально подготовленными данными. Самым эффективным и быстро приносящим результаты воздействием считаются ИО, направленные на органы подготовки и принятия решения противника.

Основной принцип применения наступательных ИО, согласно разработанной в США доктрине, заключается в том, что основными объектами их воздействия являются процессы принятия решений человеком.

*К **наступательным** ИО можно отнести* также операции:

- психологические воздействия, например суггестия - скрытое информационное воздействие на организационно-техническую, социальную систему или отдельные личности, как правило, те, на которые возложены функции принятия решений;
- дезинформация;
- радиоэлектронная борьба, как средство воздействия на телекоммуникационные средства и специальные радиоэлектронные средства противоборствующей стороны;
- компьютерные сетевые атаки, в состав которых входят такие воздействия, как распространение компьютерных вирусов, нарушение систем контроля доступа в корпоративные информационные сети, сети банковских структур, информационные сети управленческих структур и пр.;
- физическая атака (разрушение) информации и информационных систем противника.

Наступательные ИО поддерживаются организационными мероприятиями и техническими средствами, обеспечивающими их секретность и скрытность. Их подготовка и проведение сопровождаются сбором информации о противоборствующей стороне и ее аналитическим исследованием. Таким образом, **разведка и шпионаж** можно отнести к разновидностям наступательных ИО. Одна из основных задач планирования и проведения наступательных ИО состоит в обеспечении их скрытности, невидимости для противника. **Коварность информационной агрессии** заключается в том, что она может проводиться вне явного проявления конфликта между противоборствующими сторонами. Сторона, против которой применяется информационное оружие, может и не подозревать об этом, и только при вхождении конфликта в активную фазу, наряду со скрытыми угрозами и операциями в ход идут явные информационные операции, такие как поражение телекоммуникационных средств противника постановкой помех, разрушение информационных систем путем активизации специально введенных в них программно-аппаратных средств и прочее.

К *неявным информационным операциям* относится, в первую очередь, психологическое воздействие. **Под психологической информационной операцией** (ПСИОП) понимают совокупность действий по передаче противнику выборочной информации и установок. Эти операции разрабатываются с целью оказания влияния на эмоции, мотивации, отношения, доминанты, рассуждения, логические выводы и, в конечном счете, на поведение управленческих структур и организаций противника, отдельных групп населения и отдельные личности противоборствующей стороны. Они имеют стратегические, операционные и тактические прикладные программы, включая информационные воздействия, осуществляющие военный обман и дезинформацию противника.

В стратегическом плане ПСИОП могут принимать форму политических или дипломатических действий, объявлений или сообщений. На операционном плане ПСИОП может включать распространение листовок, передачу сообщений с помощью радио и телевизионных широковещательных передач и другие способы передачи информации, которые направлены на деморализацию, бездействие, отступление или сдачу вражеских сил. Постоянное осуществление ПСИОП ускоряет деморализацию противника и способствует дезертирству. На тактическом уровне ПСИОП включает различные способы воздействия, направленные на поддержание постоянного страха и разногласия во вражеских рядах; ПСИОП может влиять на поведение отдельных личностей через непосредственную связь с ними.

Доктрина информационных операций США рассматривает, в частности, операции оказания **гуманитарной помощи** как разновидность информационного воздействия. Примером прекрасно спланированной и успешно реализованной информационной операции может служить создание США фондов поддержки развивающихся стран, через которые осуществлялась финансовая поддержка ученых и развитие в этих странах телекоммуникационных сетей и Интернет-технологий. Цели этой операции - психологическое воздействие на слои общества, являющиеся носителями передовых и критических технологий, создание условий для их эмиграции в США и другие страны запада, создание и расширение технологической базы в виде Интернет для расширения информационной агрессии. В 1999 г. в США разработана архитектура и концепция военных операций через Интернет.

Другим примером применения ПСИОП служит **манипуляция сведениями о событиях**, происходящих в недружественной стране, и представление их в собственных СМИ в таком виде, чтобы сформировать в негативном плане мировое общественное мнение, осуществить ее информационную изоляцию, оправдать применение экономических санкций. Такая информационная операция проводится в настоящее время против России на основе манипуляции сведениями о событиях в Чечне.

Особой областью информационного противоборства являются **средства и методы ведения радиоэлектронной борьбы (РЭБ)**. По существу РЭБ присущи все элементы информационной войны. Отличия можно усмотреть, во-первых, в том, что проявление противоборства наблюдается между организационно-техническими системами и ведется радиоэлектронными средствами, во-вторых, в том, что ввиду ограниченности средств и объектов воздействия в ней до сих пор не использовались напрямую информационные операции типа ПСИОП, а лишь сопровождались ими. Во многом элементы стратегии и тактики РЭБ применяются в других информационных операциях, например, проводимых в компьютерных сетях.

В доктрине информационных операций РЭБ рассматривается и как средство нападения, и как средство защиты. **Средства РЭБ включают**:

- радиоэлектронную разведку, которая может производиться во всем спектре электромагнитного и оптического излучения, а также с применением радиотехнических средств для анализа механических и звуковых колебаний, магнитных полей;
- радиопротиводействие, направленное на подавление электромагнитного воздействия на собственные средства телекоммуникаций и управления;
- радиомаскировку, целью которой является активное и пассивное сокрытие электромагнитных излучений собственных радиоэлектронных средств и других систем;

- помехозащиту, предназначенную для активного влияния на системы управления оружием противника.

Оборонительные *информационные операции* проводятся с целью сохранения работоспособности собственных информационных телекоммуникационных систем, циркулирующей и хранящейся в них информации, а также предотвращения информационного воздействия на собственные системы управления и управляющие структуры. Они призваны гарантировать своевременный, точный и адекватный доступ к собственным информационным ресурсам и исключать возможности эксплуатировать противником собственную информацию и информационные системы для его целей.

Оборонительные ИО включают:

- защиту информационного обеспечения,
- операции по обеспечению секретности,
- физическую защиту информации и информационных систем,
- контробман,
- контрпропаганду,
- контрразведку,
- РЭБ и другие специальные информационные операции.

Защита информационного обеспечения направлена на достижение безопасности информации и информационных систем, гарантируя их доступность, целостность; на идентификацию и аутентификацию пользователей, конфиденциальность и надежность функционирования. Она обеспечивает восстановление информационных систем, включая защиту, обнаружение атак и возможные ответные реакции. Защита информационного обеспечения использует технологии и процессы типа многоуровневой защиты, управления доступом, безопасных сетевых технологий и программных средств обнаружения вторжения.

Оборонительные ИО содержат четыре взаимосвязанных процесса:

- защита информационной среды,
- обнаружение нападения,
- восстановление функционирования,
- ответные действия.

Для обеспечения эффективной обороны необходимо планирование и осуществление всех доступных информационных воздействий как наступательного, так и оборонительного характера в полной их интеграции. Стратегия и тактика применения наступательных информационных боевых средств и средств противодействия им постоянно совершенствуются. Об этом свидетельствуют многочисленные публикации в США, посвященные анализу проводимых информационных операций как в мирной фазе , так и в условиях конфликтов, а также разработке планов развития информационных боевых средств в период до 2025 г.

Наиболее опасным источником угроз информационной безопасности социальным, организационным и организационно-техническим системам являются угрозы, связанные с информационным воздействием. Наиболее подвержены скрытому информационному воздействию молодежь, малообразованные и пассивные слои социальных и организационных систем.