Е.С.Волкова (5 курс, каф. НБ), В.В.Матвеев, д.т.н., проф.

МЕТОДЫ И ТЕХНОЛОГИИ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В УПРАВЛЕНИИ СОЦИАЛЬНЫМИ СИСТЕМАМИ

Уровень развития сетевых технологий, их интеграция в различные области общественной жизни, концентрация узлов сетевой инфраструктуры и других сетевых ресурсов на одних территориях и их отсутствие на других в информационном обществе всегда приводит к промышленному, экономическому, культурному отставанию и общему регрессу территорий и государств, находящихся в стороне от информационных потоков.

Информационное противоборство – соперничество социальных систем в информационно-психологической сфере по поводу влияния на те или иные сферы социальных отношений и установления контроля над источниками стратегических ресурсов, в результате которого одни участники соперничества получают преимущества, необходимые им для дальнейшего развития, а другие их утрачивают [1].

Цель информационного противоборства – обеспечение национальных интересов в информационно-психологической сфере [1]. Одним из важнейших национальных интересов является обеспечение информационно-психологической безопасности государства.

Основные способы достижения целей информационного противоборства: информационно-психологическое превосходство (доминирование); асимметричный ответ на внешние воздействия более сильных субъектов информационного противоборства.

Субъекты информационного противоборства:

- государства, их союзы и коалиции;
- международные организации;
- негосударственные незаконные (в том числе – незаконные международные) вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности;
- транснациональные корпорации;
- виртуальные социальные сообщества;
- медиа-корпорации (контролирующие средства массовой информации и массовой коммуникации – СМИ и МК);
- виртуальные коалиции.

Объектом информационного противоборства является любой объект, в отношении которого возможно осуществление информационного воздействия (в том числе – применение информационного оружия) либо иного воздействия (силового, политического, экономического и т.д.), результатом которого будет модификация его свойств как информационной системы.

Основной инструмент ведения информационной войны – информационное оружие. К информационному оружию относятся, во-первых, средства информационно-технического характера, которые уничтожают, искажают или похищают информацию, несмотря на систему защиты, ограничения доступа к этой информации законных пользователей. А, во-вторых, это средства информационно-психологические, которые дезорганизуют информационные системы, путем дезинформации, выстраивании ложных логических информационных концепций, интерпретаций и пр., воздействуя, таким образом, на общественное мнение, на жизнь общества, государства или группы государств в целом.

Итак, информационное оружие – это «устройства и средства, которые предназначены для нанесения противоборствующей стороне максимального урона в ходе информационной борьбы (путем опасных информационных воздействий)» [2].

Информационная инфраструктура России в виду ряда причин является уязвимой от воздействия наступательных средств ведения информационного противоборства,

получивших название «информационное оружие». К этим причинам «Доктрина информационной безопасности Российской Федерации» относит: отсутствие единой государственной политики в области обеспечения информационной безопасности России; недостаточное финансирование мероприятий по обеспечению информационной безопасности России; увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию создания конкурентоспособных российских информационных технологий; монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами; использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры и т. д.

Информационное оружие возможно классифицировать по методам воздействия на информацию, информационные процессы и информационные системы противника. Это воздействие может быть физическим, информационным, программно-техническим или радиоэлектронным. Основным предназначением такого оружия является контроль информационных ресурсов.

Существует несколько уровней применения манипулятивных технологий в качестве способа управления поведением людей, влияния на их индивидуальное и массовое сознание. Во-первых – это организованное влияние и психологические операции, осуществляемые в ходе реализации межгосударственной политики. Второй уровень информационно-психологического воздействия манипулятивного характера касается использования различных средств и технологий во внутриполитической борьбе, экономической конкуренции и деятельности организаций, находящихся в состоянии конфликтного противоборства. Наконец, третий уровень включает манипулирование людей друг другом в процессе межличностного взаимодействия.

Технические достижения двадцатого века предоставили качественно новые возможности средствам массовой информации, превращающиеся в руках ограниченной части населения в мощный инструмент информационной экспансии. Подлинный плюрализм в средствах массовой информации, точно также как влияние широких масс на информационную политику частных и государственных кампаний, явление весьма редкое и скорее является исключением, чем правилом в силу отсутствия подлинной независимости СМИ. Вместе с тем, мир стоит на пороге очередного прорыва в области распространения информации благодаря расширяющимся всемирным сетям кабельного и спутникового вещания, а они, в свою очередь, способствуют появлению новых технологий информационно-психологического воздействия.

Создание единого глобального информационного пространства, являющееся естественным результатом развития мировой научно-технической мысли и совершенствования компьютерных и информационных технологий, создает предпосылки к разработке и применению информационного оружия. Владение эффективным информационным оружием и средствами защиты от него становится одним из главных условий обеспечения национальной безопасности государства в XXI веке.

ЛИТЕРАТУРА:

1. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. – М.: Горячая линия – Телеком, 2003.
2. Панарин И.Н. Информационная война и Россия. – М.: Мир безопасности, 2000.