Ковалев Алексей Константинович,
аспирант, ФГБОУ ВПО "Северо-Западный институт управления"
(ф) РАНХиГС, Санкт-Петербург
Сухостат Валентина Васильевна,
доцент, к.т.н., к.п.н., ФГБОУ ВПО "Северо-Западный институт управления"
(ф) РАНХиГС, Санкт-Петербург

СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ И ТЕХНОЛОГИЙ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ В ПРОЦЕССЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Интенсивное внедрение информационных технологий, рост удельного веса безопасности информации в обеспечении национальной безопасности государства привели к тому, что информационный ресурс становится одним из главных богатств страны.

Превращение информации в товар привело к резкому обострению международной конкуренции за обладание информационными рынками, технологиями и ресурсами, а информационная сфера в значительной мере определяет и эффективно влияет на состояние экономической, оборонной, социальной, политической и других составляющих национальной безопасности страны.

Возросшее и принимающее все более острые формы за последние годы соперничество в информационной сфере позволяет назвать это соперничество информационным противоборством.

В связи с переходом от силовых методов борьбы к несиловым, мягкой силе и сетевым войнам, изменился характер воздействия. Сегодня главным оружием является информационное влияние с целью подрыва государственного суверенитета. И Россия, как влиятельный игрок на международной арене, подвергается внешнему информационному влиянию наиболее остро.

Анализ процесса современного информационного противоборства

За прошедшую историю как социальное и общественно-политическое явление война не изменила своего внутреннего содержания: она была и осталась борьбой за смену и перераспределение социальных ролей в ходе развития общества. Война сохранила неизменной и свою сущность: выявление управляющей воли путём именно вооруженной борьбы. В то же время, в ходе общественного прогресса война претерпела немало изменений в форме и методах её ведения (рис.1).

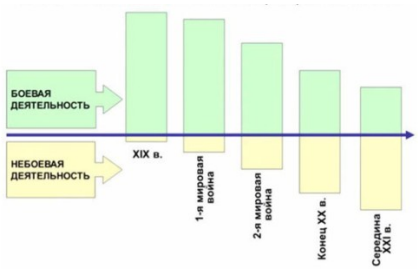

Рис.1 Динамика изменения соотношения боевой и небоевой деятельности войск (сил) на поле боя

Необходимость максимального использования возможностей всех имеющихся средств разведки и боевых платформ привела к переходу от платформоцентрической модели управления войсками и оружием к сетецентрической. Сетецентрическая война предполагает «концентрацию всех имеющихся информационных, политических, военных, экономических и др. ресурсов на поражение (перепрограммирование действий) потенциального противника».

Основной задачей ведения сетецентрических войн является «совокупность действий, направленных на формирование модели поведения друзей, нейтральных сил и врагов в ситуации мира, кризиса и войны».[10, с.104] Это означает установление тотального контроля над всеми участниками настоящих или предполагаемых боевых действий и манипулирование ими во всех ситуациях: когда война ведется, когда она готовится и когда царит мир.

Одной из разновидностей нового типа войн является информационная война как составная часть сетецентрической войны. Здесь в качестве оружия

выступают не пушки и автоматы, а информация. Информационная война – это «открытые и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере».[11, с.13]

Информационное противоборство – это «форма борьбы сторон, представляющая собой использование специальных (политических, экономических, дипломатических, военных и иных) методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленных целей».[9, с.175]

Выделяют два вида информационного противоборства: информационно-техническое и информационно-психологическое. Объектами воздействия и защиты при информационно-техническом противоборстве являются информационно-технические системы (системы связи, телекоммуникационные системы, системы передачи данных).

При информационно-психологическом противоборстве главными объектами воздействия и защиты являются психика правящей элиты и населения противостоящих сторон, системы формирования общественного сознания и мнения, принятия решений.

Таким образом, этот вид противоборства применяется в отношении организационных и социально-экономических систем, к которым относятся жизненная сила страны (население), элита (государственное управление) и материальные объекты и инфраструктура (рис.2).

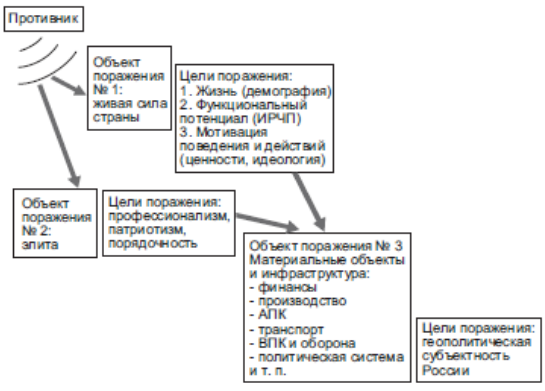

Рис.2 Объекты информационного противоборства

В сегодняшних условиях, когда информация и информационные технологии становятся предметом ведения борьбы, возникает необходимость обеспечения информационной безопасности, т.е. способности государства сохранить свои потенциалы в условиях угрозы и применения против него информационного оружия.

Информационная безопасность на сегодняшний момент затрагивает практически все составляющие национальной безопасности: экономическую, социально-политическую, продовольственную, военную, экологическую и технологическую.

На фоне проникновения информационной структуры во все сферы деятельности государства все более актуальной становится задача обеспечения информационной безопасности как неотъемлемой составляющей национальной безопасности страны.

Государственная политика в Российской Федерации по обеспечению информационной безопасности реализуется через правотворчество, правоприменение и участие государства в развитии правосознания и правовой культуры граждан.

Основными нормативно-правовыми актами и методическими документы в области защиты информации в Российской Федерации являются:

1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 5 декабря 2016 г. № 646.

2. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, утв. Президентом Российской Федерации 9 мая 2017 г. № 203.

3. Стратегия национальной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 31 декабря 2015 г. № 683.

4. Концепция внешней политики Российской Федерации, утв. Президентом Российской Федерации от 30 ноября 2016 г. № 640.

5. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, утв. Президентом Российской Федерации 24 июля 2013 г. № Пр-1753.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики информационной безопасности государства.

В сегодняшних условиях информационно-психологической войны целью государственной политики в информационной сфере должно стать противодействие угрозам информационной безопасности личности, общества и государства. А это, в свою очередь, предполагает совершенствование правового обеспечения информационной безопасности.

Научно-техническое развитие ознаменовало переход к новой модели государственного управления: от прямого принуждения (директивная модель) к мотивационному опосредованному воздействию. В историческом смысле это соответствовало утверждению модели постиндустриального общества.

В новой модели государственного управления важное место занимает формирование контекстов. Теперь решение передается не в виде прямой директивы, а с помощью конструирования программирующего поведение экономического субъекта контекстного поля. Человек воспринимает это решение как собственный выбор, хотя в действительности оно навязывается ему со стороны.

Таким образом, для работы в режиме сетевых войн необходимо новое в ментальном отношении кадровое обеспечение структур государственной безопасности, поскольку главной составляющей успеха в современном государственном управлении являются не директивы управления, а модель, программирующая поведение субъектов через сценарные контексты и использующая несиловые методы воздействия на противника.

Методы и технологии информационного воздействия на потенциалы государственности РФ в условиях современного информационного противоборства

В связи с переходом к новой модели государственного управления, которая заключается в использовании несиловых форм воздействия, изменились и цели борьбы. Теперь это не физическое уничтожение противника и варварский захват его территорий, а тщательно продуманное поэтапное влияние на сознание противника.

В этих условиях важнейшей целью ведения информационного противоборства является разрушение сложившегося восприятия базовых оснований, формирующих культурную идентичность нации, в первую очередь ее духовно-ценностные ориентиры, традиции, обычаи – то, что составляет самобытность народов.

При этом конечной целью информационного противоборства является «завоевание и удержание информационного превосходства над противником, и как следствие, установление тотального манипуляционного контроля, то есть установление мирового господства». [11, с.18]

Государственная система управления и государственность страны представляет собой модель, основными компонентами которой являются государство (институты власти), территория и население, разбивающееся на компоненты «общество» и «человек» (рис.3).

Рис.3 Система государственности

Если устранить один из элементов модели, разрушится вся система. Одной из основных задач информационного противоборства как раз является

деструкция государственной системы управления. В такой ситуации перед атакующим стоит задача выбрать, какой из элементов системы вывести из равновесия в первую очередь.

Задачи информационного противоборства могут быть определены «через воздействие на каждый объект информационного влияния».[11, с.13] Когда объектом информационного противоборства является население страны, то задачи информационного противоборства заключаются в следующем:

- манипуляция массовым сознанием;
- подмена существующей системы ценностей и внедрение ложных ориентиров;
- создание межэтнических и межконфессиональных конфликтов;
- разрушение национальной культуры и подмена языка национального общения.

На территории России с 1994 г. осуществляет свою деятельность американская неправительственная организация Московский Центр Карнеги – подразделение Фонда Карнеги за Международный Мир. В 2007 г. было объявлено о «Новом видении» Фонда, который стал позиционировать себя в качестве первой международной, а в перспективе – глобальной научно-исследовательской организацией (рис.4).

Рис.4 Фонд Карнеги и глобализационные процессы

Центр ведет широкую издательскую деятельность: публикует сборники статей, монографии, справочные и периодические издания. При этом Центр финансируется «Фондом Карнеги за Международный Мир», который,

финансируется американскими и европейскими частными фондами, ТНК и государственными организациями среди которых – фонды Сороса и Рокфеллера, МИД Франции, Госдеп США, Национальный Совет по разведке, министерства обороны и энергетики США, Министерство по международному развитию Великобритании и иные структуры, занятые обеспечением интересов и безопасности своих стран.

С конца 2004 г. ежемесячно по разработанной Центром методологии осуществляется мониторинг уровня демократического развития 10 различных регионов России. Центр Карнеги при помощи Института этнологии и антропологии РАН выстроил слаженную информационно-мониторинговую сеть с отделениями во всех значимых регионах страны, которая занимается сбором информации по наиболее проблемным вопросам развития России. В свою очередь, владение этой информацией и ее тщательный анализ позволяют планировать проведение операций «базовых эффектов» — основных операций эпохи сетевых войн, что создает предпосылки для дезинтеграции страны с последующим разделом на ряд управляемых, слабых в политическом, экономическом и военном отношении территориальных образований.

Для эффективного ответа на деятельность сети неправительственных организаций государству стоит тщательнее изучать социально-ориентированные проекты, предлагаемые некоммерческими организациями, на предмет угрозы общественному сознанию через навязывание ложных ценностей и разрушение фундаментальных оснований государственности.

В последнее время ареной для информационного противоборства становятся социальные сети. Уже сейчас они – существенный инструмент информационного влияния, в том числе – средство для манипулирования личностью, социальными группами и общества в целом.

Увеличение числа пользователей сети Интернет и аккаунтов в социальных сетях ставит необходимость проведения мониторинга социальных сетей на предмет распространения информационных вбросов.

В связи с этим и возникает необходимость изучения моделей влияния в социальных сетях как одного из основных методов информационного противоборства.

Формально социальная сеть представляет собой граф G(V,E), в котором V – множество вершин (агентов) и E – множество ребер (отношений и факторов) связей между агентами, например: знакомства, дружбы, сотрудничества, коммуникации) (рис.5).

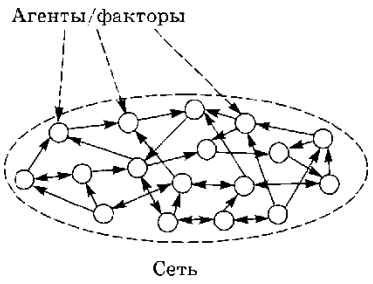

Рис.5 Структура социальной сети

Распространение информации и мнений в социальных сетях можно сравнить с эпидемией, где в качестве вируса разносятся информационные вбросы.

Модель SIR показывает, каким образом распространяются вирусы – ложные мнения, в том числе, и в социальных сетях.

Рассмотрим «модель информационной эпидемии и защиты от нее» [6, с.184-186], как один из случаев информационного противоборства.

В модели информационного противоборства в социальной сети, наряду с обычными агентами (разносчиками мнений) в ситуации участвуют два игрока: *A и B* (рис.6). Между агентами в социальной сети существуют связи, заданные симметричной квадратной матрицей $G = (g_{km}), k, m \in N$. Элемент g_{km} равен 1 (ненулевое доверие), если между агентами k и m имеется связь, либо агенты совпадают (т.е. $g_{km} = 1$ для всех m); в противном случае $g_{km} = 0$.

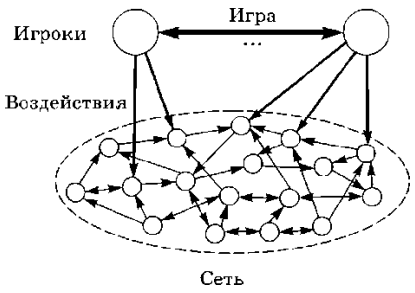

Рис.6 Информационное противоборство

Игрок *B* стремится «инфицировать» сеть, т.е. распространить в сети некоторую информацию, мнение и пр. Для этого он может выбрать одного из агентов и инфицировать его. В каждый момент дискретного времени инфицированным оказывается каждый агент, связанный с инфицированным в предыдущий момент. Формально: пусть в момент *t* имеется множество инфицированных агентов $S_t \epsilon N$.

Тогда в следующий момент *t+1* инфицированными окажутся:
$S_{i+1} = \{m \epsilon N \vee \exists k \epsilon S_i g_{km}=1 \}$.*(1)*

Стратегией игрока *B* в данной игре является выбор агента $j \epsilon N$, с которого он начинает инфицирование сети.

Игрок *A* стремится противодействовать инфицированию. Он проводит периодический мгновенный мониторинг сети, в ходе которого выявляет множество инфицированных агентов и мгновенно останавливает дальнейшее распространение инфекции. Стратегией игрока *A* является выбор периода мониторинга *i*. Выбор периода *i=1* означает, что инфицированным оказывается - при стратегии игрока *B* - агент *j*. Выбор *i=2* означает, что инфицированными оказываются агент *j* и все агенты, связанные с ним (т.е. такие агенты $m \epsilon N$, что $g_{mj}=1$). Множеству стратегий игрока *A* принадлежит также элемент ∞, что означает отсутствие мониторинга.

В общем случае множеством инфицированных агентов при выборе игроками *A* и *B* стратегий *i* и *j* соответственно является множество *Si*, определяемое за *i* шагов из рекуррентного соотношения (1) с начальным значением $S_1 = j$. Обозначим это множество через $\partial(i, j)$.

Игроки выбирают стратегии одновременно и независимо (игра в нормальной форме).

Для описания выигрышей игроков при выборе ими пары стратегий (*i, j*) предположим, что:

1) каждый агент $k \in N$ обладает для игроков некоторой ценностью: a_k для игрока *A* и b_k для игрока *B;*

2) затраты игрока *A* на мониторинг с периодичностью *i* составляют c_i.

При этих двух предположениях выигрыши игроков *A* и *B* при выборе пары стратегий (*i, j*) составляют соответственно:

$$f_{ij} = -\sum_{k \in \partial(i,j)} a_k - c_i, (2)$$

$$h_{ij} = \sum_{k \in \partial(i,j)} b_k. (3)$$

Одним из основных вопросов является моделирование того, какие действия изберут агенты в той или иной ситуации. Набор этих действий агента называется решением игры.

Для контроля блогосферы и социальных сетей необходимо выстраивание взаимодействия государства и бизнеса в вопросах мониторинга социальных сетей. В результате такого сотрудничества, государство сможет использовать исследования компаний по мониторингу социальных сетей в качестве оснований для проверки блогеров.

Рассмотренные методы и технологии информационного противоборства объединяет тот факт, что все они носят манипулятивный характер и направлены на изменение массового сознания общества, при этом факт воздействия для самого объекта остается незаметным.

Рекомендации по совершенствованию государственного управления в России в процессе информационного противоборства

Сегодня перед Россией стоит задача противодействия угрозам информационной безопасности и сохранение своей целостности. Для предотвращения угроз информационной безопасности необходимо выстроить полноценный информационный щит, основой которого должны стать следующие составляющие:

- усовершенствованная нормативно-правовая база;
- единые силовые структуры и органы управления в сфере информационного противоборства;
- государственный медиа-холдинг;
- государственный сегмент Интернета.

Законодательная составляющая выражается в формировании и совершенствование системы правовых норм противодействия угрозам информационной безопасности.

Перед государством стоит задача анализа динамичности развития информационной сферы и дополнения Доктрины информационной безопасности РФ в соответствии с изменениями.

Также в Доктрине должны быть четко определены механизм, содержание и принципы государственной политики в сфере информационного противодействия. В список существующих угроз необходимо включить угрозу цивилизационной идентичности, угрозу идейно-духовным потенциалам государства и угрозу психологической дезориентации общества. В ответ на разрушение цивилизационной идентичности необходимо формально закрепить базовые ценности российской цивилизации; в ответ на разрушение идейно-духовных потенциалов государства целесообразным является создание в рамках новой Доктрины раздела, посвященного обеспечению духовно-нравственной защиты российского общества; в целях предотвращения психологической дезориентации общества, которая проводится через различные каналы СМИ, разработать раздел «О психологической безопасности российских граждан» в новой Доктрине. Стоит уделить внимание повышению компьютерной грамотности населения.

На организационном уровне существует необходимость создания системы противодействия информационным угрозам – совокупность сил и средств, включающая в себя «стратегический анализ и оценку угроз, информационное воздействие и информационное противодействие». [9, с.131]

В связи с этим встает вопрос о создании единого центра управления по предотвращению угроз в сфере информационного противоборства. В перечень функций единого центра следует внести следующие:

- систематическая деятельность по выявлению угроз в информационной сфере и их источников в целях выявления начала атаки для своевременного принятия мер по ее отражению;

- управление существующими силами и средствами и всестороннее обеспечение их действий;
- проведение научных исследований по проблемам этой сферы;
- организация взаимодействия между различными элементами государственной системы информационной борьбы, а также иными государственными и негосударственными структурами и организациями;
- повышение безопасности информационных и телекоммуникационных систем.

В условиях разложения государственности посредством использования информационных средств, актуальной задачей для российского правительства становится расширение влияния российских СМИ на международной арене.

Одним из эффективных элементов системы противодействия угрозам информационной безопасности является создание государственного сегмента в Интернете.

Указом Президента РФ от 22.05.2015 N 260 «О некоторых вопросах информационной безопасности Российской Федерации» сегмент международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении ФСО РФ, преобразован в российский государственный сегмент Интернет.

Государственный сегмент интернета предлагается отнести к критической информационной инфраструктуре России. Через него ведомства должны осуществлять доступ в интернет и публикацию в интернете информационных материалов. За счет использования зашифрованных каналов связи и обслуживания со стороны квалифицированного персонала ФСО госведомства должны получить безопасный доступ в интернет, защищенный от вирусов и хакерских атак, а граждане – доступ к публикуемым ими материалам.

Продвижение внедрения должно осуществляться и на региональные и отраслевые органы власти, с привлечением к работе квалифицированных специалистов в области информационной безопасности.

С изменением характера информационного воздействия возникает необходимость обеспечения информационной безопасности, т.е. способности государства сохранить свои потенциалы в условиях угрозы.

Анализ нормативно-правовой базы Российской Федерации в сфере информационной политики и информационной безопасности показал, что она не полностью отражает современное состояние информационной сферы.

В результате оценки методов и технологий информационного воздействия на потенциалы государственности Российской Федерации, были определены направления совершенствования государственного управления в России в ответ на оказываемое информационное воздействие.

Представленные направления совершенствования государственной политики в сфере противодействия информационным угрозам России и предложенные меры по их реализации при условии системного применения будут способствовать осуществлению эффективной политики государства в сфере информационного противоборства.

Список литературы

1. Указ Президента Российской Федерации от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» // СПС КонсультантПлюс.

2. Указ Президента Российской Федерации от 30.11.2016 № 640 «Об утверждении Концепции внешней политики Российской Федерации» // СПС КонсультантПлюс.

3. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС КонсультантПлюс.

4. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 № Пр-1753) // СПС КонсультантПлюс.

5. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации — СПб.: СПбГУ ИТМО, 2010. — 98 с.

6. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства. — М.: Издательство физико-математической литературы, 2010. — 228 с.

7. Курзенев В.А., Наумов В.Н. Методы и модели прогнозирования социально-экономических процессов. — СПб: РАНХиГС, 2012. — 566с.

8. Манойло А.В. Объекты и субъекты информационного противоборства // Мир и политика. — 2012. — № 12. — С.186-194.

9. Панарин И.Н. Информационная война, PR и мировая политика. Курс лекций. — 2-е изд., стереотип. — М.: Горячая линия – Телеком, 2014. —352 с.

10. Смирнов А.И. Глобальная безопасность в цифровую эпоху: стратагемы для России. — М.: ВНИИгеосистем, 2014. —394 с.

11. Сулашкин С.С. Информационная война против Российской Федерации. Материалы круглого стола. — М.: Научный эксперт, 2011. — 128 с.