

Анатолий НОГОВИЦЫН –
заместитель начальника
Генерального штаба
Вооруженных сил РФ,
председатель Военно-научного
комитета Генерального штаба
Вооруженных сил РФ,
генерал-полковник,
доктор военных наук

Недооценка роли и значения информационных войн может привести к значительному отставанию России от зарубежных стран в области информационных технологий, снизить ее готовность к отражению информационного воздействия.

Информационное противодействие: от подготовки – к готовности*

Характер соперничества современных государств и других объектов социальной природы отражает нали÷ие нового фактора – информационного. Посредством целевого воздействия на информационную систему и среду реализуются угрозы национальной безопасности в разли÷ных сферах деятельности: полити÷еской, экономи÷еской, военной, в области духовной жизни. Применение информационного оружия (этот термин уже никем не воспринимается как метафора) – это скрытое военно-политическое и экономи÷еское давление на информационную инфраструктуру и информационную сферу с целью получения преимуществ и обеспечения своих интересов в материальной сфере без открытого объявления войны.

Борьба в информационной сфере преследует те же результаты, ÷то и вооруженные конфликты, экономи÷еская экспансия и про÷ие виды агрессивных воздействий. Сей÷ас новой целью за÷астую становится разум ÷еловека, и конфликт может быть разрешен не силовыми методами, а применением тех или иных информационных технологий. Этим обусловлено расширение спектра угроз безопасности России.

Под воздействием электронных средств массовой информации и коммуникации на сознание и психику ÷еловека возникла опасность развития в обществе (под÷еркнем, в любом) агрессивной потребительской идеологии, распространения идей насилия, нетерпимости и других негативных явлений. Достижение ими определенных пороговых зна÷ений, характеризующих степень общественно-полити÷еской деструкции, указывает специалисту, ÷то население является объектом информационно-психологи÷еского воздействия как составляющей

* Материал подготовлен на основе лекции, про÷итанной студентам выпускных курсов Российской академии государственной службы при Президенте Российской Федерации в декабре 2008 г.

возможно ведущейся против этой страны необъявленной войны. Примеров тому – множество, ÷то свидетельствует о новых тенденциях ее развития, связанных с прорывом в области информационных технологий. Их анализ потребовал от военно-полити÷еского руководства (ВПР) ведущих государств переосмыслить свои военные политики, провести трансформацию теории и практики строительства вооруженных сил.

В совершенствовании опыта ведения информационных войн мировыми державами можно выделить несколько этапов.

На **первом этапе** (50-60-е годы XX в.) ведение «информационной войны» сводилось к проведению психологи÷еских операций (акций), в ходе которых психологи÷ескому воздействию подвергались в основном ли÷ный состав вооруженных сил, принимающий непосредственное у÷астие в ведении боевых действий, и население прифронтовой полосы.

Для **второго этапа** (90-е годы XX в.) было характерно проведение информационно-психологи÷еских операции (акций), в ходе которых массированному идеологи÷ескому и психологи÷ескому воздействию подвергались население и ли÷ный состав вооруженных сил противоборствующих сторон. Для этого привлекались крупнейшие мировые средства массовой информации (СМИ) и силы психологи÷еской войны государства. Кроме того, в ка÷естве объекта выступала и мировая общественность, обеспе÷ивающая позитивное мировое общественное мнение о действиях субъекта военных действий.

Третий этап (на÷ало XXI в.) характеризуется зна÷ительным возрастанием роли информационного противоборства в достижении превосходства над противником, прежде всего в системах управления.

Активная подготовка к информационным войнам (ИВ) ведется рядом зарубежных стран мира, и в первую очередь США. Уни÷тожение противника в новых реалиях планируется с помощью информационного оружия, способного разрушать сети и компьютерные системы управления военных и других жизненно важных объектов государства. Многие эксперты с÷итают, ÷то по эффективности его можно причислить к оружию массового поражения.

Основные направления ведения информационного противоборства Вооруженными силами США определяет «Доктрина борьбы с системами управления», введенная в действие в 1996 году. Это первый документ, в котором изложены принципы борьбы с системами управления как «объединенное использование приемов и методов безопасности, военного обмана, психологи÷еских операций, радиоэлектронного противодействия и физического разрушения объектов системы управления, при одновременной защите своих сил и сил союзников, а также воспрепятствование аналогичным действиям со стороны противника».

В октябре 1998 года министерство обороны США ввело в действие «Объединенную доктрину информационной войны». Позже она была переименована в



«Объединенную доктрину информационных операций». При÷ина изменения состояла в том, ÷то возникла необходимость разъяснить соотношения понятий информационных операций и информационной войны. Они были определены следующим образом:

- информационная операция – действия, предпринимаемые с целью затруднить сбор, обработку, переда÷у и хранение информации противником при защите собственной информации и информационных систем;
- информационная война — комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-полити÷еское руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника.

На современном этапе информационная война вклю÷ает в себя действия, предпринимаемые в целях достижения информационного превосходства в обеспе÷ении национальной военной стратегии путем воздейст-



вия на информацию и информационные системы противника с одновременным укреплением и защитой собственных информационных систем и инфраструктуры.

Проводя линию на всемерное усиление роли информационного противоборства в решении внешнеполити÷еских зада÷, американское руководство продолжает активно совершенствовать теорию и практику информационных операций, рассматривая их в ка÷естве основы современного военного искусства. По мнению экспертов Пентагона, информационные операции призваны создавать необходимые условия для достижения полного господства над объектом. При этом их цель состоит в том, ÷тобы облег÷ить и обезопасить процесс принятия и реализации решений американским руководством в разли÷ных условиях, а также повлиять на принятие и реализацию решений противником в нужном направлении.

Характер информационных операций к 2020 году будет определять их органическое объединение с военными и иными действиями вооруженных сил и специальных служб. Информационные операции планируется проводить в мирное и военное время, при разрешении конфликтов и в гуманитарных и иных операциях. При÷ем эти действия будут коалиционными или согласованными с аналоги÷ными действиями многонациональных партнеров.

Захват и удержание информационного превосходства над противником приобретает приоритетное зна÷ение по отношению к доминированию на море, на суше, в воздухе и в космосе. Предполагается, ÷то информационные операции могут развиться в самостоятельную отрасль военного искусства, базирующуюся на специальных органах, силах, средствах и обу÷енных специалистах. При÷ем в настоящее время они в явном виде не регулируются нормами международного права, определяющими правила ведения военных действий.

Совершенствование современной американской концепции информационных операций проводится по пяти основным направлениям: развитие теории; повышение эффективности управления силами и средствами; обу÷ение и подготовка специалистов; усиление анализи÷еского и разведывательного обеспе÷ения и усиление оперативных возможностей.

Признается, ÷то действующая сегодня теорети÷еская парадигма «информационной войны» оказалась эклекти÷ной и практи÷ески плохо реализуемой, т.к. она базируется на идее объединения в содержании информационных операций многих разли÷ных и слабо взаимосвязанных между собой областей деятельности. Отме÷ается, ÷то их сближает между собой лишь только тот факт, ÷то они все каким-либо образом связаны с военной информацией. Исклю÷ены из обращения термины «наступательная информационная операция», «оборонительная информационная операция» и «информационная война». Введено и детально раскрыто понятие «информационная обстановка». Предложен новый концептуальный подход к структуре информационных операций, определяющий три основные функции и пять базовых составных элементов, вклю÷енных в содержание понятия «информационная операция».

Приме÷ательно, ÷то до последнего времени решающую роль в информационном противоборстве играли психологи÷еские операции, мероприятия по оперативной маскировке и по обеспе÷ению безопасности собственных сил и средств, однако в новую редакцию доктрины вклю÷ены также сетевые операции и радиоэлектронная борьба как основной вид ведения информационных операций. Остальные элементы отнесены к обеспе÷ивающим (Support) и взаимосвязанным (Related) действиям. По американским документам «*сетевые операции*» (СМ 7) вклю÷ают в себя компьютерные сетевые атаки, сетевую защиту и использование компьютерных сетей противника в своих целях.

В обновленном документе уто÷няется роль и суть физи÷еского уни÷тожения критически важных элементов информационной инфраструктуры и в целом информационных объектов противника: они рассматриваются как вспомогательный элемент информационной операции и представляют собой действия по применению средств огневого поражения и физи÷еского уни÷тожения с целью вывода из строя ключевых элементов системы управления и связи.

Значительное место в новых доктринальных документах отведено взаимодействию США и стран-партнеров в области информационных операций. В них отме÷ается, ÷то каждая страна-у÷астник может иметь свою концепцию информационных операций, однако на раннем этапе желательно включать эти государства в процесс планирования совместных действий. Указывается, ÷то каждое из них может внести вклад в это дело, предоставляя необходимые данные по своему региону. Урегулирование потенциальных конфликтов в информационной сфере между ÷ленами коалиции входит в обязанности командования многонациональных сил.

Наряду с процессом реорганизации органов информационного противоборства ВС США, направленным на их оптимизацию, в США продолжаются разработка новых и усовершенствование существующих средств воздействия на информационные инфраструктуры потенциальных противников.

Информационно-техни÷еское противоборство США планируют вести, в первую о÷ередь, путем организации и проведения кибернети÷еских атак в информационных сетях, а также применяя оружие «направленной энергии».

С другой стороны, так как компьютерные сети становятся все более важным элементом в инфраструктуре государства, они нуждаются в организации глубокой эшелонированной обороны, основанной на постоянной глобальной и региональной оценке обстановки с централизованной возможностью оперативного выявления и идентификации угроз и проведения ответных действий. Такая стратегия основана на «борьбе с сетью», которая рассматривается как система оружия или как система, интегрирующая боевые возможности, приоритетные для выполнения боевых зада÷ объединенными силами.

Информационно-психологическому противоборству придается также особое зна÷ение. В первую о÷ередь это связано с неуда÷ным ходом иракской кампании, которую Белый дом объясняет эффективным ведением Ираком «террористической пропаганды». По мнению американских экспертов, именно благодаря пропаганде в массовом сознании сформировалось устойчивое неблагоприятное общественное мнение о действиях Вооруженных сил США. Вследствие этого США проиграли информационно-психологи÷ескую войну на «идеологи÷еском фронте».

Практика информационно-психологи÷еского противоборства показывает, ÷то террористи÷еские организации активно используют возможности современных информационных технологий. Благодаря Интернету географи÷ески разбросанные и изолированные исламистские группировки превращаются в виртуальное транснациональное террористи÷еское сообщество, в перспективе способное к вполне реальным скоординированным террористи÷еским действиям в глобальном масштабе. Сложившиеся реалии вынуждают Пентагон связывать понятие победы над терроризмом с возможностью дискредитации в общественном сознании экстремистской идеологии. Декларируя необходимость активизации борьбы с террористи÷еской идеологией и распространением идей экстремизма, в том ÷исле и по каналам Интернета, администрация США расширяет понятие «тихих гаваней», подводя под него те ресурсы Интернета, которые представляют террористам возможности для сбора разведывательных сведений, осуществления коммуникаций и планирования террористических действий.

Извлекая уроки из иракской кампании, Вашингтон в своей внешнеполитической деятельности также планирует в перспективе использовать ряд приемов ведения информационно-психологи÷еского противоборства, к которым можно отнести:

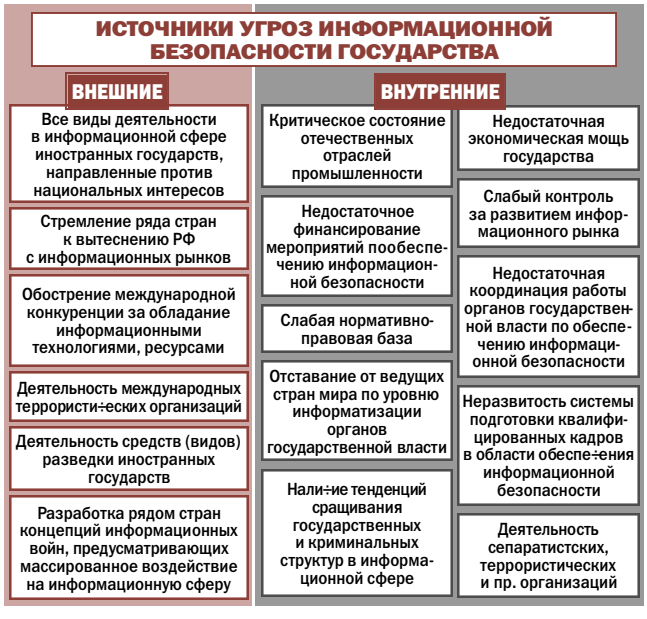
- официальные выступления в СМИ и международных организациях представителей американского истеблишмента с осуждением «нарушений прав ÷еловека» за рубежом;
- публичную поддержку оппозиции, действующей в «репрессивных нациях», вклю÷ая встре÷и с ними на высшем уровне в Белом доме, Госдепартаменте и американских посольствах;
- информационную поддержку «свободных и справедливых выборов», становления «гражданского общества», а также свободы СМИ и свободы вероисповедания;
- дискредитацию представителей власти «репрессивных режимов» путем публи÷ного предъявления к ним претензий и объявления персональных санкций;
- призывы в СМИ к ÷ленам международного сообщества не поддерживать «репрессивные режимы»;
- объявление о создании коалиций с другими «демократическими нациями» с целью «продвижения свободы, демократии и прав ÷еловека» в определенных странах и регионах;
- укрепление и создание неправительственных и других организаций, осуществляющих воздействие на существующие международные у÷реждения (ООН, ОБСЕ, ОАГ, ЛАГ и т.п.), – с тем, ÷тобы использовать их потенциал для установления «демократии в регионах, которые испытывают в ней недостаток»;
- активную пропаганду американских ценностей ÷ерез СМИ, расширение образовательных программ для иностранных студентов и у÷еных, поддержку ÷астного сектора, увели÷ение каналов диалога и контрпропаганды, «÷тобы пустить корни в сердцах и умах людей во всем мире».

Приведенный перечень детализирует новое положение о ведении информационных операций в любых регионах мира в поддержку «общественной дипломатии» с целью продвижения американских внешнеполитических инициатив путем оказания влияния на иностранную аудиторию и средства формирования общественного мнения.

Отсюда со всей о÷евидностью следует, ÷то проведение стратеги÷еского курса Вашингтона на дальнейшую «демократизацию» России будет обеспе÷иваться активным применением всего арсенала современных средств, способов и приемов информационного противоборства.

Это условие должно определять характер государственной политики обеспе÷ения информационной безопасности Российской Федерации, основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. В целом сложившееся положение должно мобилизовать государство и общество к реализации поставленной в Доктрине информационной безопасности Российской Федерации (2000 г.) зада÷е – завершению формирования государственной информационной политики России.

Порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере базируется на соблюдении баланса интересов



ли÷ности, общества и государства в информационной сфере. В основе организации деятельности по обеспе÷ению информационной безопасности лежат принципы соблюдения Конституции РФ, законодательства РФ, общепризнанных положений и норм международного права при осуществлении деятельности РФ.

Все более зна÷имым становится принцип открытости в реализации функций федеральных органов государственной власти, органов власти субъектов РФ и общественных объединений, предусматривающий информирование общества об их деятельности. При этом необходимо у÷итывать условия правового равенства всех у÷астников процесса информационного взаимодействия вне зависимости от их полити÷еского, социального и экономи÷еского статуса, основывающегося на конституционном праве граждан на свободный поиск, полу÷ение, передачу, производство и распространение информации любым законным способом.

В производственно-практи÷еских направлениях деятельности органов государственного управления сверхактуально приоритетное развитие оте÷ественных технологий, производство технических и программных средств, способных обеспе÷ить совершенствование национальных телекоммуникационных сетей, их подклю÷ение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Анализ причин отставания нашего государства в обеспе÷ении информационной безопасности показывает, ÷то необходимо активизировать деятельность по всем направлениям: проведению объективного, всестороннего анализа и прогнозирования угроз информационной безопасности, разработке мер по ее обеспе÷ению; подготовке и реализации федеральных программ обеспе÷ения информационной безопасности, объединяющих усилия государственных и негосударственных организаций в данной области; организации работы законодательных (представительных) и исполнительных органов государственной власти РФ по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности РФ. Специального рассмотрения заслуживает деятельность общественных объединений, направленная на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации.



Сферой особого внимания государства по-прежнему остается разработка, создание, развитие, использование, экспорт и импорт средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации. При всех финансовых сложностях надо и впредь проводить необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ и принимать меры по защите внутреннего рынка от проникновения на него нека÷ественных средств информатизации и информационных продуктов.

В заклю÷ение необходимо сформулировать несколько проблемных вопросов в области информационного противоборства.

В последнее время бытует мнение, ÷то США и НАТО, ÷тобы втянуть Россию в новую гонку вооружений, умышленно раздувают зна÷ение и роль информационных войн, а также успехи в разработке информационного оружия. Коне÷но, доля истины в этом есть. Но нельзя недооценивать и реальные факты, свидетельствующие о создании специальных органов, сил и средств информационной войны как в правительственной, так и в военной и даже в гражданской структурах США и стран НАТО. Недооценка роли и зна÷ения информационных войн может привести к зна÷ительному отставанию России от зарубежных стран в области перспективных, особенно информационных, технологий. Может оказаться зна÷ительно сниженной готовность России к отражению информационного воздействия на нее в слу÷ае новой войны или других военных конфликтов, в том ÷исле проводимых террористи÷ескими силами, ÷то не позволит своевременно разработать более дешевые способы асимметри÷ного ответа на действия агрессивных сил.

В следующем номере:

«Победить в информационной войне может та страна, которая выстроит информа - ционном пространстве и предложит своим гражданам яркий символический проект национальной идеи – систему национальных приоритетов, идей и традиций, – которые для большинства окажутся более значимыми, чем любые информационные воздействия и соблазны извне».

Профессор кафедры российской политики факультета политологии МГУ И.А. ВАСИЛЕНКО