Информационные войны

ЭПИЗОД 1-Й: РУССКАЯ ДОКТРИНА

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

Доктрина информационной безопасности Российской Федерации.

Стремительные темпы развития компьютеризации и информатизации общества неизбежно ведут к созданию единого мирового информационного пространства, в котором будут аккумулированы все средства сбора, накопления, обработки, обмена и хранения информации. По мере внедрения информационных технологий в различные сферы общественной жизни страны возникают серьезные проблемы, связанные с обеспечением исправного функционирования элементов информационной инфраструктуры, сохранности информации и т. д., с которыми уже столкнулись в развитых странах Запада, и в первую очередь в США, обладающих половиной всего мирового информационного ресурса.

ИНФОРМАЦИОННОЕ ОРУЖИЕ

В России уже появился ряд концептуальных документов, рассматривающих информационные угрозы национальной безопасности. Прежде всего, это «Концепция национальной безопасности Российской Федерации» и «Доктрина информационной безопасности Российской Федерации».

Информационное пространство фактически стало театром военных действий, где каждая противоборствующая сторона стремится получить преимущество, а в случае необходимости — разгромить противника. Размах противоборства в информационной сфере достиг таких масштабов, что потребовалось создание специальной концепции, получившей название информационной войны, или информационного противоборства.

Впервые работы по созданию концепции информационной войны начались в США в начале 1990-х годов. В настоящее время существует несколько вариантов трактовок термина «информационная война». Однако отличия между ними незначительны, поэтому с полным основанием можно использовать вариант термина, представленного в Уставе Сухопутных войск США «Информационные операции» (август, 1996 г.). Согласно этому документу «информационная война — это комплекс мероприятий по достижению информационного превосходства путем воздействия на информацию, информационные процессы, информационные системы и компьютерные сети противника при одновременной защите своей информации, информационных процессов, информационных систем и компьютерных сетей».

«Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние. К внешним источникам относится разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним».

Доктрина информационной безопасности Российской Федерации.

Разумеется, в любой войне применяют оружие. Информационные войны в этом плане не исключение. Согласно одному из существующих определений информационное оружие — это комплекс программных и технических средств, предназначенных для контроля информационных ресурсов объекта воздействия и вмешательства в работу его информационных систем. Информационное оружие возможно классифицировать по методам воздействия на информацию, информационные процессы и информационные системы противника.

МЕТОДЫ ВОЗДЕЙСТВИЯ

Это воздействие может быть физическим, информационным, программно-техническим или радиоэлектронным.

Физическое воздействие осуществляется путем применения любых средств огневого поражения. Однако более корректным было бы отнести к информационному оружию физического воздействия средства, предназначенные исключительно для воздействия на элементы информационной системы: противорадиолокационные ракеты, специализированные аккумуляторные батареи генерации импульса высокого напряжения, средства генерации электромагнитного импульса, графитовые бомбы, биологические и химические средства воздействия на элементную базу. С помощью противорадиолокационных ракет в первые дни воздушной операции коалиционных миротворческих сил в зоне Персидского залива (1991 г.) было выведено из строя 80% наземных РЛС Ирака.

Графитовые бомбы применялись американскими вооруженными силами в ходе войны в Персидском заливе и в Косово. Их поражающий эффект достигается путем создания над объектом облака площадью до 200 кв. м из произведенных на основе углерода и обладающих сверхпроводимостью тонких волокон. При соприкосновении волокон с токонесущими элементами (изоляторы, провода и т. д.) происходили короткое замыкание и вывод из строя электросетей.

Биологические средства представляют собой особые виды микробов, способные уничтожать электронные схемы и изолирующие материалы, используемые в радиоэлектронной технике.

Информационные методы воздействия реализуются посредством всей совокупности средств массовой информации и глобальных информационных сетей типа Интернет и станциями голосовой дезинформации.

Так как основным элементом информационной инфраструктуры являются люди, мотивация деятельности которых базируется на их физиологических, социальных и информационных потребностях, то правильно рассчитанное применение так называемых информационно-психологических методов воздействия оказывает прямое влияние на уровень безопасности государства. Особенно это касается России, где пока отсутствует организованная система формирования и поддержания в обществе необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

ТОТАЛИТАРНЫЕ СЕКТЫ

«Наибольшую опасность в сфере духовной жизни представляют следующие угрозы информационной безопасности Российской Федерации:

— деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;

— возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект».

Доктрина информационной безопасности Российской Федерации.

Почему тысячи образованных, умных и на вид благополучных людей позволяют втягивать себя в мириады культов? Чем объяснить тотальный контроль над жизнью последователей, которым обладают псевдорелигиозные организации? Каким образом они добиваются полной покорности и преданности своих членов? Почему их адепты порой готовы отдать жизнь во имя торжества «истинного» учения?

Тоталитарные секты вербуют своих членов очень эффективно. Но, вопреки распространенным мифам, массовый гипноз, «промывание мозгов» и применение физической силы здесь ни при чем. После громких скандалов и судебных разбирательств многие крайности, свойственные прежним методикам «обращения», уже почти не используются. Гораздо чаще приемы психологического кодирования сочетаются с эффективными маркетинговыми методами и добротной рекламой.

Преступный характер деструктивных культов в своей основной, «подводной», части хорошо замаскирован. И лишь иногда он прорывается наружу такими страшными последствиями, как гибель 923 членов Народного храма в Гайане в 1978 г.; 88 сожженных приверженцев Дэвида Кореша в Вако (США) в 1993 г.; еще 53 сожженных адепта Храма Солнца в Швейцарии и Канаде в 1994 г.; едва не состоявшееся массовое самоубийство «белых братьев» в Киеве осенью 1993 г.; 11 жертв и 5000 пострадавших от газовой атаки секты «Аум Синрике» в Токио в 1995 г. Несомненно, что именно культовый характер ряда экстремистских политических организаций на Ближнем Востоке (например, организация «Хамаз» и т. п.) объясняет непрерывное «производство» террористов-камикадзе, взрывающих мины на себе.

Научно-технический прогресс в области информационных технологий, развитие СМИ стерли национальные границы в информационном пространстве и создали беспрецедентные возможности для подавления противника с помощью нетрадиционных средств поражения, не вызывающих физического разрушения. Проходя через сознание каждого члена общества, длительное массированное информационно-психологическое воздействие разрушающего характера создает реальную угрозу существованию нации в результате трансформации ее исторически сложившейся культуры, основных мировоззренческих и идеологических установок.

«ДЕМОНЫ» КОМПЬЮТЕРНЫХ СЕТЕЙ

Средствами реализации программно-технических методов являются компьютерные вирусы, логические бомбы и аппаратные закладки, а также специальные средства проникновения в информационные сети. Эти средства используются для сбора, изменения и разрушения информации, хранящейся в базах данных, а также для нарушения или замедления выполнения различных функций информационно-вычислительных систем.

Средства сбора информации позволяют производить несанкционированный доступ к компьютерным системам, определять коды доступа, ключи к шифрам или другую информацию о зашифрованных данных и по каналам обмена передавать полученные сведения заинтересованным организациям.

«Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

— противоправные сбор и использование информации;

— уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

— перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

— несанкционированный доступ к информации, находящейся в банках и базах данных».

Доктрина информационной безопасности Российской Федерации.

В настоящее время разработаны специальные программные продукты, так называемые ноуботы (Knowbot — Knowledge Robot), которые способны перемещаться в информационной сети от компьютера к компьютеру и при этом размножаться, создавая копии. Ноубот вводится в компьютерные системы и, обнаружив интересующую его информацию, оставляет в этом месте свою копию, которая собирает информацию и в определенное время передает ее. С целью исключения обнаружения в ноуботе могут быть предусмотрены функции самоперемещения и самоуничтожения.

Задачи сбора информации решаются и с помощью программных продуктов «Демон» («Demon»), «Вынюхиватели» («Sniffers»), «Дверь-ловушка» («Trap Door»). Программный продукт «Демон», введенный в систему, записывает все команды, вводимые в нее, и в определенное время передает информацию об этих командах. Аналогично действуют и «Вынюхиватели», которые считывают и передают первые 128 бит информации, необходимых для входа в систему. Программы используются для вскрытия кодов доступа и шифров. «Дверь-ловушка» позволяет осуществлять несанкционированный доступ к информационным массивам базы данных в обход кодов защиты. При этом система и элементы защиты его не распознают.

«Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

— распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

— деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации».

Доктрина информационной безопасности Российской Федерации.

Таким образом, 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.

ВНУТРЕННЯЯ УГРОЗА

Ярким примером внутренней, прежде всего информационной, угрозы является противоправная деятельность «Русского национального единства».

Заключение политологической экспертизы по назначению Южно-Сахалинского городского суда по делу № 2-2077/98 (определение суда от 18.02.1999 г., письмо судьи Л.В. Прокопец от 25.02.1999 г.): «РНЕ пропагандирует культы силы и устрашения, прежде всего, своей атрибутикой и символикой, аналогичными гитлеровскому стилю (приветствие вскидыванием руки, использование свастики), военизированным характером организации и военизированной униформой, также аналогичными фашистскому стилю плакатами, на которых изображены грозные и могучие воины РНЕ, маршами, демонстрирующими силу, призывами к расправе с врагами, а также прямыми угрозами властям».

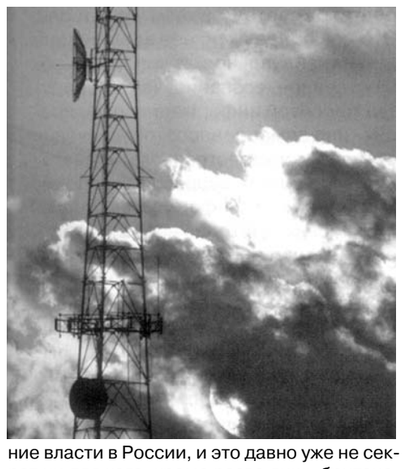
Баркашов дошел даже до оправдания гитлеровских преступлений на почве расизма в отношении славян: «И, кстати, Гитлер был по-своему прав, называя славян «недочеловеками»: народ, позволивший захватить власть в стране большевистскому режиму, другого определения не заслуживает» («Собеседник», № 7, 1993 г.).

Идентификация РНЕ как фашистской организации, осуществленная значительной частью общества, вызвала в конце концов реакцию московских властей, запретивших в декабре 1998 г. проведение всероссийского съезда РНЕ в Москве, закрывших штаб РНЕ в Терлецком парке и запретивших распространение газет и других пропагандистских материалов РНЕ. Подобные акции в последнее время были, как известно, в том или ином виде и масштабе осуществлены и в ряде других городов и регионов России. После отмены регистрации московской региональной организации РНЕ 19.04.1999 г. Бутырским межмуниципальным судом г. Москвы по представлению столичного прокурора С. Герасимова мэр Москвы Ю. Лужков в интервью первой программе телевидения (ОРТ) прямо назвал РНЕ «организацией фашистского типа».

«Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют: информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации».

Доктрина информационной безопасности Российском Федерации.

Скажем, Борис Березовский представляет на сегодня угрозу как внешнюю, так и внутреннюю. БАБ реально готовит свержение власти в России, и это давно уже не секрет ни для кого, кроме разве лишь британских правоохранительных органов. Но то, что беглый лондонский олигарх уполномочен выдвигать программы революционных переворотов со страниц официозной британской прессы, — это, пожалуй, новое слово в многочисленных и неоднозначных похождениях БАБ.



В минувшем августе британский еженедельник The Sunday Times опубликовал очередной манифест «предпринимателя», призывающий к ликвидации «преступного путинского режима». Основным адресатом послания стали западная публика и политическая элита, которых Березовский без обиняков заклеймил «в глубокой интеллектуальной деградации». Из-за этой самой деградации Запад, по мнению лондонского «политэмигранта», недостаточно энергично поддерживает «реакцию Польши, Чехии, Эстонии и других государств на агрессивные действия Путина». Березовский призывает, чтобы Запад «выступил единым фронтом» вместе с восточноевропейскими государствами, чтобы свергнуть «преступный режим» в России.

ХОЛОДНАЯ ВОЙНА

«Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

— вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

— девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе».

Доктрина информационной безопасности Российской Федерации.

Холодная война не окончена. Объявленная России по окончании Второй мировой, она продолжается по сей день и в действительности только набирает обороты. Ее главные сражения еще впереди.

В борьбе за геополитическое влияние и экономические ресурсы соперники России посылают все новые вызовы, запускают информационные вирусы и с помощью современных информационных технологий и средств коммуникации внедряют их в массовое сознание.

Над производством и распространением снарядов информационных атак на Западе работают целые государственные управления, по своему масштабу и влиянию не сильно уступающие официальным спецслужбам. Они формулируют выгодные своей стране мифы, способствуют их распространению и оказывают поддержку тем, кто в силу идеологических или финансовых аргументов их ретранслирует. Они выстраивают свои тезисы в единые, внешне вполне логично выглядящие сюжеты и пытаются как можно более глубоко интегрировать их в общественную «повестку дня» атакуемого государства.

При всей видовой и содержательной разности все эти «отравленные» информационные продукты имеют единую цель: ослабить Россию, разобщить ее народы, убедив их представителей в очередной небылице. Все банально: разделяй и властвуй. Однажды эта технология уже сработала: именно с очернения российской истории и разрушения советской идеологии начался распад СССР. Теперь вдохновленные «удачным экспериментом» авторы хотят повторить его и с Российской Федерацией. Информационная война продолжается.

Вадим ФЁДОРОВ.
По материалам интернет-сайтов.

Заседание коллегии области

(Окончание. Начало на 1-й стр.)

Оптимизации работы загородных оздоровительных лагерей будет способствовать увеличение числа данных учреждений, работающих в круглогодичном режиме. Это благоприятно скажется на здоровье и занятости детей, которые будут обеспечены организованным отдыхом не только в летние, но и в осенние, зимние и весенние каникулы. Как подчеркнул Е.С. Строев, первоочередное право получения путевок на отдых попрежнему должны иметь дети-сироты, дети из малообеспеченных семей и дети, оставшиеся без попечения родителей.

Вторым на заседании был рассмотрен вопрос о работе Службы по государственному строительному надзору по реализации своих полномочий.

По информации руководителя Службы по государственному строительному надзору (СГСН) А.С. Бойко, в настоящее время ведомство осуществляет контроль за более чем 200 стройками различного назначения. За девять месяцев текущего года СГСН произведены 193 проверки на стоящихся и иных объектах капитального строительства.

Итоги надзора характеризуются повышением уровня производственно-технологической дисциплины в строительных предприятиях. Во многих подрядных организациях возобновлена ступенчатость внутрипроизводственного контроля качества строительно-монтажных работ. К числу добросовестных заказчиков-застройщиков, своевременно проводящих экспертизу проектной документации, соблюдающих законодательство в строительной сфере, относятся, прежде всего, такие организации, как центр рыночных отношений «Развитие», ОАО «Орелстрой», ЗАО «Инжилком», ЗАО «ФСК «Чайка», ЗАО «Стройкомплект-2000», ОГУ «Орелгосзаказчик».

Подводя итоги обсуждения, Е.С. Строев подчеркнул, что ответственность Службы государственного строительного надзора возрастает в условиях значительного увеличения объемов строительства, прежде всего — жилищного. Это требует постоянного жесткого контроля на всех этапах исполнения строительных работ.

Внедрение новых технологий строительства требует от сотрудников службы постоянного повышения профессионального уровня, понимания основных тенденций развития отрасли, тесного взаимодействия с другими компетентными органами. «От качества надзорной деятельности в данной сфере напрямую зависят жизни людей», — сказал Е.С. Строев.

В заседании коллегии принял участие председатель областного Совета народных депутатов И.Я. Мосякин.

Пресс-служба губернатора.