Гриняев С.Н.

Поле битвы - киберпространство

Теория, приемы, средства, методы и системы ведения информационной войны

По материалам иностранной печати

Москва, 2004

УДК 519.7

ББК 30.17

Г 856

Книга содержит материал о развитии теории, средств и методов информационной войны в ряде стран, прежде всего – в США. Показан ход развития приемов ведения информационной войны: от «информационной борьбы первого поколения», которая рассматривалась ее авторами как расширение классической радиоэлектронной борьбы, до «информационной борьбы третьего поколения», в качестве которой обсуждаются операции на основе эффектов. Именно операции на основе эффектов сегодня являются основой реализации внешней политики развитых государств в информационную эпоху.

Материал книги сформирован на основе статей, ранее опубликованных автором в «Зарубежном военном обозрении», «Независимом военном обозрении», в «Красной Звезде», а также в целом ряде других изданий.

Книга рассчитана на широкий круг читателей, интересующихся вопросами, связанными с влиянием информационных технологий и процессов глобализации на жизнь современного общества, на проведение внешней и внутренней политики государства, а также на военное искусство в информационную эпоху.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 6

ГЛАВА 1. ИНФОРМАЦИОННАЯ СФЕРА КАК СФЕРА ПРОТИВОБОРСТВА XXI ВЕКА 9

1.1. О тенденциях развития современного мира 9
1.2. Ноополитика – основа американской информационной стратегии XXI века 15
1.3. Особенности становления информационной эпохи 18
1.4. Новые возможности – новые проблемы 22
1.5. Основные элементы модели нового миропорядка – американского глобализма 44
1.6. Угрозы и вызовы информационной революции 53
1.7. Новая геополитическая концепция США в эпоху глобализации и информационной революции 70
1.8. Будущее Евразии. Основные ориентиры прогноза «Глобальные тенденции 2020» 77

ГЛАВА 2. ОСНОВЫ БОРЬБЫ В ИНФОРМАЦИОННОЙ СФЕРЕ. СРЕДСТВА И СИСТЕМЫ БОРЬБЫ В КОМПЬЮТЕРНЫХ СЕТЯХ 93

2.1. О появлении термина «информационная война» в иностранной литературе 93
2.2. Основные понятия информационной войны 96
2.3. Информационная борьба. Информационное превосходство и информационные операции 99
2.4. Определение информационного воздействия и информационного оружия 106
2.5. Распределенные атаки с отказом в обслуживании – наиболее характерный и наиболее опасный тип информационной атаки на компьютерные сети 115
2.6. Системы обнаружения информационных атак на компьютерные сети – оборонительное информационное оружие 118
2.7. Перспективные системы обнаружения компьютерных атак на основе мобильных программ-агентов 144
2.8. Системы контроля и перехвата информации в глобальных информационных сетях 155
2.9. Системы контроля электронных платежей и проблема борьбы с легализацией незаконных финансовых средств международными террористическими организациями 166
2.10. Информационное и технологическое превосходство – основа достижения «всеохватывающего господства» США в XXI веке 181
2.11. Современные тенденции в области защиты информации и информационной борьбы 185
2.12. Изменения в области защиты информации после терактов в США 11 сентября 2001 года 189
2.13. Трансформация подходов к ведению информационной войны в современных условиях. Первое и второе поколение методов информационной войны 196
2.14. Операции на основе эффектов – третье поколение методов информационной войны 199

ГЛАВА 3. ОРГАНИЗАЦИЯ РАБОТ В ОБЛАСТИ ИНФОРМАЦИОННОЙ ВОЙНЫ В США И РЯДЕ ДРУГИХ СТРАН 211

3.1. Взгляды министерства обороны США на проблему разработки и применения информационного оружия 211
3.2. Подход администрации США к обеспечению информационной безопасности информационной инфраструктуры 219
3.3. О реализации Национального плана защиты информационных систем США 223
3.4. О работах Агентства национальной безопасности США 236
3.5. О работах в США по созданию особо защищенных информационных систем 247
3.6. Организация крупномасштабных сетей 257
3.7. Эксперты RAND Джон Арквилла и Дэвид Ронфелд о путях борьбы с сетевыми структурами новых противников 266
3.8. Информационная война как способ разрешения конфликтов в информационную эпоху 272
3.9. О работах в области информационной войны в Великобритании, Франции, Германии, КНР 282

ГЛАВА 4. ИНФОРМАЦИОННАЯ БОРЬБА В КОНФЛИКТАХ ПОСЛЕДНЕГО ДЕСЯТИЛЕТИЯ 301

4.1. Информационная борьба в ходе агрессии против Союзной Республики Югославии 301
4.2. Управляемый хаос - базовая концепция управления кризисом в Македонии 315
4.3. Опыт информационной войны США в Афганистане в ходе антитеррористической кампании 329
4.4. Анализ деятельности сторон по организации и ведению информационной войны в ходе агрессии коалиционных сил против Ирака 351
4.5. Оценка экспертами Национального центра защиты инфраструктуры США угрозы эскалации противостояния между различными общественно-политическими, этническими и религиозными организациями в глобальной сети Интернет 368
4.6. Реализация принципов ноополитики: международный терроризм как инструмент глобального управления в информационную эпоху 382
4.7. Операция «Silver Key». Деятельность спецслужб Запада по нейтрализации интеллектуального потенциала ряда стран мира 398
4.8. Сценарий учений вооруженных сил США по отработке приемов ведения информационной войны 402

ЛИТЕРАТУРА 424

Своим родителям посвящает автор эту книгу

Введение

Вторая половина XX века характеризовалась масштабными изменениями в жизненном укладе общества – процессы глобализации, колоссальные достижения в различных отраслях науки и техники привели к глубоким изменениям в области межгосударственных отношений.

Одно из таких существенных изменений - уменьшение общего числа военных конфликтов между государствами в последнем десятилетии XX столетия. Так, согласно исследованиям Стокгольмского научно-исследовательского института мира (SIPRI), число межгосударственных вооруженных конфликтов в мире медленно, но устойчиво снизилось с 36 в 32 регионах планеты в 1989 году, до 25 конфликтов в 24 регионах в 1997 году.

На этом фоне рядом экспертов отмечается ***взрывной рост числа внутригосударственных конфликтов***, причем природа этих конфликтов, в отличие от межгосударственных, лежит в культурной и духовной (т.е. информационной) сферах и непосредственно не связана с разделом сфер влияния и ресурсов. Большинство современных внутригосударственных конфликтов возникает между этническими и религиозными группами. Поразительно, но значительная часть конфликтов конца XX века имела именно религиозные корни!

В дополнение к материалам SIPRI результаты ряда исследований, проведенных Международным институтом стратегических исследований (IISS) в Лондоне, Научно-исследовательским институтом в Осло (PRIO), а также в рамках Междисциплинарной программы исследования причин

нарушения прав человека (PIOOM) в Лейденском университете в Нидерландах, подтверждают, что за последние годы резко возросло число внутригосударственных конфликтов малой интенсивности.

В ходе научных работ в указанных организациях было расширено изучение случаев применения насилия для достижения политических целей вне межгосударственных вооруженных конфликтов. Рассматривались не одна, а две категории меньших по интенсивности конфликтов: конфликт низкой интенсивности, в котором потери составляют от 100 до 1000 человек убитыми ежегодно, и ***сильно политизированный конфликт***, в котором потери меньше 100 человек в год, но данный тип конфликта имеет существенный отрицательный политический эффект на общество и международное общественное мнение. Причем влияние международного сообщества на конфликты такого рода весьма ограничено, что затрудняет их разрешение.

Другой характерной чертой конфликтов XX века стало то, что в них резко возросла опасность для гражданского населения. Если в начале двадцатого столетия 85-90 процентов потерь в военных конфликтах приходилось на кадровых военных, то в конце двадцатого столетия почти три четверти потерь – гражданское население.

И еще одна интересная тенденция. Экспертами отмечается значительное ухудшение в отношении агрессора к побежденной стороне и мирному населению. По мнению Верховного комиссара ООН по правам человека (UNHCHR), ***гражданские лица сегодня*** не только жертвы войны, сегодня они все больше ***выступают как один из инструментов войны***. Это в полной мере подтвердилось в ходе агрессии США, Великобритании и их союзников против Ирака.

Активизация международного терроризма внесла дополнительную напряженность между странами. Примером тому стала атака международного терроризма против США в сентябре 2001 года, повлекшая за собой развертывание глобальной антитеррористической кампании, крупномасштабную военную операцию коалиционных сил в Афганистане и Ираке.

Характерно, но разрушение биполярной социалистическо-капиталистической модели, долгое время державшей мир в страхе войны, не остановило кровопролитие, потому что причины войн не были устранены. На этом фоне, несмотря на резкий рост значения информационного ресурса государства, одной из основных причин конфликтов все же остается и истощение природных ресурсов планеты при нарастающих темпах их потребления и роста населения планеты. В этой связи ослабленная кризисом, но богатая ресурсами Россия может стать объектом пристального «внимания» со стороны ближних и дальних соседей, нуждающихся в сырье для обеспечения своего существования и развития.

Острое неприятие мировой общественностью варварского отношения к мирному населению, к применению различных средств массового поражения людей вынуждают военно-политическое руководство ведущих стран мира искать новые формы разрешения международных споров.

Указанные тенденции развития военно-политической обстановки в начале XXI века предполагают необходимость пересмотра не только подходов к ведению современного боя, но и к формированию системы национальной безопасности страны в целом.

Учитывая характер и движущие силы конфликтов XXI века, основными средствами их разрешения станут невоенные и, прежде всего, информационные меры.

Автор является сторонником идеи, согласно которой сегодня ряд развитых стран строят свою внешнюю и внутреннюю политику на основе единой информационной стратегии. В США такая стратегия получила в работах специалистов RAND наименование «ноополитика». Именно из этой позиции и строится изложение материала в настоящей работе.

Автор выражает благодарность всем, кто откликнулся на просьбу автора и принял живое участие в обсуждении рабочих материалов книги. Прежде всего, это Чугунов В.С., Прокофьев В.Ф., Матвиенко Ю.А. и многие другие. Особую благодарность и признательность автор хотел бы выразить Хлюстову Михаилу за оказанную помощь и поддержку при обсуждении материала книги.

Глава 1. Информационная сфера как сфера противоборства XXI века

1.1. О тенденциях развития современного мира

Нам с вами довелось жить в интересный, весьма динамичный, насыщенный событиями, но в то же время драматичный период истории. Не каждому поколению удается встретить не только новый век, но и новое тысячелетие. Нам же посчастливилось наблюдать, кроме того, и смену общественной формации! Мы стали свидетелями процессов трансформации, приведших постиндустриальное общество последней трети XX века к обществу информационному начала века XXI. Важнейшей движущей силой этих процессов стала информатизация: глубокое проникновение информационных и телекоммуникационных технологий во все сферы жизни и деятельности человека.

По общему признанию экспертов, сегодня хорошо налаженная распределенная сеть информационно-вычислительных комплексов способна сыграть не меньшую (а по многим оценкам даже большую) роль в общественной жизни, чем ту, что в свое время сыграли электрификация, телефонизация, радио и телевидение вместе взятые. Свидетелем тому человечество стало на примере развития глобальной сети Интернет.

Сегодня Интернет инициирует процесс создания новой виртуальной среды обитания цивилизации. В последние годы Интернет – динамичная, в значительной степени самоорганизующаяся система, позволяющая говорить о новом социальном явлении – открытом Интернет-сообществе.

В последние годы стало абсолютно ясным, и это было подтверждено в Доктрине информационной безопасности Российской Федерации, что информационная сфера, являясь системообразующим фактором современного общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности государств, а с развитием прогресса такая зависимость будет только возрастать.

Во многом современный мир - это уже не только мир, в котором материальная база является предметом ожесточенного соперничества, в этом новом формирующемся мире ключ к успеху будет лежать в умелом управлении информационными возможностями и ресурсами.

Вполне очевидно, что активное и всестороннее внедрение информационных технологий привело к тому, что трансформировалась сама структура общества. Современное общество во многом свободно от национальных границ. В большинстве сфер общественной деятельности появились новые функциональные структуры, в основе которых лежит Сеть. Это и транснациональные корпорации, и современная электронная экономика, и объединения научных коллективов, работающих над единой проблемой, но физически расположенных в разных частях планеты. Но такие изменения коснулись и теневой стороны жизни человечества. Сетевые структуры стали основой мировой преступности и терроризма.

Сегодня резко возрос жизненный темп общества, особенно это касается «хабов» - крупнейших городов, ключевых центров глобального информационного общества. Возросший темп привел к возрастанию числа стрессовых ситуаций: сегодня человек, практически, постоянно живет в состоянии перманентного стресса.

Глобализирующийся мир ставит множество новых вопросов перед человечеством. Все большее значение приобретает электронная торговля. Стираются временные границы. Обсуждается проблема введения единого мирового Интернет-времени. Новые проблемы возникают и в области

законодательства, – проведение электронных торгов в Интернет требует создания новой законодательной базы.

Рисунок 1 Карта одного из сегментов сети Интернет (точками показаны отдельные компьютеры)

Российскими экспертами глобализация характеризуется тремя основными факторами[1]:

- развитие глобальных информационных сетей;
- компьютеризация финансовых систем;
- развитие транспортных сетей.

Топология этих сетей такова, что глобальные связи существуют только между центрами локальных сетей (именуемых в зарубежной прессе «хабами»). Поэтому пространства, покрытые сетями, оказываются неравнозначны в своей ценности. Возникает небольшое количество особых мест. По естественным причинам эти точки в разных сетях имеют тенденцию к географическому совпадению. В результате возникает крайне неоднородная структура. Появляются небольшие участки пространства, «центры гравитации» (center-of-gravity), где доступ к разнообразным средствам коммуникации, как и знаниям, достаточно легкий. Здесь оказывается наибольшее количество образованного населения, именно здесь протекает основная экономическая жизнь. По экспертным оценкам, глобальный мир сегодня – это совокупность таких универсальных центров.

Глобальные центры становятся центрами миграции. Это ведет к очень сильной социальной поляризации: местное население центров обладает большими правами в сравнении с мигрантами.

Глобализация экономики дает возможность практически мгновенного перевода огромных денежных средств. Высокая концентрация банковской сферы в «центрах гравитации» ведет к тому, что большая часть транзакционных расходов остается именно в них. Кроме этого появляются направление виртуальных «центров гравитации» - регионов с низкими

налогами на экономическую деятельность. Это привлекает в такие регионы финансовые средства – появляются различные оффшорные зоны.

Несопоставимость скорости оборота денежных средств в различных секторах новой экономики (в финансовом секторе – минуты или часы, в промышленности – недели и месяцы) ведет к серьезным изменениям в структуре экономики – становится невыгодным вкладывать деньги в производство, а выгоднее их выводить на финансовый рынок. Происходит гипертрофирование финансовой сферы и практическое уничтожение сферы производства. Сегодня из нескольких триллионов долларов ежедневного оборота мировой экономики только 4% тратятся на обеспечение потребностей населения планеты в промышленных товарах и продовольствии. Остальные деньги – это перекачка финансовых средств между банками с целью получения транзакционной прибыли.

В условиях кардинального изменения самих принципов мироустройства под влиянием процессов глобализации особое место занимает вопрос обеспечения национальной безопасности.

Тотальная «сетивизация» общества привела к тому, что наряду с традиционными игроками международных отношений – государствами – все большее значение приобретают негосударственные структуры. Среди совокупности сфер жизнедеятельности современного общества на первое место выходит принципиально новая сфера - информационная.

Рисунок 2 Какая судьба ждет "новый мир по-американски"?

Революционные изменения видны во многих отраслях мировой экономики, прежде всего это область информатизации общества. Волна «цифровой революции» создала абсолютно ***новый экономический сектор***, которого раньше просто не было. Такая ситуация провоцирует рост интенсивности конфликтов с целью захвата и удержания превосходства в данном секторе новой мировой экономики. Капиталом, который играет главенствующую роль в «цифровой революции», является ***интеллектуальный капитал,*** прежде всего, в области информационных технологий. Основной продукт этого сектора — ***информация*** — обладает

[1] Компьютера № 17 (394) 8 мая 2001

уникальными свойствами, не присущими другим секторам экономики. Информация в отличие от всех других ресурсов пригодна для многократного использования и для многочисленных пользователей, при этом, чем больше и чаще она используется, тем более ценной она становится.

Стремительное развитие и повсеместное применение информационных технологий, превращение информации в ценнейший ресурс жизнедеятельности обусловливает движение человечества к информационному обществу. Это нашло отражение в принятой 22 июля 2000 года странами «Большой восьмерки» Окинавской хартии глобального информационного общества, в соответствии с которой Россия становится полноправным членом мирового информационного сообщества. Вместе с тем положение Российской Федерации в этом сообществе будет зависеть от того, что она привнесет в него и насколько сможет обеспечить защиту собственных интересов, в том числе и в области информационной безопасности.

Как отмечается в Доктрине информационной безопасности России, национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе развития технического прогресса эта зависимость будет возрастать. Сегодня информация ***стала инструментом власти***.

Каковы же главные тенденции геополитического развития мира в XXI веке? Согласно мнению ряда ведущих отечественных и зарубежных специалистов, прежде всего, происходит быстрое формирование глобального всепланетарного общества на основе достижений информационной и телекоммуникационной революции. Растут масштабы кризиса духовной сферы жизнедеятельности человечества. В мире создано единое глобальное информационное пространство, в котором развернулось геостратегическое информационное противоборство между ведущими странами мира за достижение превосходства в мировом информационном пространстве[2].

Отличительным признаком информационной эры служит непрерывность инновационного процесса, комплексность нововведений, охватывающих все основные элементы сфер жизнедеятельности общества.

---

[2] Панарин И.Н. Информационная война и власть. – М.: «Мир безопасности», 2001, - 224 с.

В январе 2001 года американской корпорацией RAND были опубликованы результаты исследования «Новые основания роста: американская инновационная система сегодня и завтра».

Этот документ - итог многолетней работы по выбору направления действий правительства США, направленных на поддержку национальной инновационной системы. В документе констатируется, что внедрение инноваций, основанных на научных и технологических достижениях, является основой повышения национального благосостояния Америки.

По мнению экспертов RAND, об этом свидетельствует интенсивное преобразование американской экономики за последние двадцать лет. В таком контексте развитие системы поддержки процесса поиска и внедрения инноваций стало одним из наиболее важных национальных приоритетов, показывающим насколько важно понимание того, что сегодня и в будущем именно инновационные технологии являются источником роста национального благосостояния, подобно тому, как в прошлом таким источником была добыча полезных ископаемых.

Авторы отчета отмечают, что в последнее время существенно изменилось понимание понятия «творческой деятельности». Оно стало более емким. Дискуссии на тему инноваций сдвинули акцент в этом вопросе с отдельных и вполне конкретных изделий (поиск критических технологий, например) к процессам, с индивидуальных выводов - на механизмы получения этих выводов. Эта трансформация взглядов привела к тому, что поиск инновационных технологий превратился в сложную систему тесно взаимосвязанных компонентов. Главные действующие лица в этой системе - частный сектор, правительственные агентства и лаборатории, университеты, некоммерческий сектор исследований – взаимосвязаны друг с другом различными способами, которые не позволяют ни описать, ни проследить эту взаимосвязь.

Однако, как мы увидим далее, процессами глобализации оказались затронуты не только инновационная сфера, но и подходы к проведению внешней и внутренней политики государства в новую эпоху.

1.2. Ноополитика – основа американской информационной стратегии XXI века

Столь внушительные, а главное стремительные изменения привели к тому, что желание удержать глобальное лидерство вынуждает сегодня руководство ряда развитых стран пересматривать роль и место своих государств в новом, быстро меняющемся мире, пересматривать фундаментальные подходы к проведению внешней и внутренней политики.

В последние годы много говорится о «революции в военном деле» (revolution in military affairs), однако, по мнению американских специалистов уже следует говорить и о «революции в дипломатии» (revolution in diplomacy).

Результаты проведенных за последние пять лет исследований по этой проблеме, изложенные в отчете RAND «Рождение ноополитики: формирование американской информационной стратегии»[3], позволили экспертам этого широко известного аналитического центра администрации США сделать выводы о том, что традиционная стратегия в настоящее время претерпевает существенные и глубокие изменения. Сегодня, по мнению авторов, благодаря цифровой и телекоммуникационной революции, мы стали свидетелями рождения ее новой области – «информационной стратегии». И хотя это направление еще не полностью сформировалась, уже стало очевидным, что в дальнейшем оно приведет к существенному пересмотру ряда понятий и ключевых подходов в проведении внешней и внутренней политики государств.

Современный мир - это уже не только мир, в котором материальная база является предметами ожесточенного соперничества, ***в этом новом формирующемся мире ключ к успеху будет лежать в умелом управлении информационными возможностями и ресурсами — стратегическом планировании и управлении***.

Исследования по возможной альтернативе современной политики были начаты с переосмысления самой сути информационного пространства. По мнению экспертов RAND, существующие понятия киберпространства и информационной сферы (как совокупность киберпространства и средств

[3] The Emergence of Noopolitik: Toward an American Information Strategy, John Arquilla, David Ronfeldt, RAND/MR-1033-OSD, 1999, 102 pp., ISBN 0-8330-2698-4

массовой информации) должны быть объединены как части более широкого понятия “ноосферы”. Само это понятие появилось еще в начале XX столетия, и было введено французским ученым Тейаром де Шарденом. Всестороннее развитие оно получило в работах нашего соотечественника, академика Вернадского.

Обсуждение сути «ноосферы» предваряется следующим ключевым предположением: на самых высоких уровнях политического руководства разработка информационной стратегии может способствовать появлению новой парадигмы, основанной на идеях, духовных ценностях, моральных нормах, законах и этике, переданных посредством «мягкой силы» в противоположность традиционной политике силы и ее акценту на ресурсы и способности, связанные с традиционной, материальной «грубой силой».

Считается, что первоначально информационная стратегия сможет достаточно хорошо служить на второстепенных ролях традиционной политики, однако это будет происходить все реже. Государственные деятели будут всегда иметь возможность обратиться за помощью к традиционным формам силы, но с каждым разом будут все больше и больше видеть выгоды в применении стратегии, которая сначала действует «мягкой силой», а традиционную силу используют в дополнительной роли.

Такое стратегическое мышление должно побудить сдвиг в базовой стратегии, сдвиг, постоянно увеличивающийся вместе с возвышающимся значением информационной стратегии.

Рисунок 3 ЦРУ - один из активных игроков в ноополитике

Ноополитика - это форма политического руководства, которая необходима для взаимодействия с ноосферой, самым широким информационным пространством сознания, в котором объединены киберпространство (или «Сеть») и инфосфера (киберпространство плюс средства массовой информации). Ноополитика – это метод реализации внешней политики в информационную эпоху, который подчеркивает первенство идей, духовных ценностей, моральных норм, законов и этики, основанный на применении «мягкой», а не «грубой» силы.

Авторы идеи подчеркивают, что руководящим мотивом ноополитики не могут быть национальные интересы, определенные в терминах государственности. Ими отмечается, что национальные интересы по-прежнему будут играть важную роль, но они должны быть определены больше в общечеловеческом, а не государственном масштабе и быть совмещенными с более широким, даже глобальными интересами в единую расширяющуюся транснациональную сетевую структуру.

В то время как традиционный реализм в политике, исповедуемый Г.Киссенджером, имеет тенденцию ставить во главе угла государства, ноополитика поставит на их место сети государств, государственных и негосударственных организаций. Реальная политика противопоставляет одно государство против другого, однако ноополитика поощряет межгосударственное сотрудничество в коалициях и других совместных структурах.

Вместе с тем, ноополитика вряд ли, по мнению авторов, в ближайшем будущем полностью вытеснит существующую парадигму «реальной политики», основанную на твердой силе. Скорее всего, два подхода будут существовать, поддерживая определенное равновесие, которое будет разным для разных регионов планеты, так как каждому из них свойственно определенное своеобразие. Сегодня некоторые регионы мира - уже полностью погружены в динамику информационного возраста, в то время как другие кажутся средневековым.

Таким образом, ноополитика в ближайшие года еще не станет универсальным средством, она будет более подходящей методологией управления для отдельных регионов мира, но менее подходящей в других. Предполагается, что ноополитика будет наиболее приходной там, где доминируют высокоразвитые общества: например, Западная Европа и Северная Америка. Но она будет менее эффективна там, где условия остаются традиционно ориентированными на государство и материальные ресурсы, а не на коалицию, и таким образом основанными на продолжение применения методов традиционной политики (например, многие регионы Азии).

1.3. Особенности становления информационной эпохи

На современном этапе развития общества многие традиционные ресурсы постепенно утрачивают свое первоначальное значение. Вместе с тем все большее значение приобретает информация. Информация становится сегодня главным ресурсом научно-технического и социально-экономического развития мирового сообщества. Уже принято говорить о новом витке в развитии общественной формации - информационном обществе.

Переход информации в разряд важнейших ресурсов человечества вызывает к жизни и проблему борьбы за обладание этим ресурсом, за право распределять этот ресурс.

Сам этот ресурс является весьма специфичной составляющей в совокупности других ресурсов развития государства. Его объекты и объединяющая их информационная инфраструктура имеют своеобразные особые пространственно-временные характеристики, не ограничивающиеся пределами национальной территории. Эти факторы заметно сказываются на общей оценке потенциала того или иного геополитического субъекта, на его способности к устойчивому развитию, на возможности воздействовать на него извне, восприимчивости к скрытому перераспределению информационного ресурса противника специальными силами, средствами и способами информационной борьбы /6/.

Ряд экспертов отмечает, что ведущееся вокруг информационного ресурса соперничество, борьба за обладание этим ресурсом, достижения и удержания информационного превосходства сегодня занимает значительное место в геополитической конкуренции развитых стран.

С конца 80-х годов XX века во многих странах неоднократно проводились исследования по изучению уязвимости информационных автоматизированных систем различного назначения.

Так, по итогам 2001 года в США было зафиксировано около 300 тысяч случаев вторжения в системы государственного назначения (без учета систем военного назначения). Почти 200 тысяч (65%) таких вторжений оказались успешными. Кроме того, было зафиксировано свыше 16 тысяч вторжений в системы Министерства обороны США.

Возросло количество случаев намеренного внедрения компьютерных вирусов в системы государственного и военного назначения: с 583 в 1995 году и 896 - в 1996 г, до 1200 – в 2000 году. И это только число официально зарегистрированных случаев.

Начиная с 1996 года зафиксирована тенденция роста числа фактов несанкционированного доступа в компьютерные сети федеральных ведомств и увеличение финансовых потерь от подобных инцидентов. Поданным некоторых консалтинговых агентств, средний ущерб от одного компьютерного преступления в США составляет сегодня около 450 тыс. долларов, а ежегодные потери некоторых фирм достигают 5 млрд. долларов.

Кроме этого, по информации ФБР среди методов шпионажа все большую роль играют методы, основу которых составляют компьютерные технологии. Так, Федеральная разведслужба Германии успешно провела операцию под кодовым названием RAHAB, в ходе которой осуществлялось программное вторжение в различные базы данных и компьютерные системы США, содержащие информацию по электронике, авиации, химии, оптике, компьютерам и средствам телекоммуникаций. Ряд подобных фактов хорошо описан в книге «Компьютерная преступность и информационная безопасность», вышедшей в 2000 году под редакцией А.П. Леонова /21/.

В конце XX века ежегодные потери от промышленного шпионажа, в соответствии с отчетами ФБР, составили сумму в размере от 24 до 100 млрд. долл. По оценкам Отдела науки и техники при президенте США, ежегодный урон, наносимый американскому бизнесу иностранными компьютерными хакерами, достигает 100 млрд. долл. Потери от несанкционированного доступа к информации, связанной с деятельностью финансовых структур США, составляют не менее 1 млрд. долл. в год /21/.

Наиболее часто используемый канал, по которому осуществляется сегодня несанкционированный доступ к информации – это сеть Интернет (65% случаев). По результатам тестирования установлено, что 2/3 коммерческих и государственных узлов Интернет не защищены от подобного вторжения.

Внешние атаки могут преследовать и более серьезные цели, чем пассивный сбор данных такие как, например, выведение из строя главных

компьютерных узлов. По мнению экспертов, чтобы парализовать жизненно важные точки созданной инфраструктуры, достаточно нанести удар всего по нескольким десяткам объектов.

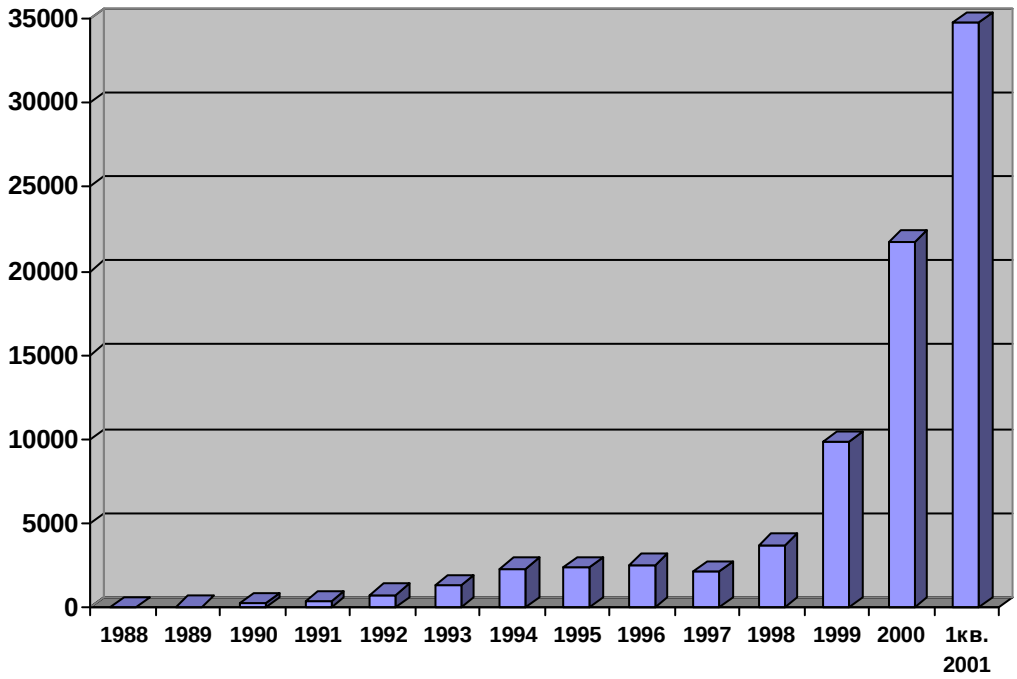

Рисунок 4 Динамика компьютерных инцидентов (по данным CERT)

Результаты масштабного тестирования в 1995-1996 г.г. Министерством обороны США 8932 системы военного назначения с применением средств проникновения, используемых хакерами, показали, что в 7860 (88%) случаях попытки проникновения обнаружены не были.

Все это послужило поводом для предложений администрации президента США по увеличению бюджетных расходов на работы, связанные с обеспечением информационной безопасности и НИОКР в этой области с 1,75 млрд. долларов в 2000 году до 2,03 млрд. долларов в 2001 году.

Отдельной строкой в бюджете предусматриваются расходы в объеме 251 млн. долларов на продолжение и даже активизацию борьбы с хакерами и кибертеррористами.

Кроме того, в последние годы в США, Франции, Великобритании, Швейцарии активно осуществляется реализация концепций комплексной защиты информационных инфраструктур государств. Особый упор делается

на обеспечении безопасности информационных систем правительственных министерств и ведомств.

Темпы научно-технического прогресса создают такую ситуацию, когда техника защиты критических инфраструктур должна догонять быстрорастущий уровень угроз.

Разнообразие информационного оружия, форм и способов его воздействия, особенности появления и применения породили сложнейшие задачи защиты от него. К сожалению, иностранные специалисты первые поняли и оценили значение информационного оружия. Это послужило поводом к разработке стратегической концепции строительства вооруженных сил стран НАТО на ближайшую перспективу – «Единая перспектива 2010» (Joint Vision 2010) - в основу которой положено информационное превосходство над противником во всех сферах ведения военных действий.

Американские военные считают, что преимущество в информационном оружии должно упрочить мировое лидерство США в следующем веке. Этим объясняется большой интерес и активность американцев в исследовании проблем информационной войны. Все сказанное подтверждается докладами и дискуссиями на ряде международных конференции по информационной войне, большую часть участников которых составляют сотрудники государственных учреждений, армии и разведывательного сообщества США - АНБ, ЦРУ, ФБР.

Уже сегодня информационное оружие стало одной из важнейших составляющих военного потенциала США, позволяющей выигрывать малые войны и разрешать конфликты без применения обычных вооруженных сил. В войсках создаются специальные подразделения и структуры для ведения информационной войны. Во всех военных учебных заведениях США введены специальные курсы по информационным войнам и налажен выпуск офицеров по специальности этого профиля. Подробнее реализацию основных положений государственной политики США по вопросу обеспечения информационного превосходства и информационной безопасности мы рассмотрим далее в третьей главе этой книге.

1.4. Новые возможности – новые проблемы

Одна из ключевых проблем в области достижения информационного доминирования в мирное и военное время заключается, по мнению экспертов Пентагона, в интеграции информационных воздействий в общую стратегию национальной безопасности государства. Экспертами вооруженных сил США в ряде работ последних лет отмечается насущная необходимость разработки единой концепции информационной войны, включающей как военный, так и финансовый, экономический, психологический, юридический и другие аспекты.

Характерно, что с развитием подобных работ главная стратегическая цель наступательных информационных действий смещается с активного воздействия на автоматические системы и средства вооружений, ***на личность***, т.е. человека принимающего решения. По мнению экспертов, такие действия могут быть наиболее эффективными в мирное время и на начальных этапах зарождения конфликта, что хорошо согласуется с основными целями политики национальной безопасности США.

Успех в решении новых проблем связывается американскими специалистами с необходимостью широкого реформирования структуры национальной безопасности, включая и военную сферу.

На основе прогноза стратегических условий до 2020 года американские военные эксперты выявили и зафиксировали в официальных документах ряд основных тенденций мирового развития, ставящих перед США потенциальные проблемы в обеспечении национальной безопасности и реализации своих глобальных интересов. При этом отмечается, что заключения, базирующиеся на прогнозе тенденций развития, могут быть относительно точными только для ближайшего времени (от одного года до трех лет), но точность их теряется по мере удаления в будущее. Вполне понятно, что некоторые тенденции (например, демографические) могут быть отслежены с высокой степенью точности. Другие же (типа геополитических) менее предсказуемы. Они подвержены значительно более быстрым изменениям под влиянием различных событий.

Учет тенденций и особенностей различных вариантов развития стратегической обстановки приводит военных аналитиков США к

следующему общему выводу: государства хотя и остаются доминантными единицами международной системы, но во все большей степени будут подвергаться влиянию увеличивающейся мощи многонациональных корпораций и международных организаций.

Развитие технологий, продолжающаяся геополитическая трансформация, демографическое "давление", а также усиление обозначившихся экономических и социальных тенденций могут радикально изменить реалии сегодняшнего времени. Диапазон возможных сценариев широк и их сложно (или невозможно) предсказать. В подобных условиях центральной проблемой для оборонного ведомства является, следовательно, развитие в том направлении, которое позволит эффективно реагировать на любой вариант развития событий. Это предопределяет необходимость постоянной адаптации сил к просматривающимся тенденциям.

В условиях стремительного изменения обстановки в мире, перед руководством американского военного ведомства встает вопрос о скорейшей трансформации вооруженных сил, о придании им способности противостоять современному противнику, активно использующему средства и методы ассиметричной войны.

1.4.1. Трансформация военно-морских сил США

Согласно принятым в США взглядам на военное строительство, ключевые вызовы военно-морским силам в ближайшие 10-25 лет будут исходить от развития асимметричных военных способностей противника, позволяющих предотвратить доступ американских сил к портам, летным полям, базам, инфраструктуре прибрежных районов морей и океанов, доступность которых определяет эффективное применение сил флота на отдаленных театрах военных действий. Считается, что подобные угрозы могут исходить от современных малошумных дизель-электрических подводных лодок, оперирующих на малых глубинах прибрежного шельфа, шахтных комплексов противокорабельных крылатых ракет, а также от систем береговой ПРО/ПВО и - потенциально – от оружия массового поражения.

Ряд аналитиков отмечает, что администрация Буша определила трансформацию вооруженных сил и флота как главную цель ее оборонной

политики. Основные задачи по разработке теоретических положений трансформации военно-морских сил и корпуса морской пехоты США возложены на следующие военно-научные подразделения ВМС США.

Лаборатория изучения приемов противоборства корпуса морской пехоты. С 1995 года лаборатория изучения приемов противоборства корпус морской пехоты (The Marine Corps Warfighting Laboratory, MCWL) проводит цикл экспериментальных тактических упражнений и командно-штабных тренировок, цель которые состоит в отработке принципиально новых приемов боевого применения сил морской пехоты в условиях противодействия угрозам XXI века. Основная направленность тренировок – отработка приемов проведения быстрых, решающих операций в прибрежных районах, новые приемы проведения морских десантных операций, а также отработка действий в городских условиях. Технологическая направленность проводимых исследований – разработка новых видов нелетального оружия и применение беспилотных летательных аппаратов для поддержки действий морской пехоты.

Рисунок 5 Один из проектов боевого корабля нового поколения для ВМС США

Военно-морское командование по изучению основ боевого применения сил флота. Военно-морское командование по изучению основ боевого применения сил флота (Navy Warfare Development Command, NWDC) было сформировано в 1998 году и расположено в военно-морском военном колледже в г. Ньюпорт. Основная задача командования – генерировать новые идеи преобразования военно-морских сил, а также оценивать предложения, подготавливаемые другими подразделениями флота. В настоящее время NWDC координирует ряд масштабных учений сил флота (Fleet Battle Experiments, FBEs), цель которых состоит в исследовании новых военно-морских оперативных концепций.

Среди важнейших проектов, целью которых является определение облика перспективных сил флота, являются следующие программы.

Сетевое противоборство. До настоящего времени центральной концепцией, подкрепляющей усилия по преобразованию сил флота, является

сетевое противоборство (network-centric warfare, NCW), которое основано на использовании современных информационных технологий для организации взаимодействия персонал, боевых кораблей, авиации и береговой инфраструктуры в составе информационных сетей, способных к быстрой передаче критической информации.

Эксперты в управлении флота полагают, что NCW значительно увеличит способности военно-морских сил и их эксплуатационную эффективность. Основу реализации концепции NCW составляют программы формирования единой системы ПРО/ПВО по программе Cooperative Engagement Capability (CEC), программа IT-21 по созданию корпоративную интрасети для военно-морских судов и программа развертывания внутренней сети корпуса морской пехоты ВМС США (Navy/Marine Corps Intranet, NMCI).

Проект «Уличный боец» («Streetfighter»). Проект «Уличный боец» выполняется, главным образом в Военно-морском военном колледже под руководством адмирала Артура Жебровски (Arthur Cebrowski), раннее активно покровительствовавшего NCW. Проект нацелен на разработку принципиально новых способностей военно-морских сил и эксплуатационных концепций их применения для борьбы в прибрежных водах, защищенных силами береговой обороны. Предполагается, что в результате реализации программы «Уличный боец» силы, сформированные на основе отработанных принципов, могли бы составить специализированное 10-20-процентное дополнение к сегодняшним военно-морским силам. Планируется, что такие специальные силы будут включать три главных элемента - сети небольших, распределенных датчиков, беспилотные летательные аппараты и транспортные средства, для развертывания сетей датчиков, а также новые виды судов (особенно скоростных и малоразмерных), которые могли бы эффективно уклоняться от средств поражения противника и решать задачи прорыва береговой обороны.

Кроме перечисленных программ выделяется еще несколько направлений исследований. Так, флот стремится увеличить число целей, которые авианосная группа может атаковать в течение 24 часов, от нескольких сотен до тысячи, путем наращивания числа вылетов самолетов палубной авиации и увеличения количества хранимых на авианосце средств

поражения (бомбы, крылатые ракеты и др.) для самолетов палубной авиации. Работая в этом направлении, флот развивает проекты авианосца следующего поколения CVX, беспилотного воздушного транспортного средства, беспилотного боевого ударного летательного аппарата палубного базирования.

Усилия по преобразованию надводных кораблей сосредотачивают на эсминцах класса Sumrall (DD-21), которые будут широко оснащены средствами автоматизации, с целью резкого снижения необходимой численности экипажа. Также для этого класса кораблей разработан принципиально новый проект корпуса малой заметности, современные системы разведки и управления огнем. Кроме того, установка элементов системы противоракетной обороны на надводных судах ВМС даст флоту возможность участвовать в решении задач обеспечения прикрытия от ударов баллистических и крылатых ракет объектов на континентальной части США. Одним из перспективных проектов является создание (совместно с DARPA) подводного транспортного корабля.

Столь широкая и разнообразная программа модернизации военно-морских сил США в последнее время вызывает все больше вопросов среди военных экспертов и аналитиков Пентагона.

Ряд высокопоставленных чиновников военно-морских сил США утверждают, что текущее состояние дел в области трансформации сил флота вполне приемлемо, что флот в ближайшее время будет способен выполнить все возлагаемые на него задачи по прорыву береговой обороны противника и по обеспечению условий, необходимых для развертывания армейских подразделений и авиации. Вместе с тем ими утверждается, что существующая в настоящее время практика финансирования процессов трансформации ВМС должна быть пересмотрена. Необходимо обеспечить сбалансированное финансирование работ по новейшим программам, а также по программам перевооружения и модернизации сил флота.

Существует, однако, и другое мнение, согласно которому в сегодняшней сложной международной обстановке предпринимаемых усилий по трансформации ВМС явно не достаточно. Предпринимаемые усилия должны быть существенно расширены и ускорены, если американские военно-

морские силы собираются эффективно выполнять возложенную на них миссию в ближайшие 10-25 лет. Ряд аналитиков, поддерживающих эту точку зрения, утверждают, что некоторые мероприятия, представленные должностными лицами ВМС как трансформационные фактически нацелены всего лишь на процессы модернизации существующего вооружения без внесения революционной новизны.

Прежде всего, подвергается сомнению будущее эффективное использование авианосцев и других надводных кораблей в хорошо защищенных прибрежных водах. Ряд экспертов утверждают, что необходим пересмотр существующих приемов боевого применения сил флота с тем, чтобы американские военно-морские силы имели возможность участвовать в конфликте с возможно более дальних дистанций от берега, чем это запланировано в настоящее время. В свою очередь это поднимет вопросы об уместности инвестиций в ряд проектов, включая беспилотные самолеты палубного базирования, проект нового корабля огневой поддержки десанта и, собственно, вопросы применения морского десанта.

Сторонниками интенсификации процессов трансформации военно-морских сил предлагаются следующие основные шаги по ускорению проводимых работ.

Создание ***военно-морских экспериментальных сил (Fleet Battle Exercises/experimental forces).*** По мнению аналитиков сегодня необходимо расширить практику применения результатов учений по программе FBEs в практику боевого применения сил флота, а также гарантировать, что результаты проведенных исследований – это практически важное достижение в развитии теории противоборства на море, а не простые демонстрации существующих способностей. Другие варианты включают создание постоянных экспериментальных военно-морских сил для проверки новых идей без привлечения регулярных частей флота.

Проект «Уличный боец». Ряд специалистов предлагают расширить возможности проекта «Уличный боец» по формированию боеспособных подразделений прорыва береговой обороны, имеющих на вооружении соответствующие быстроходные малозаметные корабли. При этом целесообразно уже в самое ближайшее время приступить к практической

отработке приемов боевого применения подобных сил специального назначения.

Альтернативная архитектура военно-морских сил. Среди руководства военно-морских сил США существует мнение о необходимости разработки ряда принципиально новых концепций строительства военно-морских сил. Это связано с тем, что существующая архитектура ВМС закладывалась сразу после Второй мировой войны и во многом сегодня устарела, а эволюционные процессы частичного ее изменения не могут полностью удовлетворить текущие потребности в организации эффективного управления современными силами флота. Альтернативная архитектура сил флота должна учитывать принципиально новые возможности перспективных проектов палубной авиации, надводных и подводных судов, а также современные особенности организации систем разведки, управления и связи.

Беспилотные транспортные средства. Ряд экспертов считает, что в текущих условиях необходимо увеличение финансирования проектов по разработке беспилотных подводных транспортных средств, беспилотных транспортных летательных аппаратов и беспилотных ударных летательных аппаратов палубного базирования.

Подводное оружие и системы разведки. Многие сходятся во мнении о необходимости скорейшего развития подводных средств вооружения, что позволит серьезно повысить эффективность действий сил флота в прибрежных районах.

Одним из наиболее важных проектов в этом направлении считается переоборудование четырех старых подводных лодок «Трайдент» (SSBNs) в носителей крылатых ракет (SSGNs). Проблема переоборудования старых атомных подводных лодок заключается в том, что в их энергетических установках уже выработалось все ядерное топливо и необходимо принимать решение о целесообразности перевооружения с последующей повторной заправкой реактора, либо о списании лодок из состава флота.

Судно арсенала. Другим предложением, направленным на интенсификацию работ по трансформации ВМС является возобновление проекта создания судна-арсенала, начатую в 1996 и прекращенную в 1997 году. Судно-арсенал должно быть большим надводным кораблем с

небольшой командой и вооружением в 500 крылатых ракет.

Острова-базы. Ряд экспертов ВМС предлагают развивать вместо авианесущих групп направление создания искусственных баз-островов на основе ряда сцепленных нефтяных платформ. Такие острова позволят обеспечить необходимое удаление от береговой черты противника и использовать ля нанесения авиационных ударов обычную сухопутную авиацию, которая по соображениям дистанции взлет/посадка не может использоваться на авианосцах. Такие базы могут также использоваться и для обеспечения действий сухопутных сил и авиации на удаленных театрах военных действий.

В целом эксперты признают, что военно-морские силы останутся одной из важнейших составляющих военной мощи США и в ближайшие годы. Кроме того роль ВМС в проводимой антитеррористической операции позволяет командованию ВМС активизировать ряд процессов, направленных на трансформацию существующей архитектуры флота, на придание ей способности противодействовать угрозам XXI века, которые, как полагают эксперты Пентагона, будут исходить в основном не от регулярных армий, а от сетевых структур транснациональной преступности, террористических организаций и стран-изгоев.

1.4.2. Основные программы работ по трансформации военно-морских сил США

Ряд российских и зарубежных военных экспертов отмечают, что сетевое противоборство (network-centric warfare, NCW) остается одной из базовых и наиболее перспективных стратегических концепций развития военно-морских сил США в ближайшее десятилетие.

Как отмечают военные эксперты Пентагона, цель создания этой концепции заключается в том, чтобы организовать усилия по преобразованию и подготовке ВМС к военным действиям в конфликтах XXI века. Основной акцент в развитии концепции NCW сосредотачивается на использовании современных информационных технологий для формирования единой интегрированной сети информационных систем военно-морских судов, палубной авиации и береговой инфраструктуры. Создание такой сети позволит существенно сократить время на оценку

ситуации и принятие решений в ходе применения сил флота, что даст возможность командующему завоевать информационное превосходство над противником и действовать внутри его цикла управления. По мнению ряда экспертов, внедрение подобной концепции могло бы значительно повысить боевую эффективность военно-морских сил и привести к существенным изменениям в военно-морской тактике, доктрине боевого применения, а также к изменению структуры сил и средств флота.

Ключевыми научно-исследовательскими и опытно-конструкторскими программами, в рамках которых осуществляется реализация концепции NCW, являются: программа кооперативного взаимодействия при отражении атаки противника на силы флота (Cooperative Engagement Capability, CEC), программа IT-21 и программа создания внутренней сети корпуса морской пехоты США (NMCI).

Одной из наиболее серьезных угроз ВМС США в ближайшие десятилетия будет угроза применения противокорабельных крылатых ракет типа «Гранит» и «Базальт» российского производства. С целью противодействия этой угрозе в рамках программы CEC осуществляется разработка единой интегрированной информационно-телекоммуникационной сети, объединяющей военно-морские суда и самолеты палубной авиации в единственную разведывательно-ударную сеть противовоздушной и противоракетной обороны. Наличие такой сети позволяет в реальном времени интегрировать данные о целевой обстановке, полученные от радарных установок, размещенных на кораблях и самолетах ВМС в единое информационно поле целевой обстановки на театре военных действий. Наличие такого информационного поля позволяет организовать на основе данных, полученных с других кораблей и самолетов, поражение противокорабельных крылатых ракет средствами ПВО с кораблей, радиолокационные средства которых не могут непосредственно обнаружить цели, на которые выдается целеуказание. Наличие подобной сети позволяет также организовать управление ракетами ПРО/ПВО, запущенными одним кораблем, другим кораблем или самолетом, что существенно расширяет возможности имеющихся средств противоракетной и противовоздушной обороны.

Эксперты ВМС США заявляют, что CEC – это ключевой элемент всей

концепции NCW, который обеспечивает революционное усовершенствование противовоздушной и противоракетной обороны авианосной группы. По их мнению, CEC также имеет многообещающий потенциал для интегрирования с информационными системами армейских комплексов ПРО/ПВО типа «Patriot» и системой дальнего радиолокационного обнаружения и предупреждения АВАКС.

Планируется, что к интегрированной информационной системы ПРО/ПВО в первую очередь (в течение ближайших лет) будут подключаться авианосцы, крейсеры и эсминцы, оборудованные системой ПРО/ПВО «Aegis», некоторые десантные суда и самолеты раннего радиолокационного обнаружения и предупреждения E-2C «Hawkeye».

Еще в 1994 г. по личному указанию министра обороны Уильяма Перри работы по реализации программы CEC были активизированы как одни из наиболее значимых для реформы ВМС. Опытный образец системы проходил испытания в начале 1996 г. в ходе учений «Mountain Top». Планировалось также проведение сертификации и ввод системы в состав ВМС США в конце 1996 г. Однако, до настоящего времени система не введена в боевой состав флота. В ходе испытаний был выявлен целый ряд недостатков, особенно в области радиоэлектронной совместимости средств обнаружения и управления огнем, а также несовместимость программного обеспечения системы CEC и существующей систем ПВО на некоторых судах, особенно оснащенных последней, шестой версией системы ПВО Aegis. После устранения выявленных недостатков, очередной вариант системы CEC был опробован в феврале-марте 2001 г.

Кроме проблем с функционированием системы серьезным препятствием является и недостаток канального ресурса для обслуживания потребностей CEC. Должностные лица ВМС США признают, что система CEC (и NCW вообще) вносят существенные проблемы в организацию информационного обмена с силами флота в силу того, что основным слабым звеном становится отсутствие достаточного количества широкополосных каналов связи (прежде всего космических) из числа доступных флоту в настоящее время.

По некоторым данным, один из подрядчиков, выполняющий заказы по

созданию СЕС, предложил дополнить СЕС подсистемой названной «тактической компонентной сетью» (Tactical Component Network, TCN). Эксперты утверждают, что включение TCN в состав СЕС позволит существенно уменьшить потребную полосу пропускания, не сокращая при этом эффективность СЕС.

Что касается программы IT-21, то она является одной из крупнейших инвестиционных программ ВМС США, основной целью которой является организация интегрированной сети флота, объединяющей информационные системы кораблей и позволяющей объединить процессы обмена тактическими и административными данными как во внутренней сети отдельного корабля, так и между судами ВМС. Предполагается, что создаваемая по программе IT-21 сеть будет построена на базе широкодоступных, коммерческих технологиях и средствах вычислительной техники и обеспечит передачу мультимедиа-данных (текст, данные, графика, изображения, голос и видео). Эксперты ВМС США утверждают, что создаваемая сеть необходима для реализации концепции NCW и без нее невозможна намеченная трансформация ВМС в соответствии с новыми угрозами. Полагают, что реализация IT-21 значительно улучшит боевую эффективность ВМС США и позволит получить существенное сокращение материальных затрат, а также времени и привлекаемого личного состава, для выполнения различные тактических и административных задач.

Программа создания внутренней сети корпуса морской пехоты США (NMCI) – это программа построения сети, которая свяжет воедино силы флота и корпуса морской пехоты аналогично взаимодействию кораблей ВМС по программе IT-21. После завершения создания в 2003 году, NMCI будет объединять около 360 тысяч автоматизированных рабочих мест в местах базирования частей и подразделений морской пехоты на континентальной части США, Гавайях, Гуаме, Пуэрто-Рико, Гуантанамо (Куба) и в Исландии.

Еще в октябре 2000 года руководство ВМС США заявило, что предоставило группе компаний во главе с корпорацией Electronic Data Systems (EDS) контракт на 6.9 миллиардов долларов на монтаж, поддержку и периодическую модернизацию NMCI в течение последующих 8 лет.

Рисунок 6 Проект беспилотного аппарата палубного базирования

Первые 42 тысячи автоматизированных рабочих мест NMCI в 29 местах базирования уже установлены. Планируется, что система будет полностью развернута к октябрю 2003 года. Вместе с тем, руководство ВМС США полагает объединить усилия по реализации проектов NMCI и IT-21. Это связано с рядом трудностей, возникших при развертывании масштабной сети по проекту NMCI. Прежде всего, вызывает сомнение способность ВМС финансировать в должном объеме создание двух схожих сетей по отдельным программам, а также выполнение программ NMCI и IT-21 без ущерба другим задачам по реформированию ВМС США.

Как отмечает ряд экспертов, реализация трех базовых программ внедрения концепции NCW в ВМС США ставит ряд серьезных проблем перед руководством ВМС США, которые должны быть разрешены в ближайшее время. В противном случае часть программ может быть закрыта по причине недостаточного финансирования.

Среди возможных проблем внедрения концепции NCW в практику боевого применения сил флота эксперты выделяют следующие.

Технические проблемы в программе CEC. Среди экспертов до настоящего времени нет единого мнения о том, удалось ли решить все выявленные на этапе испытаний проблемы. Делается вывод о том, что предложенный в последнее время руководством ВМС новый график ввода системы CEC может быть в очередной раз сорван. Кроме этого выявленные проблемы интеграции сложных технических систем на этапе развертывании системы CEC показали отставание теоретических вопросах построения и взаимодействия сложных человеко-машинных комплексов от практики их реализации.

Адекватность существующей полосы пропускания каналов нуждам CEC. Эксперты отмечают, что нерешенным остается вопрос об интеграции TCN в структуру CEC как часть решения проблемы оптимизации управления полосой пропускания доступных каналов, а также то, что этого решения окажется достаточным для эффективного функционирования CEC.

Контроль реализации проекта NMCI. По мнению экспертов,

потенциальные проблемы проекта NMCI касаются вопросов финансирования этого проекта и его приоритетности в сравнении с другими задачами ВМС США. Остается под сомнением и вопрос, связанный с оценкой эффективности развертывания системы NMCI, в сравнении с уже существующими информационными системами.

Вопросы, касающиеся NCW в целом. В отношении концепции NCW эксперты выделяют следующие потенциальные проблемы, касающиеся концепции в целом:

- *тактика, доктрина и организация:* руководство ВМС признает, что для достижения эффективного применения новой концепции предстоит развить новую тактику, доктрину боевого применения и организацию военно-морских сил; это может повлечь значительные изменения в существующих приемах борьбы на море и ставит серьезную проблему переквалификации всего персонал флота;

- *перспективный облик ВМС:* сегодня флот пытается добавить NCW к уже существующей архитектуре, которая постепенно формировалась в течение нескольких десятилетий. Проблема состоит в том, каким образом концепция NCW учитывается в принятых в ВМС взглядах и планировании будущего облика военно-морских судов, самолетов палубной авиации и облика ВМС в целом;

- *способность к взаимодействию союзников:* эксперты считают, что если бы флот НАТО и другие союзнические флоты вкладывали средства в развитие NCW, то способность к взаимодействию в рамках этой концепции резко возросла, однако в настоящее время не наблюдается инициативы со стороны союзников США к участию в развитии этой концепции. Единоличное же развитие новой концепции формирования и применения ВМС с течением времени все более и более будет осложнять вопросы взаимодействия сил США и союзников;

- *информационная безопасность*: руководство ВМС США признает, что одним из слабых звеньев разрабатываемых проектов остается недостаточная защищенность информационных систем от воздействия со стороны противника с использованием сил и средств информационной войны.

1.4.3. Трансформация военно-воздушных сил США

Афганская антитеррористическая кампания поставила перед американскими военными ряд серьезных проблем. Которые потребовали принятия мер по серьезному пересмотру форм и способов применения вооруженных сил в ходе подобных операций. Так. По мнению американских экспертов, в ходе антитеррористической кампании будут наиболее часто использоваться следующие формы действий вооруженных сил:

• предоставление военной и гуманитарной помощи режиму (совместные военные действия, военные советники, обучение, контакты между представителями вооруженных сил, гуманитарные операции);

• разрешение кризисов и стабилизация (поддержание мира, принуждение к миру);

• прямые военные действия на территории государства без согласия его руководства.

Наиболее вероятно, что указанные действия будут иметь место в регионах, которые сильно отличаются друг от друга по внутриполитической обстановке, климату, географии и характеристикам угрозы. Специалисты Пентагона считают, что в течение ближайших нескольких лет наиболее вероятными точками, в которых американские вооруженные силы могут оказаться вовлеченными в борьбу с террористическими организациями, являются Алжир, Босния, Колумбия, Эквадор, Сальвадор, Гондурас, Индонезия, Кения, Никарагуа, Панама, Перу, Сомали, Судан, Таджикистан, Узбекистан и Йемен.

Рисунок 7 В будущем ставка будет сделана на беспилотные аппараты. Стратегический БПЛА "Global Hawk" заходит на посадку

Масштабы возможных операций и их географическое разнообразие влечет за собой необходимость изменений в структуре и функциях военно-воздушных сил (ВВС) США. Боевые действия ВВС США во многих регионах будут иметь место в условиях неопределенной внутриполитической обстановке, разнообразном климате и рельефе местности. При этом в качестве противника им будут противостоять не регулярные войска, а

отдельные террористы и мелкие отряды боевиков, что серьезно ограничивает эффективность традиционного боевого применения военной авиации. По мнению экспертов, такая ситуация приведет к существенному пересмотру основных подходов к боевому применению ВВС. Потребуется пересмотр организации и проведения воздушных операций: значительно возрастет важность сбора развединформации, ее оперативная обработка, а также высокоточные удары авиационными средствами поражения.

Аналитики Пентагона полагают, что в новых условиях особую важность приобретет постоянный и непрерывный процесс сбора развединформации о террористических группах, широкое использование аэрофотосъемки и космического зондирования высокого разрешения наряду с быстрым и эффективным ее анализом. Это позволит обеспечить необходимый темп проведения антитеррористической операции, достичь и удерживать информационное превосходство над противником.

Военные эксперты отмечают, что потребность в постоянном наблюдении и высокоточных ударах по целям, расположенным в географически распределенных регионах, потребует поиска новых подходов и технологий по их реализации. В этом контексте значительная роль в предстоящих операциях в ходе антитеррористической кампании будет отведена беспилотным летательным аппаратам типа «Predator» и «Global Hawk» (первый уже использовался в боевых условиях в Косово, а второй прошел испытания в Афганистане). Также будет сосредоточено повышенное внимание и на создании все более и более сложных комплексов наведения для кинетического оружия, а так же других средств поражения, включая нелетальное оружие.

Как считают военные специалисты, война в Афганистане показала необходимость в модернизации существующего парка транспортной авиации и, прежде всего, самолетов-заправщиков. Все необходимые запасы в период афганской кампании поставлялись исключительно воздушным путем в течение первых шести месяцев с начала операции, что позволило существенно сократить расходы на создание необходимой транспортной инфраструктуры. Это стало возможным благодаря широкому внедрению новых подходов к боевому обеспечению, которые получили общий термин «эффективное боевое обеспечение». Необходимость в смене существовавших

подходов к боевому обеспечению вызвана существенным увеличением темпа проведения операций за прошедшие десятилетия. Использование системы промежуточных ремонтных баз, по мнению экспертов Пентагона, явилось ключевым моментом, позволившим достичь успеха и существенно расширить спектр действий по поддержке войск и повысить оперативность развертывания подразделений.

Все это, а также прогноз военно-политической обстановки, повлечет за собой проведение множества относительно маломасштабных, но весьма распределенных в пространстве (и периодически обостряющихся) операций. Это в свою очередь, предъявляет новые требования к возможностям ВВС.

Оперативная и эффективная работа любых вооруженных сил зависит от хорошо обученного персонала. Недостаток квалифицированных кадров ощущался в ВВС США еще до 11 сентября 2001 года, но в настоящее время этот вопрос стала серьезно влиять на возможности всего вида вооруженных сил. Как считают эксперты ряда аналитических компаний, с существующими кадровыми и материальными ресурсами, политикам, принимающим решения, придется выбирать: или принять большие риски при поддержании того же уровня внешне и внутриполитических усилия, или ограничить общее число или продолжительность проводимых операций, в которых американские вооруженные силы в ближайшее время будут участвовать. В этой связи эксперты RAND отмечают, что последняя позиция находится в противоречии с требованиями американской стратегии национальной безопасности, особенно в отношении долгосрочной антитеррористической кампании. Это ведет к тому, что запланированное сокращение численности ВВС в настоящее время представляется невозможным, по крайней мере, в ближайшей перспективе.

Военные действия не являются важнейшим средством в борьбе с терроризмом. От военных потребуются и другие подходы к разрешению стоящих задач. В этой связи многие эксперты полагают, что акцент на борьбе с терроризмом все же не повлечет масштабных изменений в существующей структуре ВВС США. Вместо этого существенно будут пересмотрены основные подходы к применению этого вида войск. Открытый и активный поиск новых понятий и подходов будет актуальным для ВВС США в ближайшей перспективе.

Кроме того, в последнее время рядом научно-исследовательских подразделений военно-воздушных сил США разработана новая стратегическая концепция противоборства.

Причина, побудившая американских военных разработать новую концепцию боевого применения вооруженных сил, позволяющую проводить практически молниеносные операции, по мнению самих разработчиков заключается в высоких темпах развития систем ПВО, а также возможность применения противником ОМП и ассиметричных средств поражения (информационные, экономические и др.), которые будут серьезно препятствовать или не позволят совсем провести США стратегическое развертывание своих вооруженных сил.

Основой новой концепции являются высокомобильные *стратегические ударные силы* (Global Strike Task Force). Их цель – молниеносным ударом подавить сопротивление противника и подготовить плацдарм для развертывания основных сил. Идеолог новой концепции генерал Джон Джампер – начальник штаба ВВС США.

Один из ключевых элементов новой концепции – это отход от традиционного понимания разведки как совокупности процессов сбора, анализа и реализации информации о противнике. В новой концепции разведка ориентируется на *прогноз действий противника* на поле боя. Появился даже термин «прогнозируемое восприятие боевого пространства».

Согласно положениям новой концепции, основной рабочий элемент органов управления – группа целеуказания в реальном времени (time-critical targeting cell) – оперативное подразделение, включающее представителей разведки, командования и аналитических подразделений. Задача группы – сопровождать одну или несколько целей с выдачей прогноза ее возможных действий в заданный интервал времени. Свои функции группа выполняет с использованием специального программного обеспечения анализа массивов данных (data mining), которое позволяет выявлять скрытые закономерности в поведении противника на основе анализа данных в базах, формируемых из информации средств разведки и наблюдения.

Классическим системам командования и управления в этом случае отводится роль перераспределения целей между средствами поражения, отслеживание точных координат цели и их передача на борт боевой техники.

Стратегические ударные силы предполагается формировать из самолетов дальнего радиолокационного наблюдения, выполняющих роль воздушных командных пунктов и осуществляющих взаимодействие с космическими системами наблюдения и связи, а также боевых платформ: F-22 как основного истребителя для завоевания господства в воздухе; бомбардировщиков B-2 и F-117 – для поражения целей противника. Для формирования единой системы связи и передачи данных предполагается широко использовать стратегические беспилотные летательные аппараты “Global Hawks”. Основная среда коммуникационного взаимодействия – традиционные средства связи ВВС системы Link-16. При этом мобильные группы сил специального назначения, действующие на территории противника, также будут включены в единую информационную систему, что позволит оперативно отображать ситуацию в боевом пространстве.

Современный уровень развития информационных технологий, особенно в части алгоритмов сжатия и обработки видео и аудио информации, позволяет существенно улучшить технические характеристики системы Link-16.

Рисунок 8 Массированная переброска по воздуху - основа проекции силы

Работы по концепции стратегических ударных сил проводятся в рамках общей программы модернизации вооруженных сил США в соответствии со стратегической концепцией «Единая перспектива -2020» («Joint Vision 2020»). Основные элементы нового подхода отрабатывались в ходе командно-штабных учений «Millennium Challenge 2002», которые прошли в США в июне-августе 2002 года.

Реализация концепции стратегических ударных сил позволит вооруженным силам США максимально использовать преимущества от информационного превосходства над противником, что даст возможность навязывать ему удобный для американских военных темп проведения

операций, тем самым управляя поведением противника и прогнозируя его ответные действия.

1.4.4. Трансформация сухопутных сил армии США

Афганская операция показала, что в ближайшее время продолжится трансформация сухопутных сил армии США, начатая в рамках стратегической концепции «Единая перспектива 2020» (Joint Vision 2020), в направлении усиления роли, так называемых, «легких» и «средних» подразделений, способных выполнять боевые задачи в условиях возросшего темпа проведения операций, обладающих высоким уровнем огневой мощи и возможностью к быстрому развертыванию как с зарубежных баз, так и непосредственно с территории США. Кроме указанных «легких» и «средних» подразделений сухопутных сил существенно возрастет и роль сил специальных операций.

По мнению американских военных экспертов, начатая более двух лет назад антитеррористическая кампания повлекла за собой значительные изменения в структуре и тактике действия американских сухопутных сил. Прежде всего, это связано со значительной неопределенностью масштабов предстоящих операций, регионов действий и темпа объявленной кампании. Несмотря на возникающие неопределенности, эксперты Пентагона склоняются к тому, что проведение долгосрочной глобальной кампании против терроризма повлечет за собой обширное использование американских наземных войск в широком диапазоне миссий. Они полагают, что в этой связи армия США столкнется с необходимостью еще более оперативного развертывания, размещения войск на еще большем числе долгосрочных зарубежных базах, а также обеспечения дополнительных возможностей в противодействии террору.

Мнение экспертов ряда аналитических центров армии США заключается в том, что для подготовки к будущему, армия уже сегодня должна подвергнуться существенной модернизации, как минимум по двум направлениям. Первое направление связано с резким возрастанием темпов проведения операций, а также в необходимости поддержки и проведения операции в многочисленных новых регионах базирования. Во-вторых, армия должна существенно скорректировать функции и задачи легковооруженных

частей и частей со средним вооружением (так называемые "легкие" и "средние" силы), чтобы повысить наступательную мощь в борьбе с терроризмом, увеличить темп проведения операций. Важно, что в ходе такой трансформации не должна быть утрачена способность армии США вести масштабные войны с применением тяжелой техники.

На сегодняшний день армия США уже достаточно долго находится в таких регионах, как Босния, Косово и др. По мнению экспертов Пентагона, они останутся там и в ближайшей перспективе. Особо подчеркивается, что события 11 сентября 2001 года показали необходимость присутствия американских войск в этих регионах в качестве сил стабилизации. Существенным добавлением к уже существующим местам базирования войск США станет создание новых военных баз в ходе антитеррористической кампании. Сегодня около 6 000 американских солдат уже находятся в Афганистане, и будут находиться там до полного устранения террористической угрозы, исходящей с территории Афганистана. Развертывание значительных по численности подразделений армии США возможно не только в Средней Азии, но также и в Юго-Западной Азии и Африке.

Поскольку Соединенные Штаты планируют проводить войну широким фронтом, планируется, что армия будет выполнять и другие типы операций (главным образом поддержание мира и принуждение к миру). В этой связи, по мнению военных экспертов США, стабилизация ситуации в главных энергетических регионах планеты (районы Персидского залива и Каспийского моря) потребует расширенных операций по поддержанию мира.

Всестороннее обучение иностранных вооруженных сил в контртеррористических операциях является сегодня и продолжит быть главным элементом американской военной политики в будущем. Поскольку террористические группы стремятся к созданию своих баз в нестабильных регионах и в «несостоявшихся государствах», американские усилия будут включать самый широкий спектр действий по борьбе с партизанами и обеспечение внутренней безопасности в подобных регионах. Прежде всего, к таким районам эксперты Пентагона относят Филиппины и Грузию.

Учитывая специфику борьбы с терроризмом, военные аналитики

Пентагона склоняются к необходимости трансформации существующих подходов к организации процесса управления и взаимодействия подразделений сухопутных сил. Так, некоторые классы целей будут требовать различных комбинаций наземных сил. Например, большой комплекс хорошо защищенных сооружений в трудном горном ландшафте, сопоставимый с крепостью Тора-Бора в Афганистане, может потребовать расширенной операции с привлечением тяжеловооруженных сил. Задача также может включать одновременный удар по множеству распределенных мест базирования террористов, значительно удаленных друг от друга географически. В ходе подготовки к подобным операциям у командования будет очень мало информации и времени на принятие решения. Это потребует от лиц, принимающих решения, иметь возможность атаки с высокой вероятностью успеха на цели, имеющие важное значение, но быстро меняющих свое положение и находящихся в самых различных регионах планеты. Способность захватить или нейтрализовать оружие массового поражения в этих условиях будет особенно важна.

Вместе с тем стремительное увеличение зон активных операций, проводимых американскими силами, влечет за собой стремительную потерю способности армии США к ведению полномасштабной войны с применением тяжелого вооружения. По мнению экспертов RAND, развертывание за пределами США больше чем четырех полноценных бригад существенно снизит способность армии США к ведению полномасштабной войны. Развертывание каждой дополнительной бригады будет стремительно уменьшать способность армии США к ответным действиям в случае полномасштабного вооруженного конфликта. Причины этого кроются главным образом в американской политике военного строительства мирного времени, которая ограничивает численность личного состава, который может быть размещен за пределами территории США. В этом случае, по мнению экспертов, необходимы исследования, результаты которых позволят определить варианты создания промежуточных баз ротации персонала или варианты использования за границей резервных бригад, а также определить необходимые изменяя политики военного строительства мирного времени, или же путем увеличения численности личного состава в боеготовых подразделениях.

Рост потребностей в персонале в ходе антитеррористической компании также усиливает нехватку наиболее востребованного персонала, обладающего специализированными навыками (спецназа, специалистов по связям с общественностью, разведчиков и переводчиков) в силу того, что развертывание на зарубежных базах входит в противоречие с мобилизационными планами подготовки к возможной полномасштабной войне. Считается, что армия должна будет снять эти вопросы, возможно, разворачивая курсы по переподготовке персонала, изменяя численный состав отдельных подразделений с тем, чтобы высвободить наиболее необходимых специалистов.

Кроме существенного увеличения численности персонала армии США, в ходе антитеррористической кампании потребуется развертывание новых зарубежных военных баз, что в свою очередь потребует развития системы тылового обеспечения.

Новые задачи потребуют изменения подходов к боевому применению сухопутных сил. Возможно, будут увеличена численность сил специальных операций с дополнительными возможностями в таких ключевых областях как специальная авиация. Планируется, что с этой целью в сухопутных войсках будет развернута переподготовка армейского спецназа и подразделений легкой пехоты с тем, чтобы уменьшить нагрузку на силы специальных операций.

С целью обеспечить возможность быстрого уничтожения хорошо защищенных районов хранения оружия массового поражения, в структуре сухопутных сил планируется создание ударных бригад. Ударные бригады - обладающие высокой огневой мощью мобильные подразделения сухопутных сил. Они могут использоваться для создания оперативного соединения, которое будет включать силы специальных операций, армейский спецназ, фронтовую авиацию и моторизованную пехоту, использующую легкую колесную технику вместо тяжелых танков. Такое соединение может обеспечить необходимое соединение боевой мощи и способность к быстрому развертыванию как с зарубежных баз, так и непосредственно с территории Соединенных Штатов. При этом превосходство подобных соединений над традиционными будет обеспечиваться широким применением последних достижений в области информационных технологий, что позволит

командиру ударной бригады достигать и удерживать информационное превосходство над противником.

Таким образом, перед руководством армии США сегодня стоит серьезная проблема: необходимо трансформировать сухопутные силы с целью обеспечения эффективной борьбы с терроризмом, а также одновременно сохранить необходимый потенциал для отражения возможной агрессии в случае развязывания полномасштабного военного конфликта. Балансирование этих усилий и связанных с ними рисков будет центральной особенностью армейского принятия решения на несколько лет вперед.

1.5. Основные элементы модели нового миропорядка – американского глобализма

Активизация действий по переустройству мира потребовала от администрации США определить ключевые подходы к построению модели нового миропорядка. Об этом в частности свидетельствует ряд заявлений, сделанных высокопоставленными чиновниками администрации США.

Среди прочих заявлений можно отметить, например, сделанное заместителем Госсекретаря по политическим вопросам Марком Гроссманом перед участниками состоявшегося 21 марта 2002 года заседания Национальной ассоциации редакторов газет на тему «Прогноз глобальных тенденций на ближайшее десятилетие и выработка внешней политики США». На пресс-конференции им был сделан ряд заявлений по ключевым элементам, которые определяют состояние и перспективы становления нового мирового порядка. Всего было определено семь главных тем.

Первой и важнейшей темой, стержнем, вокруг которого строится новая система мироустройства, является объявленная США компания по борьбе с международным терроризмом. По словам президента США «каждая страна должна знать, что война с террором для Америки является не просто политикой, а настоящим обетом».

Объявленная война с международным терроризмом является важнейшим стимулом, позволяющим вплотную подойти к трансформации

вооруженных сил и всей системы обеспечения национальной безопасности США, которая бы позволила противодействовать новым угрозам.

В последнее время американские военные эксперты постоянно подчеркивают, что Америке приходится вести войну нового типа, принципиально отличную от всех войн прошлого. Как заявил заместитель министра обороны США Пол Вулфовиц: «Это - уникальная война. Она уникальна тем, что мы продолжаем вести боевые действия за рубежом, в то время как у нас дома сохраняется угроза нападения... Она уникальна тем, что она носит гораздо более изощренный и сложный характер, чем война в привычном для нас понимании этого слова. Ее уникальность состоит в том, насколько быстро она приняла такие масштабы... Она уникальна и тем, что эту войну приходится вести не только военными, но и многими другими средствами». Уже в октябре 2001 года Министр обороны США Д. Рамсфелд подчеркивал, что «мы наблюдаем появление нового поля боя... конфликтов иного типа».

По мнению специалистов, новый взгляд на угрозы XXI века заключается в том, что в будущем основная угроза будет исходить не от регулярных армий, поскольку США нет достойного противника, а от всевозможных террористических, криминальных и др. организаций, в том числе негосударственных, участники которых объединены в некие сетевые структуры. Подобные организации не имеют четкой иерархической структуры подчиненности, зачастую не имеют единого руководства, координируют свою деятельность с использованием средств глобальных коммуникаций. Отличительной особенностью таких структур является наличие единой стратегической цели и отсутствие четкого планирования на тактическом уровне. Примером такой организации является «Аль-Каида». Для достижения победы в противостоянии с таким врагом эксперты рекомендуют вести «сетевую войну».

В сетевой войне, о которой в прессе начали говорить еще в 1993 году, победа в меньшей степени зависит от силы оружия, чем от информации и связи, а эти компоненты «выгодно отличают сетевые организации от их иерархических аналогов», каковыми являются традиционные армии. Аналитики в этой связи утверждают, что выигрывает тот, у кого «лучше история, а не тот, кто обладает бомбой самого большого размера».

Как отмечают эксперты, приблизительно 90% усилий, прикладываемых США для разрешения конфликтов, ориентированы на военные операции с участием государств. По мнению экспертов RAND, такая политика понятна в той мере, насколько «хорошо мы знаем, как себя вести в отношении тех или иных государств-наций, но этого нельзя сказать о сетевых организациях». По их мнению, была сделана серьезная ошибка: разгромив талибов, находившихся во главе государства, США дали возможность большей части «Аль-Каиды» уйти в подполье и продолжить свое существование в виде невидимой террористической сети.

Рисунок 9 Самолеты ВВС США на авиабазе в одном из государств Центральной Азии

Как показывает практика, сегодня США не волнует тот факт, что у России есть тысячи ядерных боеголовок, так как они всегда могут нанести ответный удар, но они не могут применять ядерные ракеты против негосударственной организации, ячейки и связи которой разбросаны по всему миру, в том числе и в самих США. Невозможность принятия ответных мер делает невозможным и факт разубеждения применять оружие такого вида, это ведет к трансформации понятия «стратегического сдерживания».

О том, что концепция сетевой войны находит все более широкое применение в действиях вооруженных сил США говорит и то, что в настоящее время США разрабатывают новую «триединую стратегию обороны», которая должна стать «краеугольным камнем» оборонительной стратегии США в 21-м веке и которая включает широкий спектр как ядерных, так и неядерных, наступательных и оборонительных средств. Причем последним отдается даже большее предпочтение.

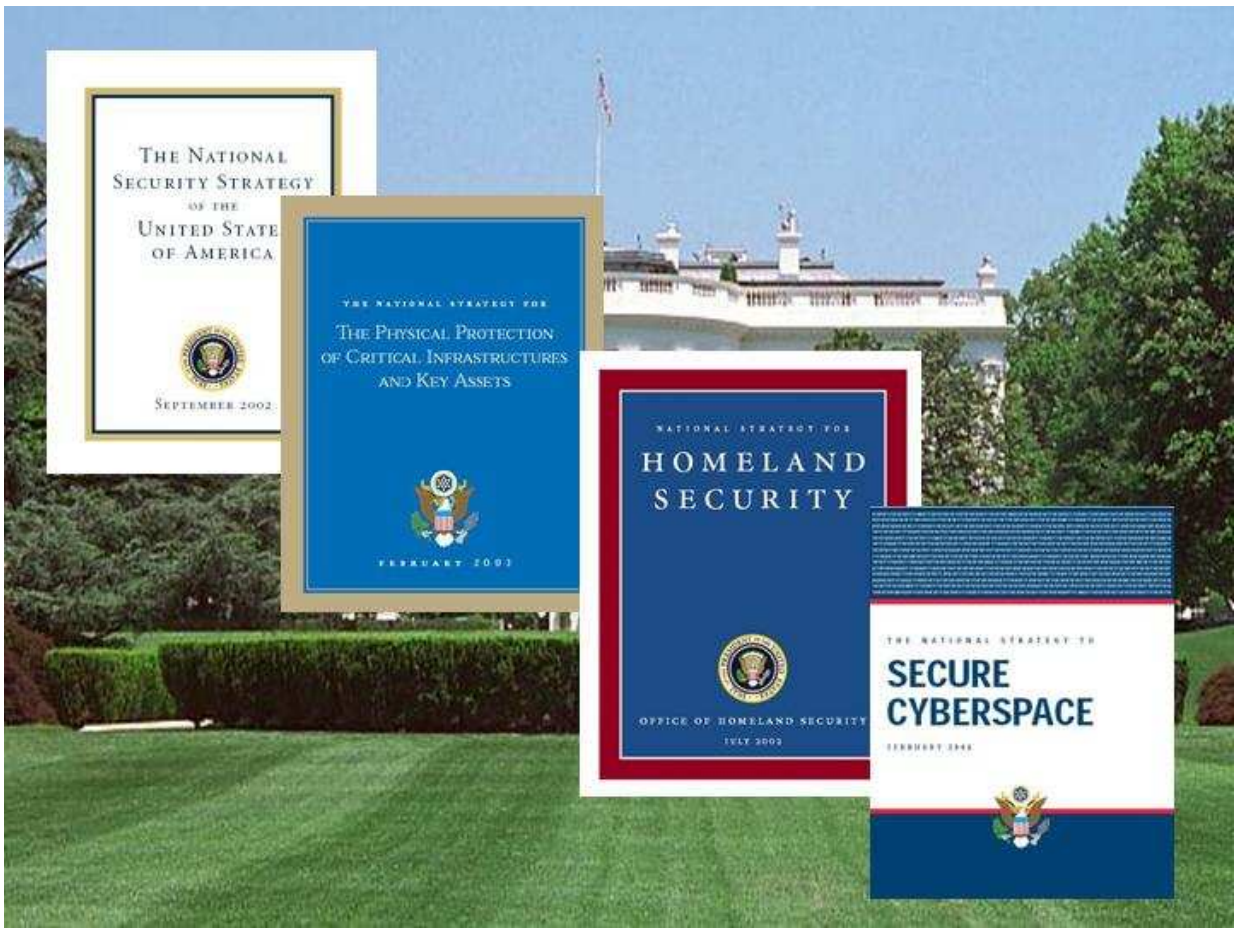

Рисунок 10 Четыре национальных стратегии США, принятых в 2002-2003 годах – «Стратегия Национальной безопасности», «Национальная стратегия защиты критической инфраструктуры», «Стратегия внутренней безопасности», «Национальная стратегия защиты киберпространства» - определивших развитие ситуации в мире в начале XXI века

Такой подход обусловлен тем, что, по мнению заместителя министра обороны США по вопросам стратегии Дугласа Фейта, в будущем сдерживание в его традиционном понимании будет функционировать менее предсказуемым образом и США потребуются значительные ресурсы для защиты своей территории и союзников от нападений, которые невозможно предотвратить.

Руководство военного ведомства США сегодня пересматривает подходы ко многим научно-техническим проектам по созданию новейших образцов военной техники. Многие из проектов, которые не удовлетворяют концепции сетевой войны, закрываются.

Избранная позиция борца с «мировым злом» позволяет администрации США широко привлекать невоенные методы управления военно-политической обстановкой в мире с тем, чтобы направить ее развитие в выгодном для США направлении. В складывающихся условиях на первое место среди потенциальных противников США в ближайшие десятилетия все яснее продвигается Китай.

В докладе, сделанном командующим Тихоокеанским командованием США адмиралом Д. Блером в феврале 2002 года, вновь подчеркивается, что «сохраняется угроза применения силы со стороны Китая» в отношении Тайваня – главного союзника США в тихоокеанском регионе. Пекинский режим, по словам адмирала, «устанавливает ракеты на боевые позиции и проводит модернизацию своих вооруженных сил, не скрывая, что это делается для устрашения Тайваня».

В условиях изменения геополитической обстановки для США крайне важно как можно быстрее занять наиболее выгодные позиции для возможного противостояния с КНР. В настоящее время это достигается под прикрытием антитеррористической операции. Продвигаясь в избранном направлении, США уже направили воинский контингент на Филиппины для подготовки подразделений филиппинских вооруженных сил якобы к борьбе с террористической группой «Абу-Саяф». США также направляют военных инструкторов в Йемен и Грузию для подготовки подразделений местных вооруженных сил.

Важнейшим элементом завоевания превосходства в возможном противостоянии с китайской диаспорой заключается в установлении тотального контроля за перемещением денежных средств в мировой экономике. В предложенной США резолюции ООН № 1373 содержатся требования о том, чтобы все страны блокировали источники финансирования террористов. При этом особо подчеркивается, что свои действия им необходимо координировать с США.

Согласно этой резолюции 142 государства мира (в том числе и Россия) издали указы и распоряжения о замораживании активов лиц и организаций, подозреваемых в терроризме на основании списка, представленного администрацией США. Всего блокированы денежные средства в объеме

104,8 млн. долларов - 34,2 млн. долларов в США и 70,6 млн. долларов в других странах.

Второй темой, определяющей состояние и перспективы современного мира, является глобализация.

В этой связи рядом экспертов подчеркивается, что глобализация всегда имела оборотную сторону. Международный терроризм - это не единственный вызов, который бросает глобализация. Провал аргентинской экономики, самоизоляция ряда стран таких, как Северная Корея, а также увеличение разрыва между странами в использовании современных цифровых технологий - все это говорит о том, что необходимо настойчивее заниматься задачами интеграции мира в современную экономическую и политическую систему.

Важность глобализации напрямую связана с объявленной войной с терроризмом. Так эксперты RAND предлагают уделять больше внимания «…осуществлению невоенных стратегий в направлении негосударственных агентов…» и в частности, международных общественных организаций. «Неправительственные организации занимают исключительную позицию для того, чтобы с уважением относится к обеим сторонам и действовать в качестве посредника». Первый урок сетевой войны свидетельствует о том, что для борьбы с сетью необходимо объединиться в сеть. Экспертами особо подчеркивается, что «…необходимо осознать, что пока мы будем прибегать к применению силы, не делая никаких различий, нам сложнее будет создать сети сотрудничества. А создание подобных сетей является стратегической целью текущей войны…».

По словам представителей администрации США глобализация нужна и полезна, прежде всего, Соединенным Штатам. По их мнению, необходимо сделать так, чтобы страны поняли те выгоды, которые глобализация несет с собой им и их гражданам, и отказались от политики, которая противоречит принципам глобализации.

Третья тема - это демократизация. Формирование гражданского общества на принципах демократии – ключевой фактор успеха в развернутой администрацией США кампании по утверждению мирового лидерства. Именно гражданское общество как система взаимосвязанных

государственных и негосударственных объединений, партий и движений позволяет заложить основу создания сетевых структур, так необходимых для продвижения принципов сетевого управления.

Отсутствие должного контроля над рядом регионов мира, заставляет США и дальше вести борьбу за демократию в таких районах, как Китай, Балканы, Центральная Азия и Африка с целью навязывания сетевой структуры гражданского общества.

Демократия, свобода личности и победа в войне с терроризмом представляют собой, по мнению высокопоставленных американских чиновников, взаимосвязанные понятия.

Четвертая тема - это альянсы. В последнее время, в связи с изменениями геостратегической и геополитической ситуации, для США остро встал вопрос о необходимости пересмотра подхода к формированию альянсов. Подчеркивается, что в новых условиях наблюдается недостаточная союзническая связность стран тихоокеанского региона, Южной и Юго-Восточной Азии. Именно поэтому сегодня США стремятся укрепить союзы с Филиппинами, Японией, Таиландом, странами Центральной Азии.

Между тем Европа формирует свою собственную идентичность в противовес лидерству США. Разговоры об односторонних действиях США в Афганистане ведутся, по мнению американских экспертов, для того, чтобы создать необходимый для Европы политический фон.

Так, на саммите в Праге решался вопрос не только о вступлении в НАТО Латвии, Литвы и Эстонии, а также Словении и Словакии, но и Румынии и Болгарии. До последнего времени в альянсе считали последние две страны по причинам коррупции, нищеты и медлительности в реформировании вооруженных сил не готовыми для вступления в Альянс. Однако «…после событий 11 сентября Черное море приобрело существенное значение в качестве естественного трамплина…», разъяснял румынский министр иностранных дел Мирча Джоанэ возросшее значение этого региона для НАТО. Он не пояснил, зачем может понадобиться этот трамплин…

Однако ясно, что Черное море граничит как с балканскими странами, так и Россией, с богатыми сырьевыми ресурсами государствами Средней Азии с характерной для них неспокойной внутриполитической ситуацией и с

Турцией. Во время недавнего визита в Румынию главнокомандующий объединенными вооруженными силами НАТО в Европе американский генерал Джозеф Ралстон сказал, что для скорейшего вступления Румынии и Болгарии в альянс существуют «весомые политические причины».

В условиях трансформации всей системы международных военных и экономических союзов встает вопрос о целесообразности присутствия России в НАТО. Складывается впечатление, что сегодня уже созрело решение о кардинальной трансформации НАТО по тем принципам, которые вырабатываются в ходе организации антитеррористической коалиции. Практика показала, что подход «кто не с нами, тот против нас» гораздо эффективнее, чем задействование Статьи V Вашингтонского договора. Россию принимают в НАТО только для того, чтобы потом блок реформировать не на принципах консенсусного принятия решений, а на вассальном принципе.

Пятую тему можно сформулировать как «новые партнеры и союзники». В результате создания коалиции против терроризма Соединенные Штаты получили возможность не только укреплять уже существующие, но и формировать новые взаимоотношения.

Верный союзник США в Азиатском регионе - Пакистан - оказался не вполне надежным в ходе операции в Афганистане. Это заставляет Вашингтон искать новых стратегических союзников в регионе. Выбор Администрации останавливается на Индии.

Индия - страна, с которой США взаимодействуют в рамках новых динамичных отношений. О новом качестве отношений Индии и США говорит начало совместных работ по обеспечению безопасности критически важной информационной инфраструктуры обоих государств от кибератак. «Нет никаких причин, почему Индия не должна быть осведомлена о вирусе или атаке, обнаруженных нами в США, если у нас есть возможность быстро и незамедлительно проинформировать наших коллег в Индии и выслать различные "заплаты" и программные решения для защиты информационной инфраструктуры Индии. И наоборот, когда Индия обнаруживает что-то и может своевременно сообщить нам об этом», - заявил 30 апреля 2002 года в Дели помощник Государственного секретаря США по политико-военным

вопросам Линкольн Блумфилд. По его словам, он провел широкие политические и военные переговоры с индийскими официальными лицами, «…чтобы создать условия для более тесных и еще более продуктивных двусторонних отношений в области безопасности…».

По словам Блумфилда, одной из тем проведенных им обсуждений была модернизация вооруженных сил Индии и возможность поставок военной техники из США.

Наряду с этим США ищет союзников и на Американских континентах. Это, прежде всего, Чили, Колумбия и, возможно, Венесуэла.

Шестая тема - это оружие массового уничтожения. События 11 сентября доказали, что необходимость добиваться ликвидации оружия массового уничтожения - химического, биологического и ядерного, - которое представляет собой угрозу Соединенным Штатам и их союзникам является сегодня насущной необходимостью.

По мнению экспертов RAND, сегодня «Аль-Каида» может выиграть войну, если получит в свое распоряжение ядерное и бактериологическое оружие.

Большинство организаций, занимающихся информационно-аналитической работой, прогнозирует, что в период до 2015 года Соединенным Штатам, по всей вероятности, придется иметь дело с угрозами применения МБР со стороны Северной Кореи, Китая, Ирана и, возможно, Ирака.

Седьмая тема - это свободные рынки и торговля.

Как отмечает администрация США, страны, придерживающиеся трех основных принципов - добросовестного управления, инвестиций в человеческие ресурсы и экономической свободы - имеют наилучшие шансы на то, чтобы выбраться из бедности. Как сказал представитель США на торговых переговорах Роберт Зеллик, «будущее принадлежит тем странам, которые для участия в процессах, идущих в современном, децентрализованном, сетевом мире, готовы открывать свои рынки, снижать налоги и укреплять свою валюту. Наше будущее принадлежит нашему народу, поэтому наша цель должна состоять в создании национальных и международных правил, позволяющих людям полностью реализовать свой

потенциал». При этом особо подчеркивается, что Соединенные Штаты и дальше будут сохранять за собой роль мирового лидера в поддержке свободной торговли и свободных рынков.

В 2001 году США было заключено соглашение о свободной торговле с Иорданией и двустороннее торговое соглашение с Вьетнамом. Завершен процесс вступления Китая и Тайваня в ВТО. Эти меры должны помочь Соединенным Штатам сформировать такую торговую систему, которая будет устойчивое развитие американской экономики.

На основе вышеизложенного можно сделать вывод о том, что США в настоящее время все активнее внедряют в практику проведения внешней и внутренней политики методологию управляемого хаоса. Роль средств управления хаосом отводится «гражданскому обществу». С целью его формирования осуществляется повсеместная организация всевозможных сетевых структур. Ключевыми факторами достижения успеха здесь являются процессы глобализации, связанные с ними вопросы построения новых альянсов и союзов, а также сетевизация мировой экономики через открытые рынки.

Наряду с продвижением выгодной США модели миропорядка продолжается демонтаж структур послевоенной системы мироустройства. Предпринимается комплекс мер для скорейшего сокращения оружия массового поражения, которое представляет серьезную опасность для США.

Все действия по формированию нового мирового порядка сегодня проводятся под прикрытием кампании борьбы с международным терроризмом.

1.6. Угрозы и вызовы информационной революции

В условиях, когда человек сталкивается с вызовами и угрозами принципиально новой для него природы, к которым он еще не успел адаптироваться и выработать контрмеры, особую актуальность приобретает деятельность по обеспечению безопасности человека – безопасности в широком смысле, охватывающей все сферы жизни и деятельности человека.

Именно с неопределенностью встающих угроз связан сегодня настоящий психоз, охвативший большинство развитых стран.

Еще вчера человек мог использовать столетия исторического опыта по выработке необходимых мер в случае возникновения той или иной угрозы: в конце XX века достаточно хорошо работали традиционные инструменты мировой политики, позволявшие разрешать, опять же, достаточно традиционные формы конфликтов, что обеспечивало военную безопасность общества; классическая экономика давала возможность использовать такие методы управления, которые позволяли избегать фатальных экономических кризисов, это в свою очередь делало безопасной экономическую сферу; четкие правила взаимодействия в условиях капиталистической или социалистической модели, в условиях устоявшихся границ сфер влияния обеспечивали достаточно низкий уровень преступности и криминализации общества в целом – личной безопасности человека мало что угрожало.

Сегодня накопленный опыт практически бесполезен: еще вчера специалисты, рассчитывая устойчивость защитного бункера, принимали вероятность падения на него магистрального авиалайнера за крайне маловероятное событие, но теракты в США 11 сентября 2001 года все изменили.

Столь значительные, а главное стремительные изменения привели к тому, что желание удержать глобальное лидерство вынуждает сегодня руководство ряда развитых стран пересматривать роль и место своих государств в новом мире, изменять фундаментальные подходы к проведению внешней и внутренней политики.

С ноября 1999 года в рамках инициативы «Информационная революция» программы стратегических оценок Национального совета по разведке США корпорацией РЭНД был проведен ряд международных научных конференций и семинаров, в ходе которых изучалось и оценивалось мнение ведущих экспертов по проблеме трансформации общества под воздействием информационной революции.

Результаты проделанной работы были обобщены экспертами РЭНД в отчете «Глобальный курс информационной революции: общие вопросы и региональные различия» («The global course of the information revolution:

recurring themes and regional variations», MR-1680-NIC), опубликованном летом 2003 года.

Исследование РЭНД является заключительным этапом в многолетней программе работ, направленной на изучение феномена глобализации и информационной революции, движущих сил развития современного общества, анализ конфликтного потенциала и выявление потенциальных угроз национальной безопасности США в ближайшие 10-20 лет.

Основная цель проведенного исследования – выявить характер воздействия информационных технологий и информационной революции на экономическую, финансовую, политическую, культурную, социальную и иные сферы жизнедеятельности современного общества, а также дать прогноз развития ситуации на ближайшие 10-20 лет.

В исследовании отмечается, что сегодня прогресс в информационных технологиях уже затронул большинство сфер бизнеса, государственной и общественной деятельности практических во всех регионах мира. Информационные технологии и связанная с ними информационная революция, превратились в один из наиболее значимых факторов, способствующих динамичной трансформации общества, его переходу от общества постиндустриального к обществу информационному. Стремясь наиболее полно использовать преимущества, которые несет с собой информационная революция, американские аналитики пытаются прогнозировать развитие информационных технологий как на краткосрочную, так и среднесрочную перспективу.

Результаты анализа позволили выявить ряд характерных особенностей развития информационных технологий и влияния информационной революции, причем ряд особенностей характерен большинству регионов мира, а некоторые из них специфичны для отдельных регионов планеты.

Так, среди особенностей, характерных большинству регионов мира, стремящихся использовать достижения информационной революции, эксперты РЭНД отмечают следующее.

1. В ближайшие 10-20 лет разработки новых технологий будут непрерывно стимулировать информационную революцию.

Среди наиболее значимых событий в области информационных технологий, которые в наибольшей степени окажут влияние на развитие ситуации в развитых странах мира в ближайшие десятилетия, эксперты РЭНД выделяют следующие:

• глубокая интеграция данных, голоса и видео как в глобальных, так и в национальных сетях;

• универсальная возможность соединения любых устройств для создания локальных сетей; широкое развитие домашних сетей, объединяющих бытовую электронику;

• конвергенция различных приложений на базе Интернет-протокола;

• широкое распространение широкополосных радиоканалов;

• пропускная способность оптических линий связи достигнет нескольких тысяч гигабит в секунду;

• существенное увеличение плотности хранения данных;

• увеличение интеграции и совместного использования кремниевых микросхем, био- и нанотехнологий с возможным применением и квантовых вычислений.

Разработка товаров и услуг на основе подобных технологий позволит информационным устройствам быть вездесущими, высокоэффективными, находиться в непрерывном контакте друг с другом. Подобные устройства обеспечат значительное взаимопроникновение физического мира и киберпространства, позволяя информационным системам всесторонне реагировать на изменения в окружающей их среде и наоборот.

Развитие информационных услуг существенно расширит доступ к информационным системам. Активно будут развиваться информационные услуги, играющие важную роль в здравоохранении (прежде всего в телемедицине), дистанционном образовании, а также специализированные системы приема платежей за подобные электронные услуги. Развитие технологии гипертекста даст возможность пользователю самому формировать свою виртуальную среду.

Наряду с развитием технологий, способствующих росту бизнеса, активно будут развиваться и технологии развлечения. Среди продуктов и

услуг информационной индустрии развлечений большая роль будет отведена следующим разработкам:

• компьютерные игры, одновременно вовлекающие многие тысячи людей, взаимодействующих в реальном времени с себе подобными;

• компьютерные игры, имеющие специальные датчики и приборы для взаимодействия с реальным физическим миром и создания высоко-реалистичной виртуальной реальности;

• массовое распространение интерент-видеокамер обеспечит не только улучшенное коммуникационное взаимодействие, но и станет одной из серьезных проблем сохранения конфиденциальности;

• активное взаимодействие людей различных культур, как результат внедрения систем машинного перевода;

• возможность просмотра спортивных событий и других зрелищных мероприятий с любой, удобной для зрителя точки;

• видео очки, размещающие изображение непосредственно перед глазами зрителя, создавая эффект присутствия;

• виртуальный киберсекс;

• музыка и кино по требованию в любое время;

• электронные книги.

Эксперты отмечают, что сегодня намного легче предсказать прогресс технологий, чем идентифицировать определенные продукты на основе таких технологий или услуги, которые появятся и будут широко распространены. Хотя прогресс технологий делает многое возможным, однако только рынок решит, какие изделия и услуги станут реальными и широко распространенными через 10-20 лет.

Однако уже сегодня можно определить ряд важных рыночных критериев, которые будут определять широкое распространение того или иного продукта или услуги:

• простота использования;

• обратная совместимость с предыдущими версиями;

• реальное ощущение преимущества от использования;

• низкая стоимость владения;

• доступность;

• некритичные отказы в работе изделия;

• состояние экономики (определяющее доступный доход потребителей);

• важность и критичность принятия нового продукта по сравнению с жизнеспособными альтернативами;

• зависимость от рыночного проникновения и успеха деловой модели производителя;

• зависимость от критической массы пользователей, что определяет взрывное распространение продуктов или услуг.

Эксперты отмечают, что бурное развитие информационных технологий и различия в восприятии плодов информационной революции в различных регионах мира в ближайшие десятилетия могут привести к обострению межгосударственных отношений. Так, по их мнению, важно помнить, что высокотехнологичные продукты на базе информационных технологий можно рассматривать либо как частный товар, который поставляется на рынок, либо как общественный товар. Так США имеют тенденцию рассматривать большинство подобных товаров как частные. Другие нации (например, Индия) рассматривают подобные продукты не только как частный, но также и как общественный продукт. Эти отличающиеся подходы и могут вести к напряженным отношениям между странами или регионами относительно интеллектуальных прав собственности, которые могут замедлить темпы глобализации в ближайшие десятилетия.

В процессе глобализации, появление «приложений убийц» серьезно затронет существующие и создаст новые рынки. Под «приложениями убийцами» эксперты РЭНД понимают такие товары или услуги, которые формируют новые рынки сбыта и способствуют перемещению в них капитала из рынков традиционных, что в свою очередь ведет к разрушению последних, уходу с них устаревших продуктов и компаний, их производивших.

Напряженные отношения, являющиеся результатом подобного развития событий, затронут в рассматриваемый период рост и распространение

продуктов и услуг, основанных на следующих информационных технологиях:

• развитие оптической технологии коммуникаций и IP-телефонии окажет серьезное негативное воздействие на отрасли телесвязи во всем мире, что приведет к масштабным структурным перестройкам на рынке услуг связи;

• противостояние программного обеспечения с открытыми кодами (прежде всего на базе операционной системы Linux) против коммерческого программного обеспечения с закрытыми кодами (на базе операционной системы MS Windows) во многом будет способствовать коренному переделу рынка программного обеспечения;

• интеллектуальная собственность и цифровые права на новые продукты и услуги создадут основные напряженности в отношениях между нациями.

2. В ближайшие 10-20 лет информационная революция породит новые бизнес-модели, которые существенно трансформируют деловой и финансовый мир.

Развитие информационных технологий способствует возникновению целого ряда новых бизнесс-моделей как для внутреннего использования в корпорациях, так и для их внешних коммуникаций с клиентами, поставщиками и конкурентами. Многие из таких моделей бизнеса основываются на той или иной форме электронной торговли, что в ближайшем будущем приведет к повышению важности последней как главной формы экономической деятельности.

Большая часть новой деловой активности сегодня сконцентрирована в географических «кластерах»: Северная Америка, Европа и отдельные части Азиатско-Тихоокеанского региона. Подобное деление сохраниться и в ближайшие 15-20 лет.

Эксперты отмечают, что наравне с «приложениями убийцами» «творческое разрушение» будет являться общей особенностью подобных деловых и финансовых преобразований с новыми, более эффективными продуктами и услугами, заменяющими старые и менее эффективные. Такой процесс будет часто сопровождаться экономическим крахом компаний, порожденных предыдущей эпохой и производящих устаревшие изделия и услуги.

Вместе с тем «информационная работа» и «информационные рабочие» становятся постоянно увеличивающейся долей экономического потенциала и рабочей силы во многих странах мира, поскольку их деловые и финансовые миры подвергаются преобразованиям под воздействием информационной революции. Через какое-то время эти новшества сформируют новые виды коммерческой деятельности в «отраслях промышленности знаний», что повлечет перемещение капитала в новые области, больше подходящие для информационной работы, чем для промышленного производства, а это в свою очередь затронет места проживания людей и вызовет новую масштабную волну миграции населения Земли.

Столь существенное повышение роли информационной работы затронет образование, требующееся людям, как при их приеме на работу, так и в процессе их карьерного роста. Через какое-то время, подобные тенденции окажут существенное воздействие на образовательные процессы во всем мире.

Преобразования, порожденные информационными технологиями, несут существенные изменения в деловой и финансовый мир. Эксперты отмечают, что для обозримого будущего бесконечный ряд новых событий в области информационных технологий будет непрерывно вести революцию в деловом и финансовом мире как по уже известным, так и по новым путям. Сами эти преобразования, в свою очередь, существенно изменят «поле игры» для правительств и общества в целом.

3. В ближайшие 10-20 лет информационная революция существенно затронет механизмы управления обществом и создает новых политических игроков.

Одним из важных выводов, который делается экспертами РЭНД, состоит в том, что некоторые традиционные механизмы управления обществом (такие как налогообложение и лицензирование) становятся все менее эффективными и более проблематичными, поскольку информационная революция позволяет действовать игрокам рынка вне досягаемости национальных правительств. Как в указанных, так и в ряде других областей правительствам, которые в наибольшей степени затронуты информационной революцией, уже сегодня необходимо найти новые механизмы или создать

новые универсальные международные структуры управления, чтобы сохранить контроль над своими государствами.

Важным элементом информационной революции является появление новых политических игроков. Новые политические игроки формируются информационной революцией в бизнесе, социальных и политических сферах, на внутринациональных, межнациональных и наднациональных уровнях, которые изменяют распределение политической власти.

В то же самое время, прогресс в информационных технологиях создает новые способы взаимодействия на основе интернет-технологий: между гражданами и их избранными представителями, между кандидатами и избирателями и среди самих граждан при обсуждении политических проблем.

Некоторые эксперты в этой ситуации предполагают, что роль этнического государства может существенно измениться в результате целого ряда подобных событий. Однако другие полагают, что тенденции в этом отношении не ясны, указывая ряд существенных функций, которые этническое государство продолжит играть в эпоху информационной революции. Учитывая значительное различие взглядов на эту проблему, эксперты РЭНД заключают, что будущая роль этнического государства в информационную эпоху до конца неясна. Считается, что различные нации изберут различные подходы. Так малые нации с большей готовностью расстанутся с рядом функций этнического государства, в то время как крупные нации будут стараться полнее сохранить традиционную роль этнического государства. Однако общим выводом является то, что протекающие процессы приведут к коренным изменениям в политической сфере государственного управления, что в свою очередь отразиться и на вопросах определения национальных приоритетов, целей и ценностей.

4. В ближайшие 10-20 лет информационная революция останется многоликой и будет формироваться социальными и культурными ценностями.

Как отмечают эксперты РЭНД, информационная революция инициирована технологиями, но направляется, прежде всего, нетехническими факторами, включая социальные и культурные. Социальные

и культурные изменения должны будут иметь место, если отдельные граждане, корпорации и нации станут полнее использовать возможности информационных технологий. В ходе подобных процессов возможно обострение международных отношений, связанное с культурными и социальными различиями наций. Прежде всего, такие конфликты активизируются на границах «цивилизованного» мира и «бурлящей пропасти» беднейших стран.

Цифровое различие внутри и между нациями сохранится. В пределах стран, распространение информационных технологий вообще усилит различия и укрепит социальные расколы, по крайней мере, пока не будет достигнуто технологическое насыщение. Кроме того, поляризация между богатыми и бедными станет более острой в силу ее отчетливой видимости в информационном обществе.

Способность приобретать и использовать новое знание будет критичной для успеха в информационном обществе, поскольку синтез новых знаний составляет растущую пропорцию всей трудовой деятельности в долгосрочной перспективе. Соответственно, развитие человеческого капитала в ближайшие годы будет являться ключевым. «Качественное образование для всех» будет одним из ключей к национальному успеху в информационную эпоху.

Подобные процессы повлекут проявление различных вызовов в различных частях мира. Глобализация, ускоренная информационной революцией, продолжит оказывать многоаспектные социальные и культурные эффекты.

Ряд экспертов отмечает, что в то время как экономические эффекты глобализации сегодня уже достаточно изучены, ее социальные последствия до конца не ясны. Эта же группа экспертов прогнозирует углубление разрыва между политическими, интеллектуальными, экономическими элитами и остальной частью населения, прежде всего в развивающихся странах.

5. В ближайшие 10-20 лет сохранится многофакторная форма и характеристика национального подхода к восприятию информационной революции.

Среди важных факторов, характеризующих восприятие нацией

информационной революции, и как следствие - росту напряженности внутри нее, эксперты РЭНД выделяют следующие:

• богатые нации лучше приспособлены для использования продуктов информационной революции, чем бедные;

• отношение разных слоев общества к происходящим изменениям различно;

• роль и место правительства и законов может изменяться в информационную эпоху;

• структура рынков капитала.

Эксперты РЭНД оценивают возможности по интеграции в глобализирующийся мир и восприятию изменений, привнесенных информационной революцией, той или иной нацией по следующим показателям:

• степень и характер проникновения информационных технологий в общество;

• занятость в отраслях обработки информации и синтеза знаний, развитие электронной коммерции;

• уровень развития бизнеса в области информационных технологий;

• потенциал «творческого разрушения» накопленный нацией;

• присутствие новых политических игроков и изменения в управлении в политической сфере;

• перемещение талантливых, высококвалифицированных работников интеллектуального труда.

В рамках изложенной выше модели ближайшего будущего эксперты РЭНД прогнозируют следующее основные тенденции развития геополитической обстановки в мире.

1. В ближайшие 10-20 лет США останутся в авангарде информационной революции.

По мнению экспертов, североамериканская (США и Канада) экономика и общество сегодня достаточно хорошо подготовлены, чтобы встретить вызовы информационной революции. Они имеют ряд преимуществ, включая

хорошо развитые инфраструктуры и человеческий капитал, экономику и само общество, которые легко адаптируются к различным изменениям, а также правовое поле с хорошей защитой интеллектуальных прав собственности. Обе - нации иммигрантов, которые привлекают энергичных, талантливых, подготовленных людей со всех континентов.

Северная Америка использует эти преимущества, чтобы держаться в авангарде информационной революции. Крушение информационных компаний в конце XX века, безусловно, замедлило темпы информационной революции в регионе, но только временно. Северная Америка будет активно развиваться и внедрять достижения информационной революции.

2. В ближайшие 10-20 лет информационная революция в Европе будет развиваться медленнее и несколько иным путем, отличным от ее развития в США и Канаде.

В то время как факторы развития информационной революции остаются теми же, что и в США, существует и ряд принципиальных отличий:

• европейцы и американцы по-разному относятся к возможным экономическим и социальным изменениям, последние проще адаптируются;

• европейцам свойственна большая экономическая и социальная активность;

• европейское желание интеграции наций в единой Европе;

• более открытый рынок США и более регламентированный правительством рынок Европы;

• больший европейский акцент на нисходящем планировании правительственными и деловыми элитами.

В области технологий европейское представление об информационной революции подобно американскому, но больше акцентировано на беспроводные технологии.

В результате этого отличного климата в Европе информационная революция будет развиваться несколько иным курсом, с большим неприятием риска европейцами, заставляющим творческий процесс разрушения идти медленнее.

3. В ближайшие 10-20 лет ряд стран Азиатско-Тихоокеанского региона продолжат стремительное развитие и масштабное использование информационных технологий.

В последние годы наблюдается активное развитие государств Азиатско-Тихоокеанского региона, их стремительное вовлечение в глобализирующийся мир. Граждане ряда стран региона составляют основную часть пользователей Интернета. Уровень интернетизации в Южной Корее, Гонконге, Японии и Австралии превышает уровень пользователей в США 2000 года. Близко от указанных стран по числу пользователей Интернет следуют Сингапур, Тайвань и Новая Зеландия. В отличие от ситуации в Соединенных Штатах, где основную часть пользователей составляют частные лица, большинство пользователей Интернет в Азии - это сотрудники высокотехнологичных компаний. Япония, Сингапур, Тайвань, Южная Корея, Малайзия, Таиланд и Филиппины – сегодня это главные производители высокотехнологичных продуктов на мировой арене, что в целом составляет 70-80 процентов всего мирового производства продукции широкого диапазона важных материалов, компонентов и изделий для высокотехнологичной продукции.

Азиатские производители, как правило, развивались по «японской модели». Южнокорейские и тайваньские компании наиболее технологически продвинуты среди остальных компаний региона после Японии, но они сталкиваются с вызовами на их пути к роли глобальных разработчиков информационных технологий.

Эксперты особо отмечают Китай как быстро растущего производителя информационных технологий. Сегодня определенные группы высокотехнологичной промышленности в Китае развиваются быстрыми темами, хотя их продукция далека от того, чтобы быть главным компонентом экономики страны.

Главные движущие силы в Китае - объем местного рынка и почти бесконечная, дешевая рабочая сила. Оба эти фактора привлекают иностранные инвестиции.

В последние годы Китай стал основным производителем высокотехнологичной продукции для азиатских стран. Ряд китайской

высокотехнологичной продукции успешно конкурирует на рынках США и Европы. В ближайшие десятилетия эта тенденция не только сохранится, но и будет нарастать, что связано со вступлением Китая в ВТО.

Китай также начинает существенно повышать собственный потенциал высококлассных специалистов в области высоких технологий за счет возвращения на родину китайцев, работавших в западных компаниях, а также после получения технического обучения за границей. В результате Китай должен продолжить стремительное движение в создании мощной высокотехнологической промышленности, что через какое-то время позволит ему стать главным игроком на рынке высоких технологий не только в Азии, но и в мире. В это же время многие нации (прежде всего европейские), которые сегодня более продвинуты, но обременены инерцией, созданной унаследованной инфраструктурой, будут терять свои позиции.

Кроме Китая Индия имеет три важных преимущества в глобальном высокотехнологичном соревновании: большое количество специалистов в области информационных технологий, большое количество образованных, дешевых рабочих, говорящих по-английски, и тесные связи многих индийских предпринимателей в американской Кремниевой Долине. В результате, в этой стране активно развивается высокотехнологичный бизнес, она - мировой лидер в производстве программного обеспечения, его производство в стране увеличилось в пятьдесят раз за последние 10 лет. Процветание и рост индийского рынка программного обеспечения и сферы услуг в области информационных технологий должны продолжиться и в ближайшие десятилетия.

Однако развитие индийского рынка программных средств может столкнуться с рядом трудностей, связанных, прежде всего, с ускоренным развитием в этой области Китая. Кроме того, индийская высокотехническая промышленность всего лишь небольшой процент от общей индийской экономики. Большая часть нации находится все еще в аграрной эпохе, еще не достигнув даже уровня индустриальной эпохи, уже не говоря об эпохе информационной. Эти факторы могут серьезно осложнить внутреннюю ситуацию в стране.

4. В ближайшие 10-20 лет геополитические тенденции, которым

содействует информационная революция, могут обозначить новые вызовы Соединенным Штатам.

По мнению экспертов РЭНД, несмотря на то, что американская экономика и общество достаточно хорошо подготовлены к встрече вызовов информационной революции, в ближайшие десятилетия появится достаточно много проигравших и отстающих в глобализации государств в различных частях планеты. Многие из этих проигравших или отстающих будут представлять серьезную угрозу безопасности США.

Информационная революция лучше позволяет разочаровавшимся народам объединиться и организоваться. Существование разочаровавшихся и хорошо организованных проигравших или отстающих будет вести к тенденциям в мире, которые могут бросить вызов жизненным американским интересам. Например:

• проигравшие в информационной революции могут стать «неудавшимися государствами». Такие неудавшиеся государства могут стать пристанищем для террористов, которые будут угрожать жизненным интересам США;

• стремление не отстать от США внесет напряжение в европейские экономики, общества и государства, создавая отстающих и проигравших в пределах Европы. Это в свою очередь может через какое-то время создать растущее напряжение и в НАТО;

• неспособность Японии достаточно измениться, чтобы справиться с информационной революцией - если это случится, может повлечь к неудаче японской экономики. Неудача экономики Японии в свою очередь приведет к вакууму в Азии, который будет заполнен Китаем. Это серьезно укрепит позицию Китая в Азии, и сделает Китай равным США конкурентом.

5. Непредвиденные обстоятельства, которые могут изменить глобальный курс информационной революции.

По мнению экспертов РЭНД, будущие «приложения убийцы», неясные в настоящее время, определят точный характер преобразований. Они определят точные детали информационной революции. Многие факторы могут замедлить или ускорить темп преобразований. Неблагоприятные финансовые события могут замедлить их, а неожиданные «приложения

убийцы» могут ускорить преобразования.

Будущие геополитические события типа новой «холодной войны», глобальный военный конфликт или крупномасштабный региональный конфликт неблагоприятно затронут развитие различных наций, регионов и мира в целом.

Постоянные, широко распространенные, разрушительные террористические акты могут иметь аналогичный эффект на отдельный регион или планету в целом.

Независимо от того, что может произойти скорость, с которой информационные технологии преобразовывают мир, вряд ли измениться. Эксперты РЭНД ожидают, что эти изменения в конечном счете будут весьма значительными.

Взгляд за горизонт событий

Разрабатывая новые подходы к проведению внешней и внутренней политики в ближайшие 15-20 лет, эксперты РЭНД пытаются заглянуть и на более длительный срок. Что же ждет человечество через 30-50 лет? Одним из важных выводов выполненного исследования является заключение о том, что ***информационная революция есть всего лишь часть более широкой технологической революции с еще более глубокими последствиями***, основные элементы которой в ближайшие 10-20 лет только начнут проступать.

Рисунок 11 Наномашины - будущее военной техники

Информационная революция не единственная рожденная технологией революция, которая сегодня идет полным ходом, она просто наиболее известна. Прогресс в биотехнологии и нанотехнологии и их совместных применениях с информационными технологиями должны кардинально изменить мир во второй половине XXI столетия.

Последствия биореволюции будут особенно глубокими и неоднозначными.

Достижения в области молекулярной биологии создали базу, необходимую для управления растительным, животным и человеческим геномами.

За прошедшее десятилетие были сделаны важные открытия, позволившие глубже понять и приступить к управлению фундаментальными структурами на микро и нано уровне. Проведенные исследования в области нанотехнологий в ближайшие годы позволят создать принципиально новые вычислительные устройства, которые в свою очередь позволят сохранить Закон Мура, и производительность компьютеров продолжит удваиваться каждые 18 месяцев. Согласно выводам экспертов подобные разработки, вероятно, изменят большинство отраслей промышленности: от новых вакцин и компьютеров, до новейших материалов для машиностроения и легкой промышленности, серьезно трансформируя мир XXI столетия.

В результате совместного применения достижений в области биотехнологий, нанотехнологий и информационных технологий полное экономическое и социальное воздействие этой объединенной технологической революции на общество будет еще более глубоким, чем от индивидуального воздействия каждой из технологий.

Способность изменять клетки и геномы животного уже привела к значительным противоречиям; способность изменять человеческий геном приведет к наиболее глубоким противоречия за всю историю человечества.

Генетически измененные продукты широко используются в некоторых частях мира и запрещены в других. Ограничения в свободном движении генетически измененных продуктов во всем мире уже стали одной из главных международных проблем. Аналогично, клонирование животных вызвало серьезные противоречия в ряде нации, в которых подобные эксперименты были предприняты.

По мнению экспертов РЭНД, все споры относительно изменения геномов растительного и животного происхождения ничто по сравнению со спорами, которые возникнут при попытках изменить человеческий геном, чтобы использовать методы генной инженерии для «улучшения» человеческого рода, клонирования людей и неограниченного продления

жизни путем пересадки клонированных органов. ***Эти конфликты по ожесточенности и напряженности превзойдут все известные до настоящего времени конфликты потому, что они затронут саму суть понятия «быть человеком».***

Поскольку темпы перечисленных технологических революций возрастают, а их синергетическое воздействие увеличивается, растет и понимание последствий их воздействия на общество будущего. Эксперты РЭНД констатируют, что в ходе указанных технологических революций сохранится неравенство отдельных наций и регионов планеты, более того ускорение темпом технологической революции приведет к углублению неравенства и как следствие – к небывалому росту напряженности во всем мире.

1.7. Новая геополитическая концепция США в эпоху глобализации и информационной революции

Изменение геополитической и геостратегической обстановки в мире, а также трансформация целей национальной стратегии США заставляет экспертов Пентагона активно разрабатывать новую геополитическую концепцию, призванную обозначить основные ориентиры США по переустройству мира в предстоящее столетие.

Как полагают военные эксперты, основу новой геополитической концепции составит подход, согласно которому положение США как лидера нового миропорядка во многом будет зависеть от того, насколько успешно будут развиваться процессы глобализации в современном мире. Еще с момента окончания Холодной войны администрация США находилась в постоянном поиске новой теории управления миром и необходимой для ее поддержки военной стратегии. Такой инструмент был найден в середине 90-х годов XX века. Им оказалась глобализация. Только при условии распространения глобализации на всю планету лидирующее положение США сохраниться.

По мнению экспертов Пентагона, та часть современного мира, которая восприняла модель глобализации, предложенную США, сегодня вполне может быть управляема невоенными средствами и, прежде всего, средствами

информационного манипулирования. Та же часть населения планеты, которая не восприняла процессы глобализации, должна быть силой «колонизирована».

Ключевой парадигмой новой стратегии является тезис ***«Разобщенность представляет опасность»*** (Disconnectedness defines danger). По мнению авторов концепции, режим Саддама Хусейна был опасно удален от глобализирующегося мира, от его правил поведения, его норм и связей, которые связывают страны в единый, подконтрольный США, механизм. Именно поэтому война с Ираком никак не связана с разоружением Ирака или продолжением объявленной США глобальной войны с террором. Эта война является, по их мнению, важным поворотным моментом, с которого Вашингтон начинает реализовывать свою новую стратегию доминирования в эпоху глобализации.

Многие отмечают, что насаждаемая и культивируемая США политика глобализации в последние годы привела к чрезвычайному расслоению общества: с одной стороны – в высшей степени глобализирванные страны Европы и Япония, а с другой – нищие государства Африки, Азии и Латинской Америки. Вместе с тем, по заявлениям авторов новой концепции, будущее современного мира будет определяться именно теми регионами планеты, в которых глобализация уже стала неотъемлемой частью жизнедеятельности общества. Эта часть планеты в предложенной геоплитической концепции носит названия «функционирующее ядро» (Functioning Core). В состав Ядра, по мнению авторов, сегодня входят Северная Америка, большая часть Южной Америки, Европейского союза, России, Японии и появляющихся экономик Азии (особенно Китай и Индия), Австралия и Новая Зеландия, Южная Африка. Общая численность населения Ядра составляет около четырех миллиардов.

Рисунок 12 Пол Вулфовиц - заместитель министра обороны и идеолог новой геополитической концепции США

Весь остальной мир, не охваченный процессами глобализации, в соответствии с предложенным подходом обозначен как «неинтегрированная

брешь» (Non-Integrating Gap), далее Брешь. Авторы называют эту Брешь «озоновой дырой глобализации», через которую в цивилизованный мир прорывается зло и ненависть. Прежде всего, в Брешь включены острова Карибского моря, фактически вся Африка, Балканы, Кавказ, Средняя Азия, ближневосточная и Юго-Западная Азия, большая часть Юго-Восточной Азии. Общее население Бреши – около двух миллиардов. Большая часть населения – мусульмане. Характерной особенностью населения этой части планеты является его очень молодой возраст и низкий доход на душу. Одним из наиболее радикальных продуктов Бреши сегодня является Аль-Каеда – сетевая транснациональная террористическая сеть.

Эксперты Пентагона, говоря о развитии масштабной операции вооруженных сил США, подчеркивают, что основная цель начатой глобальной операции - сокращение или полное устранение Бреши, что позволит установить полный контроль США над всей территорией планеты в рамках масштабной кампании всеобщей глобализации.

В этой связи, отмечают эксперты Пентагона, истинная причина войны с Ираком не в том, что Саддам Хусейн тиран, и не в том, что его режим поддержал террористические сети. Реальная причина состоит в том, что складывающаяся не в пользу Америки экономическая и политическая ситуация в мире вынуждает администрацию США иметь дело со всей Брешью как со стратегическим пространством из которого исходит смертельная угроза самому существованию Америки.

Важным принципом новой геополитической концепции является наличие разграничительной линии между Ядром и Брешью. По мнению авторов концепции, Ядро и Брешь разделяют, так называемые, «приграничные государства». К ним относятся: Мексика, Бразилия, Южная Африка, Марокко, Алжир, Греция, Турция, Пакистан, Таиланд, Малайзия, Филиппины и Индонезия. Эта линия не постоянна, она постоянно мигрирует, прежде всего из-за наличия приграничных государств: часть стран ранее входивших в ядро может в результате ряда событии перейти в Брешь, в то время как некоторые государства, ранее попавшие в Брешь могут предпринять усилия по выходу из нее. Однако таких прецедентов очень мало, чаше страна, вырвавшись из Бреши, не может долго удерживаться в

Ядре без помощи со стороны других государств, его образующих, и скатывается снова в пропасть Бреши.

Как отмечают американские эксперты, ретроспективный анализ мест применения военной силы армией США с момента окончания Второй мировой войны показывает, что большая их часть была сосредоточена именно в пространстве Бреши. Именно поэтому, говоря о возможных регионах применения военной силы США, эксперты отмечают, следующую закономерность: если страна терпит неудачу в процессе глобализации или самоизолируется от процессов глобализации, существует большая вероятность, что США в некоторый момент примут решение о проведение в отношении нее военной операции. И обратно, если страна в значительной степени функционирует по установленным законам глобализации, США будут использовать невоенные меры удержания контроля над такими государствами.

В качестве главного принципа, позволяющего отнести ту или иную страну к Бреши, определяется следующий тезис: ***положение страны, гарантирующее военный ответ США, обратно пропорционально ее возможностям к восприятию глобализации***. В этой связи аналитики считают, что есть серьезное обоснование тому, что Аль-Каеда базировалась сначала в Судане, а затем - в Афганистане. Это две из наиболее отсталых стран в мире, наименее вовлеченных в процессы глобализации.

Исходя из основных положений новой геополитической концепции, стратегия национальной безопасности США должна базироваться, по мнению экспертов, на трех основных тезисах: 1) увеличение иммунных способностей системы безопасности Ядра к новым угрозам; 2) развитие способности «приграничных государств» выполнять функции брандмауэра (пожарной стены) Ядра, способного оградить его от экспорта из Бреши террора, наркотиков, эпидемий и др.; 3) реализовывать комплекс мер, включая силовые, направленный на всестороннее сокращение Бреши. Реализация этих тезисов не может проходить без постоянного и всестороннего контроля за состоянием Бреши, способным выявить зарождение любых враждебных течений, которые могут вырваться за пределы установленного барьера.

По мнению авторов концепции, наилучшим местом для начала реализации выдвинутых тезисов является сегодня Ближний Восток. Развитие региона в направлении его единения с Ядром будет положено Израилем. Именно здесь имеется потенциал колеблющихся государств, типа Катара и Иордании, которые стремятся войти в Ядро. Однако без внешней жесткой силы переломит ситуацию в регионе достаточно сложно. Прежде всего, необходимо устранение Хусейна, как главного врага региона. Сделать это могут только США. По словам авторов проекта, сегодня Ирак – это Югославия Средне-восточного перекрестка цивилизаций. Именно поэтому смена режима в Ираке потребует длительного присутствия в регионе американских войск.

Основываясь на положениях новой геополитической концепции, эксперты делают вывод о наиболее опасных регионах планеты, в которых вероятно применение США военной силы в ближайшем будущем, это Гаити, Колумбия, Бразилия и Аргентина, бывшая Югославия, Конго и Руанда, Ангола, Южная Африка, Израиль и Палестина, Саудовская Аравия, Ирак, Сомали, Иран, Афганистан, Пакистан, Северная Корея, Индонезия.

Эксперты оценивают Южную Африку как единственную страну Ядра на Африканском континенте. Однако, ее географическое положение на «пузыре» стран Бреши ведет к тому, что Южная Африка сегодня является воротами для террористических сетей, ищущих доступ к Ядру.

В отношении Саудовской Аравии, авторы концепции выражают мнение, что «…менталитет королевской мафии, в конечном счете, вызовет бурю внутреннего протеста…».

В отношении Пакистана выражается озабоченность, что это государство может радикально изменить свое отношение к США с уходом ее нынешней администрации, превратившись в фундаменталистское исламское государство. Уже сегодня правительство этой страны не контролирует большую часть собственной территории, на которой свободно существует Аль-Каида. Наличие ядерного оружия в этом случае делает Пакистан смертельно опасным, что уже заставило во многом пересматривать политику США в отношении него.

Вызывающая, по мнению авторов концепции, позиция Северной Кореи может привести к тому, что эта страна окажется следующей из стран Бреши после Ирака, в отношении которой будет применена сила американской армии.

Также среди возможных будущих целей американской армии выделяются Китай, России и Индия. Но судьба этих стран сегодня во многом зависит от пути, которым они будут развиваться в ближайшие годы и от меры их вовлеченности в процессы глобализации.

Принятие новой геополитической концепции обуславливает и то, что в высших кругах Пентагона в последнее время вырабатывается план изменения размещения военных баз за пределами континентальной части США в соответствии с новой моделью угроз и новой геополитической концепцией, в основе которой лежит противостояние глобализированного Запада и нежелающего глобализации Востока.

Эксперты Пентагона отмечают, что необходимость подобного перемещения пунктов базирования вызвана тем, что сегодняшнее геостратегическое пространство кардинальным образом изменилось за последние пятнадцать лет. В то же время военные базы США все еще отражают ту модель угроз, которая была принята во времена Холодной войны.

Существующее в настоящее время размещение военных баз уже неоднократно выступало препятствием в ходе проведения ряда операций вооруженными силами США. Эксперты полагают, что в ближайшее время с ходом развития антитеррористической кампании число подобных проблем будет возрастать.

Согласно новой геополитической концепции Пентагона, новые миссии вооруженных сил США в ближайшие десятилетия будут включать охрану, так называемого «американского периметра безопасности», который в последние годы серьезно расширился по ряду направлений. Этот «периметр» в Европе больше не проходит через Германию, он сильно продвинулся в восточном направлении, но еще более значительно - на юг.

Также отмечается, что сегодня основная угроза для США в Европе продолжает исходить от неустойчивого положения на Балканах, где

негативная политика Ближнего Востока начинает просачиваться в Европу: по берегам Черного моря и Средиземноморья, на восточной границе Турции. Этот периметр сегодня также определяют прибалтийские государства и страны Восточной Европы, оберегающие Европу от поставок наркотиков, оружия и «живого товара» из республик бывшего СССР.

Однако еще более существенно «американский периметр» расширился на Ближнем Востоке, особенно после 11 сентября 2001 года. Кроме того, по заявлению ряда экспертов, начиная с 11 сентября 2001года само определение «Ближневосточного театра войны» существенно изменилось, включив в себя Кавказ, Среднюю Азию и значительную часть Южной Азии. Война в Афганистане привела к размещению американских войск в Узбекистане и Пакистане.

Американский периметр в Восточной Азии также расширилась. По мнению авторов плана, в дополнение к угрозам со стороны Северной Кореи, рост Китайской мощи и влияния радикального ислама в Юго-Восточной Азии должны быть расценены как важнейшие угрозы безопасности Соединенным Штатам в этом регионе в течение следующего столетия.

Необходимость перемещения американских баз вызвана тем, что столь существенно расширенный «периметр» должен постоянно контролироваться вооруженными силами США. Даже учитывая, что американские войска сегодня развернуты больше чем в сорока странах, места долговременного базирования были несущественно изменены со времен Холодной войны. Военные эксперты США отмечают, что сегодня новый периметр уже активно патрулируется, однако эта новая миссия все еще расценивается скорее как исключение чем новые правила.

Расстояние старых баз от новых войн препятствует возможности оперативного перемещения войск и их огневой поддержки. Учитывая изменение модели угроз, исходящих от надгосударственных террористических структур, базирующихся в основном на территории государств Ближнего Востока, в последнее время особенно возрос интерес американских стратегов к военным базам в Турции. Прежде всего – к военно-воздушной базе «Инжирлик», которая сегодня играет значительную роль в

операции против Ирака. Действия на Балканах также закончились расширением американских баз в Италии, особенно базы «Авиано».

Многие специалисты отмечают, что за последние десять лет американские силы в Европе переместились на юг и в восточном направлении. Эксперты Пентагона считают, что настало время признать, что это не временное явление, а постоянное изменение и необходимо приспосабливать базирование войск США. Текущее развертывание сил в регионе вокруг Ирака не было бы возможно без авиабаз в Европе, без безопасной морского транспортного пути через Средиземноморье к Суэцкому каналу и к Турции. На этом основании делается вывод о том, что было бы оправдано исследовать перспективы базирования ряда американских частей в Польше, Болгарии и Румынии или в некоторых других странах в Восточной Европе, а также существенно расширить военное присутствие в Турции.

Кроме того, отмечается, что вопрос о европейских базах не может рассматриваться в изоляции от глобального размещения американских сил. Будущее военного присутствия США в Европе должно быть согласовано с длительным американским присутствием в Афганистане и Средней Азии, а также в Ираке и Персидском заливе в целом. Аналогично, американские силы в Восточной Азии не должны быть способны только к сдерживанию Северной Кореи или Китайского удара по Тайваню, они должны быть способны поддержать войну против исламского фундаментализма во всей Юго-Восточной и Южной Азии.

1.8. Будущее Евразии. Основные ориентиры прогноза «Глобальные тенденции 2020»

В начале декабря 2003 года на интернет-сайте Национального совет по разведке (National Intelligence Council, NIC) США были представлены первые дискуссионные материалы нового исследования, посвященного тенденциям развития современного мира – «Global Trends 2020». Предыдущее исследование («Global Trends 2015»), опубликованное в конце 90-х годов прошлого века, достаточно активно обсуждалось и цитировалось в

российской прессе. Что же изменилось в оценках развития обстановки в мире на ближайшие 15-20 лет?

Отличием нынешнего прогноза от предыдущих является наличие так называемых «wild cards» - сценариев неожиданного и неблагоприятного развития событий. Как отмечается экспертами NIC, в предыдущих исследованиях им не удалось с достаточной долей уверенности спрогнозировать ряд событий, оказавших серьезное воздействие на развитие ситуации в мире. Введение таких сценариев призвано во многом исправить это упущение.

Общим вектором нового исследования стал тезис о том, что в ближайшей перспективе продолжится глобальное доминирование США, хотя эксперты не снимают со счетов и усиление влияния Китая, уменьшение стратегической важности Европы в вопросах мировой безопасности, старение ее населения, а также рост и омоложение населения в США и Китае.

Европа на рубеже 2020 года

Так, согласно выводам экспертов NIC, в 2020 году Европа будет обладать значительной глобальной экономической и политической силой, соперничая в этом с США и Китаем. Локомотивом Европы будет Евросоюз (ЕС), в который к тому времени будут входить все страны Европы, а также Норвегия, Швейцария, Исландия, балканские государства, Турция и возможно Украина.

Европа будет все настойчивее преследовать свои собственные интересы и все менее следовать в фарватере США. Она пойдет своим путем посредством реализации региональных инициатив в Средиземноморье, Африке и Ближнем Востоке – регионах, где, по мнению европейских политиков, Европа в связи с историческими, географическими и культурными причинами будет играть заметную роль.

Вместе с тем, в ближайшие 15-20 лет в Европе будут прослеживаться и некоторые негативные аспекты. Прежде всего, ЕС станет менее однородным. Сохраняться различия между западной и восточной Европой (не такие

большие как сегодня), хотя несколько уменьшится различие в уровне жизни богатых и бедных регионов.

Рост масштабов Европейского Союза сделает его более тяжеловесным и менее управляемым. Возникнет напряженность в отношениях между последователями расширения союза (максимальное включение всех европейских стран) и представителями институционального идеализма (Европа менее обширная с более глубоким уровнем кооперации). Тем не менее, по оценкам экспертов NIC, к 2020 году Евросоюз расширится, по меньшей мере, до 30 стран, при этом различия в отношениях между «старой» и «новой» Европой не будут играть существенной роли. Так называемый «франко-германский мотор» усилит центрально-европейскую группу стран, хотя сохранится как борьба за лидерство в ЕС (особенно среди ведущих стран), так и тактические альянсы между ними. Будет достигнут европейский консенсус по основным проблемам (безопасность, управление, экономика).

Вместе с тем особенно отмечается, что проблемы внутренней стабильности в странах, стремящихся в ЕС, таких как Албания, Македония, Молдавия, и возможно Украина и Белоруссия, а также давление со стороны Российской Федерации против включения последних в европейские структуры станет источником напряженности.

Демографические проблемы Европы к 2020 году

Вопрос демографии для Европы будет одним из наиболее важных. Те демографические тенденции, которые определились в последние десятилетия, будут иметь место и в будущем, результатом чего станет существенное старение населения и уменьшение его численности. К 2030 году четверть населения Западной Европы будет старше 65 лет. Среди всех частей света в Европе сохранится самый низкий уровень рождаемости. В свою очередь три западноевропейских страны (Германия, Франция и Испания) имеют низший уровень рождаемости в Европе. В этой связи обострится потребность в рабочих ресурсах. Дефицит рабочих рук может быть несколько ослаблен растущим населением внутри расширенного ЕС (за счет Балкан и Турции).

Сейчас рождаемость в центрально- и восточно-европейских государствах снижается меньшими темпами, и они будут продолжать

догонять Западную Европу по численности населения. Через некоторое время это должно изменить динамику демографических процессов внутри ЕС.

Некоторые европейские страны (например, Германия) уже сейчас борются с повышением пенсий для стареющего населения (реформа идет, но медленно). Стремясь сохранить неизменными более важные расходы, такие как расходы на образование и здравоохранение, расходы на оборону и программы оказания экономической помощи могут подвергнуться серьезному изменению. Однако, как считают эксперты NIC, остроту проблемы может снять эффективное европейское сотрудничество.

Высокая рождаемость среди иммигрантов отразиться на европейской межнациональной картине. Увеличится политическая роль мигрантов, как части электората. Правительства будут вынуждены брать в расчет такое развитие ситуации. В свою очередь это может повлиять на отношение к проблемам международной безопасности (арабо-израильский конфликт, международный терроризм) и на отношения с развитыми странами. Нарастающее противодействие процессам иммиграции, как показали результаты многих выборов по всему континенту, может быть предвестником уменьшения ее темпов, что усилит как проблему старения населения, так и проблему снижения темпов экономического роста. Для социальной стабильности будут иметь последствия усиление нетерпимости к иммигрантам.

Природные ресурсы и окружающая среда – важные проблемы для Европы 2020 года.

В ближайшей перспективе будет усиливаться давление на окружающую среду. Остро встанет вопрос обеспечения экологической безопасности населения Европы. Это станет основой нового мировосприятия: люди будут внимательнее относиться к проблемам защиты окружающей среды и рассматривать их в качестве приоритетных.

Наряду с этим Европа станет еще более зависимой от внешних энергоресурсов и будет искать источники возобновляемой энергии (хотя такие источники и не займут сколько-нибудь существенного места в общей энергосистеме Европы), атомной энергии, а также импорта энергоносителей

– особенно из России, характеризующейся своим непостоянством (хотя, по мнению экспертов NIC, без мощных инвестиций в производство и транспортную систему углеводородного сырья Россия будет не в состоянии заполнить европейский энергетический рынок). Технологические преимущества (например, производство сжиженного газа) позволят несколько диверсифицировать источники поступления газа, а новые технологии, такие как автомобили на сжиженном топливе, получат намного более широкое распространение.

В связи с затянувшейся сельскохозяйственной реформой Европа станет намного более зависимой от импорта продовольствия. Это приведет к напряженности и безработице в сельскохозяйственных районах, что серьезно подорвет сельское хозяйство в странах-новичках ЕС.

Вероятность экологических катастроф (например, затопление низменных частей Европы, таких как Нидерланды, вследствие глобального потепления, загрязнение окружающей среды) возрастет. Управление подобными процессами потребует значительных усилий и ресурсов. В силу своей значимости подобные проблемы приобретут политическую окраску, создавая напряженность в отношениях с рядом регионов мира, которые не являются такими «зелеными», как Европа.

Наука и техника.

Европа останется центром инноваций. Продолжится процесс перестройки большинства отраслей ее тяжелой промышленности. Разработка новых видов техники будет сосредоточена на высокотехнологичных направлениях (автомобилестроение, авиация и космос). Сохранится доминирование сферы услуг.

Между тем, к 2020 году Китай может составить конкуренцию Европе в производстве высокотехнологичной продукции. Тем не менее, европейские высокотехнологичные отрасли промышленности и их продукция вместе с хорошей системой образования обеспечат лидирующие позиции единой Европе.

Мировая экономика и процессы глобализации: их влияние на Европу 2020.

Реальный рост экономики ЕС будет в среднем ниже потенциального, что будет следствием сохранения элементов «старой» (западноевропейской) экономики. Сохранится относительно высокая безработица. Вместе с тем, глобализация сделает гибкость в экономике особенно важным фактором, этим будут обладать вновь принятые страны.

По оценкам экспертов NIC, в 2020 году в целом экономика ЕС будет второй по масштабам экономикой (после США). Однако Китай будет быстро догонять ЕС. Хотя Китай пока будет иметь значительно меньшую долю ВВП на душу населения, чем ЕС.

К 2020 году восточноевропейские страны станут наиболее быстро растущими в экономическом отношении. Членство в ЕС станет гарантией того, что возвращение к их политическому и экономическому прошлому невозможно, а также гарантией притока инвестиций. С другой стороны, вступление в ЕС принесет определенные финансовые затраты, весьма спорные для развития восточноевропейских стран.

Процесс глобализации будет продолжаться и расширяться. Он затронет и богатые, и бедные страны. Глобализация станет причиной переходных (транзитных) затрат и перетекания экономики в наиболее выгодные регионы, с наименьшим уровнем накладных расходов, – например, сейчас центр текстильной промышленности перемещается в Китай из богатых и среднего уровня развития стран. В свою очередь это вызовет напряженность, повышение безработицы среди рабочих, которые будут вынуждены искать другие места работы.

К 2020 году такие процессы могут усилить протекционистские тенденции, что составит определенную угрозу мировой экономике. Авторитет Всемирной торговой организации может быть подорван такими болезненными переменами.

Международная напряженность в экономике может подтолкнуть людей к переосмыслению взаимозависимости государств как части процесса глобализации. Возможны резкие, шоковые скачки цен на ряд важнейших товаров (прежде всего – нефть), которые могут быть связаны с негативным развитием событий на Ближнем Востоке.

Политическая система и безопасность Европы 2020 года.

Европейский Союз войдет в 2020 год в расширенном составе и с расширенными полномочиями (включая оборону, внешнюю политику и более гармонизированную систему налогообложения). Национальные государства сохранятся, но они будут тесно связаны общими интересами, ценностями и экономикой.

Программа европейской политики в области безопасности и обороны (ЕПБО) явится существенным, хотя и ограниченным, измерением в области безопасности и обороны (которое заполнит уменьшение численности американских войск в Европе). Вместе с тем, по мнению NIC, американские военные возможности в регионе и далее будут востребованы. Европа не будет готова пожертвовать расходами на социальную сферу ради реализации своих расхождений в военных взглядах с США.

В то время как произойдут некоторые улучшения за счет эффективного сотрудничества и уменьшения дублирования, Европа все больше будет сосредотачивать свои усилия на вооруженных конфликтах малого масштаба, контртерроризме и предотвращении конфликтов, чем на крупномасштабных военных действиях.

В условиях сокращенной численности и измененной структуры американских войск, а также в отсутствии вероятной военной угрозы ЕС возьмет на себя ответственность за свою коллективную оборону. Ключевым аспектом европейской обороны может стать Европейская система ПРО ТВД, возможно, по мнению экспертов NIC, с российским участием.

К 2020 году военный блок НАТО возможно еще сохранится, но с более размытым членством и более ограниченным потенциалом принятия решений. Основными направлениями усилий сил НАТО будут предотвращение конфликтов и миротворчество за пределами Европы, а не территориальная оборона. Некоторые направления деятельности НАТО отойдут к европейским структурам.

Одной из наиболее значимых проблем останется терроризм. Характерно, но, по мнению экспертов NIC, к 2020 году националистический терроризм (Ирландия или Испания) будет редким явлением. Вместе с тем

террористическим потенциалом обзаведутся некоторые криминальные группировки. Кроме того, религиозные экстремисты также продолжат проводить террористические атаки.

Роль США в европейских процессах.

США останутся главным союзником Европы. Однако в их отношениях будет существовать напряженность и намного более сильная, чем сегодня. Изменятся приоритеты взаимоотношений. Американские войска в Европе будут существенно сокращены. Оставшееся присутствие войск будет передвинуто дальше на восток и юг, Европа станет использоваться в основном как база для сил, участвующих в региональных конфликтах за пределами Европы, вопрос собственно европейской обороны перестанет быть актуальным.

Европа будет занята поиском путей изменения тона в отношениях с США и поиском своей новой роли на международной арене. Эти попытки станут более настойчивыми; при этом США будут рассматриваться не только в качестве друга, но и в качестве экономического и политического соперника.

Каковы же наиболее важные тенденции, формирующие региональные события до 2020 года?

- У Европы растет чувство уверенности: она будет все более настойчивой и твердой политически и экономически; будет готова проводить независимый курс во внутренней политике.
- Европа растет в размерах – все больше и больше стран вступают в ЕС или ассоциируются с ним.
- Европа растет в своем статусе – она все больше рассматривается другими (напр. Китаем) как экономическая и политическая сила, соперничающая с США.
- Усиливающаяся европейская идентичность – общие организации, общая валюта, общая политика и т.д. Люди все более ощущают себя гражданами Европы также как (а не вместо) гражданами национальных государств.

Варианты негативного развития событий в Европе 2020

- Экономика Европы стагнирует, осознание этого не может сдержать расширение, что ведет к инертности и упадку. В области оборонной политики возможны, по мнению экспертов NIC, три сценария: независимая оборонная политика с более высокими затратами; несколько более зависимая политика в области обороны, при которой сохраняются высокие расходы на социальный сектор; независимая оборонная политика без адекватных затрат, ослабляющая стратегический вес Европы.

- Европа распадается – возникают новые линии разлома, например между старой и новой Европой; севером и югом; большими и малыми государствами.

- Европа растет – и географически (например, ЕС расширяется, включив Россию) и по уровню ответственности (например, заменяя собой НАТО).

- Новая холодная война – с возрождающейся Россией и друзьями. Исламистское окружение? Или что-нибудь еще?

- Новая европейская нестабильность – возобновившийся балканский конфликт?

Россия, год 2020

По мнению экспертов NIC, Россия сегодня все еще находится на переломном моменте истории, в преддверии очередных президентских выборов. На рубеже 2020 года, очень многое будет зависеть от того, чем закончится нынешняя борьба политических сил.

Россия сегодня стоит перед огромными объективными проблемами управления:

- Политическая инфраструктура и политическая культура по-прежнему очень слабы.

- «Демократическая трансформация» не доведена до конца. Политическая элита и бюрократия на всех уровнях все более контролирует политические процессы: эта тенденция реально усилилась. В перспективе

лишь немногие политические партии и отдельные деятели будут привержены демократии западного типа.

- Рыночные реформы не завершены. Самые трудные решения оставлены на второй президентский срок В.Путина, такие как реформы ЖКХ, структурные и банковские реформы. Россия все еще сильно зависит от добывающих отраслей промышленности, следовательно, - от цен на нефть.

- Существенные демографические проблемы включают в себя хрупкость и несбалансированность населения – продолжительность жизни ниже восполняемого уровня, идет неуклонная убыль населения.

В 2020 году отношения России с окружающим миром будут оставаться двойственными и противоречивыми. Она будет определять свои интересы путями, которые не всегда будут гармонизировать с интересами ведущих европейских стран, но возврат к военной и идеологической конфронтации с Западом даже виртуально уже невозможен.

В международных отношениях Россия станет близко идентифицировать себя с Европой и возможно даже свяжет себя с ней каким-либо видом формального договора или соглашения. Станет ли это членством в Евросоюзе, будет зависеть в равной мере от ЕС и от российской политики.

В качестве члена ВТО Россия будет намного глубже интегрирована в мировую экономику, хотя в отдельных секторах и регионах, возможно, продолжаться протекционистские настроения. Многие в России (возможно, даже большинство) будут сопротивляться включению ее в глобальную международную организацию, где Россия не будет ведущим элементом, несмотря на экономические выгоды.

Основной проблемой российского руководства будет проблема примирения региональной по масштабам экономики с глобальными политическими амбициями быть Великой державой. Основными внешнеполитическими партнерами к 2020 году будут оставаться США и ЕС, за ними – Китай и Индия.

Россия останется главной державой Евразии и сохранит свой интерес к сотрудничеству в рамках СНГ. Связи в области политики и безопасности со странами СНГ скорее всего будут иметь вид асимметричных коалиций. Связи России со славянскими государствами бывшего СССР (Украина и

Белоруссия) могут быть несколько сильнее. Даже если Украина будет иметь успех в своем желании вступить в Евросоюз (а Россия будет делать все, чтобы этого не допустить), социальные, инфраструктурные и экономические связи останутся сильными.

Возможна некая форма федерации, даже союз с Белоруссией. Государства Кавказа и Закавказья (Азербайджан и Грузия) будут стремиться остаться на несколько более дальней дистанции, однако состоятельность Грузии как государства все еще может остаться под вопросом. Армения же наиболее близка к тому, чтобы стать близким и стабильным соседом при сохранении собственной идентичности.

Центрально-азиатские государства, скорее всего, будут политически отодвигаться дальше и дальше от России, сохраняя свою идентичность и некоторые экономические связи для поддержания стабильных отношений с Россией, но также выбирая и другие альянсы (особенно с США и другими основными региональными игроками).

Проблемы демографии России к 2020 году

По мнению экспертов NIC, русские до сих пор не демонстрируют даже признаков к готовности соответствующим образом решать демографические вопросы. Продолжительность жизни далека от нормальных европейских стандартов, уровень рождаемости очень низкий (соотношение смертности к рождаемости 2:1, по оценкам экспертов NIC численность населения, скорее всего, упадет со 143 до 130 миллионов человек); уровень хронических и психических заболеваний очень высок, особенно среди детей, что не позволяет говорить о формировании в будущем здоровой нации.

Существует вероятность взрывного роста заболеваемости СПИДом, гепатитом и туберкулезом. Очень маловероятно, что власти будут в состоянии справиться с этим, еще меньше – предупредить подобное развитие событий.

Сохранится неравномерное распределение населения как результат географии и исторических особенностей развития в советский период. В Сибири и районах к востоку от нее проживает только 20% населения (и этот процент быстро уменьшается).

Природные ресурсы и окружающая среда для России 2020 года.

До 2020 года значительные российские энергетические ресурсы будут эксплуатироваться в все возрастающем темпе. В этот период ЕС скорее всего станет основным покупателем российских энергоносителей, хотя экономические выгоды от прокладки трубопроводов в центрально-азиатских государствах могут заставить Россию повернуться на восток в поисках экспорта энергии. Важно то, что произойдет приток иностранных инвестиций в энергетический сектор, хотя сложная, запутанная ситуация с нефтяной компанией «Юкос» и М.Ходорковским, может и отложить поступление инвестиций, особенно если этот процесс не закончится атакой только на одного «олигарха».

Растет осознание проблем природных ресурсов и окружающей среды, также как и желание справиться с огромным грузом проблем советского наследства. Но это очень тяжелая задача и вряд ли она будет выполнена к 2020 году. Россия не очень стремится к западным стандартам.

Наука и техника России

Это направление в России традиционно сильно, но очень плохо финансируется в последние годы. Текущее состояние дел в экономике не дает надежд на перемены в ближайшем будущем, но В.Путин или его последователь могут принять политическое решение о больших инвестициях в науку и технику.

Глобальная экономика и глобализация: их влияние на Россию к 2020 году.

Сегодня Россия достигла некоторого прогресса в проведении экономических реформ, но имеет серьезные проблемы их реализации «на местах». Это положение может продлиться и до 2020 года. В дополнение, ключевые реформы идут очень трудно. Реализация этих реформ, затягиваясь по времени, может быть совсем отложена.

Россия к 2020 году не совершит такого же экономического рывка как Китай. По мировым стандартам ее экономика останется такой же

среднемасштабной. Это будет некий структурный гибрид, состоящий из элементов рынка (европейских стандартов) с существенным влиянием государства. Ключевые отрасли промышленности будут корпоративными и, скорее всего, неэффективными. Внутренние рынки (капитала, труда, производства) останутся неразвитыми и сегментированными. Слабое трудовое законодательство, высокая преступность, коррупция и незащищенность от колебаний цен на товары первой необходимости не позволят сохранить существующие высокие темпы экономического роста.

В целом производство по стране будет развиваться неравномерно, что явится причиной увеличивающегося разрыва в уровне жизни регионов. В свою очередь это будет мешать готовности руководства поднять внутренние жизненные стандарты. Несмотря на общий рост, Россия не сможет справиться с проблемой бедности, которая актуальна для миллионов россиян. Эти люди в принципе уже смирились с нуждой, и не будут являться угрозой для социальной и политической стабильности. Событий, подобных октябрю 1993 года, уже не будет.

Таким образом, в политико-экономическом плане Россия к 2020 году будет представлять нечто подобное тому, что уже наблюдается и сейчас. «Экономический коллапс», развал основной экономической инфраструктуры маловероятен. Коррупция и (в отдельных регионах и секторах) организованная преступность будут оставаться существенными факторами российской действительности.

К 2020 году в России увеличится активность иностранного капитала. Законодательная база будет в большей степени это позволять, хотя полностью и не достигнет европейских стандартов.

Хотя доступ в глобальную сеть Интернет сейчас не достаточно распространен среди населения, темпы его внедрения будут усилены (в любой форме его существования в будущем). Это позволит российским источникам информации отчасти уйти из под контроля российских властей, но в то же время может привести к ускоренной утечке русских мозгов в виде рынка труда для молодежи, этот рынок будет более мобильным одновременно и физически, и виртуально.

Политическая система и безопасность России к 2020 году

По мнению экспертов NIC, сегодня Владимир Путин пытается продолжить свою работу по совершенствованию основных законов и по проведению административной реформы. Развитию реформ и хорошему управлению угрожает децентрализация власти как на региональном, так и на федеральном уровне.

К 2020 году важные институты демократии (такие как выборы) будут существовать и на федеральном, и на региональном уровне, но российская политическая система останется авторитарной по европейским стандартам. Более глубокая демократизация – правовая сфера, развитие парламентаризма, политических партий, гражданского общества – будет фрагментарным и слабым. Соблюдение прав человека и гражданских свобод по-прежнему будет носить условный характер. Здесь возникнут существенные региональные различия: в одних регионах гражданские свободы будут относительно соблюдаться, в других – окажутся под серьезной угрозой.

В условиях отсутствия масштабных внутренних потрясений (таких как массивные экономические проблемы), федерация будет сохраняться. Парадоксально, но, по мнению специалистов NIC, политическая недоразвитость может быть фактором стабильности: будет наблюдаться отсутствие политических групп, заинтересованных в подстрекательстве к беспорядкам. Россия сохранит свое место в составе Совета Безопасности ООН.

Роль военной силы будет занимать более весомое место в официальных определениях национальной безопасности, чем в Европе, но нет сомнения в возможности возврата к советским уровням военных расходов.

Стержневым элементом военного планирования останется возможность использования стратегических ядерных сил.

Чечня, скорее всего, все еще останется запутанным клубком проблем на ближайшее будущее. Другие региональные конфликты на территории стран СНГ будут зависеть от множества факторов, но Россия не является держателем всех козырных карт и не торопится (в основном по тактическим соображениям) играть даже теми картами, которые у нее имеются.

Россия переместится ближе к НАТО. Не исключена даже просьба с ее стороны о вступлении в эту организацию.

Российско-американские отношения

Российская система взглядов не предполагает сильных отклонений от ее теперешней двойственности: США будут рассматриваться не только как ключевой объект внешней политики и как союзник, но и как успешный соперник. Россия хочет, чтобы ее серьезно рассматривали в качестве партнера: больше всего она боятся быть проигнорированной или оказаться на вторых ролях. Не допуская проявлений крайнего национализма в Россия будет держаться вместе с США. Но она будет продолжать отстаивать свои права, часто, как отмечают в NIC, неуклюжими и причудливыми способами.

Проводимое перебазирование американских войск – особенно создание постоянных баз США и НАТО на территории стран СНГ, на Кавказе и в Центральной Азии – пойдет вразрез с существующими российскими положениями национальной безопасности. Вместе с возможной разработкой американской системы ПРО эти события могут создать проблемы для российского руководства, и привести к периодам напряженности.

Каковы наиболее важные тенденции, формирующие региональные события от сегодняшнего момента и до 2020 года?

- Негативные последствия сокращения численности населения и плохого здравоохранения.

- Увеличение добычи нефти и газа и поставка их через территорию стран СНГ, а также споры вокруг их транспортировки.

- Внутренние угрозы исламского экстремизма (реальные или надуманные) и реакция на них.

- Проблемы во взаимоотношениях между Россией и странами СНГ, включая передислокацию войск США и НАТО и создание ими передовых баз.

Возможные негативные варианты развития событий

- Возврат к политической нестабильности: правление В.Путина прекращается досрочно вследствие его нездоровья или появления успешного

политического соперника (возможно из олигархов), это может сопровождаться десятилетием политической нестабильности и авантюристического правления.

- Экономическая стагнация или упадок; низкие цены на нефть или прекращение иностранных инвестиций ведет к усилению депрессии с политическими последствиями.

- Внутренний кризис безопасности: Россия переживает всплеск чеченских повстанческих действий на Северном Кавказе, действий исламистов в Центральной Азии и гражданских беспорядков на российском Дальнем Востоке вкупе с китайской иммиграцией и экономическим проникновением Китая.

- Серьезное ухудшение отношений с США и НАТО из-за развертывания элементов ПРО и военной интервенцией США и НАТО в некоторых регионах мира.

Таким образом, России к 2020 году четко очерчены границы региональной державы, и даже наличие ядерных сил, места хранения которых к тому времени, возможно, будут охраняться совместными усилиями России и США, не позволит поддержать статус России как «великой державы».

Глава 2. Основы борьбы в информационной сфере. Средства и системы борьбы в компьютерных сетях

2.1. О появлении термина «информационная война» в иностранной литературе

Сегодня много говорится об «информационной войне» (англ. *Information warfare*). Однако вряд ли кто сможет точно ответить, что же это такое. Более того, даже специалисты не смогут ответить на вопрос о том, когда же все-таки родилось само словосочетание «информационная война», когда впервые был поставлен вопрос о том, чтобы рассматривать информацию в качестве оружия? Далее, если выяснить эту информацию и дать ответы на поставленные вопросы, то, несомненно, сразу встанет целый ряд подобных вопросов, например, что есть информационная война? Какими средствами она ведется и, что ставится целью этой войны? Считать ли нападения хакеров военными действиями, если да, то какие средства ответа будут адекватными? Ниже мы попробуем дать ответы на эти и, возможно, другие вопросы по затронутой теме.

Так, например, рядом экспертов отмечается, что еще в 1976 году в одном из отчетов, подготовленных для американской авиастроительной

корпорации Boeing, под названием «Системы вооружения и информационная война»[4] впервые был использован термин «информационная война». Авторы отчета указывали, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и одной из наиболее уязвимых целей как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина «информационная война».

Рисунок 13.Основные документы КНШ, в области информационной войны

Публикация результатов проделанной работы послужила началом активной кампании в средствах массовой информации. Сама постановка проблемы весьма заинтересовала американских военных, которым свойственно заниматься «секретными материалами». Военно-воздушные силы США начали активно обсуждать этот предмет уже с 1980 года. К тому

[4] Thomas P. Rona, “Weapon Systems and Information War”, Boeing Aerospace Co., Seattle, WA, 1976.

времени было достигнуто полное понимание того, что информация может быть как целью, так и оружием.

В связи с появлением новых задач после окончания Холодной войны термин «информационная война» был введен в документы Министерства обороны США. Он стало активно упоминаться в прессе после проведения операции «Буря в пустыне» в 1991 году, где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые введен в директиве министра обороны США DOD TS 3600 от 21 декабря 1992 года.

Спустя несколько лет, в феврале 1996 года, Министерство обороны США ввело в действие «Доктрину борьбы с системами контроля и управления»[5]. Эта публикация излагала принципы борьбы с системами контроля и управления как применение информационной войны в военных действиях. Публикация определяет борьбу с системами контроля и управления как: «…объединенное использование приемов и методов безопасности, военной хитрости, психологических операций, радиоэлектронной борьбы и физического разрушения объектов системы управления для недопущения сбора информации, оказания влияния или уничтожения способностей противника по контролю и управлению над полем боя, при одновременной защите своих сил и сил союзников, а также препятствование противнику делать тоже самое…».

Рисунок 14 Информационные системы пунктов управления войсками - одна из главнейших целей в информационной войне

В этом документе также была определена организационная структура, порядок планирования, обучения и управления ходом операции. Наиболее важным является то, что данная публикация определила понятие и доктрину войны с системами контроля и управления. Это был первый случай, когда Министерство обороны США, определил возможности и доктрину информационной войны.

2.2. Основные понятия информационной войны

Завершение формирования в последние годы принципиально новой сферы противоборства – ***информационного пространства***, привело к необходимости, по мнению экспертов Пентагона, коренного пересмотра основ современной военной науки.

Прежде всего, роль и значение информационного ресурса в развитии социума на современном этапе столь велика, а отличие информационного пространства от физического столь значительно, что необходимо говорить о принципиально новой форме вооруженной борьбы – ***информационной войне***.

Информационная война определяется как, широкомасштабная информационная борьба с применением способов и средств информационного воздействия на противника в интересах достижения целей воздействующей стороны.

По направленности информационных воздействий информационная война, как правило, подразделяется на два основных вида: информационно-психологическую (психологическую) и информационно-техническую.

Эксперты Пентагона считают, что информационная война может проводиться во всех сферах общественной жизни – в экономике, политике, в военном деле, в социальных отношениях, в сфере духовной жизни и особенно в идеологии.

Ключевым отличием информационной войны от войны в физическом пространстве является то, что информационная война – это война скорее манипулятивная, а не поражающая. В зарубежной литературе в последнее время в отношении информационного оружия даже появился термин «оружие массовых разрушений» (weapon of mass disruption) в противовес традиционному «оружию массового поражения» (weapon of mass destruction).

Цель информационной войны достигается таким воздействием на противника, в результате которого он самостоятельно, без принуждения принимает благоприятные для атакующей стороны решения.

---

[5] Joint Pub 3-13.1 “Command and Control Warfare”, DOD US, February 1996.

Информационная война ведется в информационном пространстве. Основной поражающий фактор – информационное воздействие, которое представляет собой воздействие информационным потоком (потоком данных в компьютерной системе и др.) на объект атаки – информационную систему или ее компонент, - с целью вызвать в нем в результате приема и обработки данного потока заданные структурные и/или функциональные изменения.

Существует, например, мнение ряда экспертов, согласно которому необходимо полностью исключить любое участие физических средств поражения в информационных действиях (таких, как поражение пунктов управления, разрушение инфраструктуры и др.), эти действия находятся в физическом пространстве, которое является традиционной областью войны. Оно объединяет традиционные сферы противоборства - землю, море, воздух и космическое пространство. Это пространство, в котором функционируют системы вооружения, военной техники и системы коммуникаций.

Боевые действия в информационном пространстве разворачиваются в технической и психологической сферах.

Техническая сфера – область информационного пространства, в которой создается, обрабатывается и накапливается информация. Кроме того, это область, в которой функционируют системы командования, управления, связи, коммуникаций и разведки.

Психологическая сфера - область информационного пространства, которая объединяет мышление личного состава вооруженных сил и мирного населения. Это область, в которой формируются намерения командиров, доктрины, тактика, методы противоборства, мораль, понятие сплоченности подразделений, уровень подготовки, опыт, понимание ситуации и общественное мнение.

Объектом информационного воздействия является множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе, но выгодных противнику. При этом под степенью поражения информационным оружием называют емкость той части объекта информационного

воздействия, которая либо уничтожена, либо работает на цели, чуждые собственной системе, но выгодные противнику /30/.

Для каждой сферы характерны свои объекты воздействия и средства поражения. Различают одиночные (отдельные военно-политические лидеры и др.) и групповые (массы народа и личного состава вооруженных сил) объекты информационного воздействия.

Средства воздействия также различают по характеру поражающих свойств. Это может быть высокоточное воздействие на определенных лиц, на избранный социальный срез общества или на определенный ресурс в информационно-вычислительной сети, а может быть и все население некоторого региона, а также вся его информационно-телекоммуникационная инфраструктура. При этом воздействие может быть разрушающим, манипулирующим или блокирующим.

В ходе информационно-психологической борьбы главными объектами воздействия и защиты являются психика личного состава вооруженных сил и населения противостоящих сторон, системы формирования общественного мнения и принятия решений. В ходе информационно-технической войны - информационно-технические системы (системы связи и управления, телекоммуникационные системы, радиоэлектронные средства, компьютерные сети и т.д.).

Совокупность методов и средств информационного воздействия на технику и людей рассматривается как информационное оружие.

В соответствие с видами информационной борьбы информационное оружие подразделяется на два основных вида: информационно-техническое и информационно-психологическое. Главными объектами информационного оружия первого вида является техника, второго – люди.

Информационно-техническое оружие включает в себя программно-математическое оружие.

Отдельно выделяют и психофизическое оружие. Психофизическое оружие - это совокупность всех возможных методов и средств (технотронных, суггестивных, психотропных, комплексных и др.) скрытого насильственного воздействия на подсознание человека с целью модификации

его сознания, поведения и физиологического состояния в нужном для воздействующей стороны направлении.

Психофизическое оружие представляет собой нарождающуюся ветвь информационно-психологического оружия /29/.

2.3. Информационная борьба. Информационное превосходство и информационные операции

Применение современного информационного оружия отражает историческую тенденцию перехода от войн с истреблением противника к войнам, ориентированным на деморализацию и социальную деградацию противника, без его уничтожения.

Еще великий китайский философ Сун Цзы говорил о том, что идеальная война – победить противника, не вступая с ним в открытое противоборство.

Информационное оружие может применяться задолго до начала боевых действий. Боевые действия могут вообще не планироваться, тогда как борьба за достижение целей противоборства реализуется средствами информационной войны. При этом имеется в виду, прежде всего, информационное воздействие на управляющие системы в государстве: военные, политические, экономические, духовные, социальные и т.д.

Понятие «информационная война» появилось в лексиконе военных специалистов в середине 80-х годов XX века в связи с новыми задачами вооруженных сил США после окончания «холодной войны». Оно стало широко упоминаться в прессе после проведения операции «Буря в пустыне» в 1991 году, где новые информационные технологии впервые были использованы как средство ведения боевых действий.

Официально же этот термин впервые введен в директиве министра обороны США от 21 декабря 1992 года и в директиве Комитета начальников штабов вооруженных сил США TS.3600.1. Детальное изложение и разъяснение он получил в Меморандуме № 30 (1993г.) Министерства обороны и Комитета начальников штабов вооруженных сил США.

Еще в конце 1996 года американский военный эксперт Роберт Банкер на одном из симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции «Force XXI»). В ее основу было положено разделение всего театра военных действий на две составляющих - традиционное пространство и киберпространство, причем последнее имеет более важное значение. Р. Банкер предложил доктрину «киберманевра», которая должна явиться естественным дополнением традиционных военных концепций, преследующих цель нейтрализации или подавления вооруженных сил противника.

Таким образом, в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса была включена и информационная сфера. Как подчеркивают эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психика противника (появился даже термин «human network»).

Рядом специалистов под информационной войной понимается комплексное воздействие на систему государственного и военного управления противостоящей стороны, на ее военно-политическое 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.

Можно также определить информационную войну как соперничество и организованные действия (информационные операции, Information Operations, IO) конфликтующих сторон в области информационных потенциалов, проводимые с целью снижения возможностей по использованию имеющегося государственного, военного и боевого потенциала противника и сохранения (повышения) возможностей по использованию собственного потенциала.

Рисунок 15 Соотношение и роль различных видов информационных операций

Информационная война состоит из действий, предпринимаемых для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

Способность не только реагировать, но и предвидеть проблемы до того, как они достигнут кризисной точки – та способность, которую стремятся приобрести США в ближайшем будущем. При этом они ориентируются на системы и средства, позволяющие резко снизить в начальной стадии конфликта (или до его начала) функциональные возможности противодействия государства-противника путем проведения наступательных информационных операций. Основной целью таких операций является достижение информационного превосходства над противником.

Информационное превосходство в руководящих документах армии США определяется как способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое. Оно может быть также определено и как способность назначить и поддерживать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать во все время ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях.

Информационное превосходство позволяет иметь реальное представление о боевой обстановке и дает интерактивную и высокоточную картину действий противника и своих войск в реальном масштабе времени. Информационное превосходство является инструментом, позволяющим командованию в решающих операциях применять широко рассредоточенные построения разнородных сил, обеспечивать защиту войск и ввод в сражение группировок, состав которых в максимальной степени соответствует задачам, а также осуществлять гибкое и целенаправленное материально-техническое обеспечение.

Информационная война ведется путем проведения мероприятий направленных против систем управления и принятия решений (Command &

Control Warfare, C2W), а также против компьютерных и информационных сетей и систем (Computer Network Attack, CNA).

Деструктивное воздействие на системы управления и принятия решений достигается путем проведения психологических операций (Psychological Operations, PSYOP), направленных против персонала и лиц, принимающих решения и оказывающих влияние на их моральную устойчивость, эмоции и мотивы принятия решений; выполнения мероприятий по оперативной и стратегической маскировке (OPSEC), дезинформации и физическому разрушению объектов инфраструктуры.

Рис. 3. Компоненты информационных операций (по материалам иностранной печати)

Существующая в настоящее время концепция информационной войны предусматривает:

- подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления);
- электромагнитное воздействие на элементы информационных и телекоммуникационных систем (известное как радиоэлектронная борьба);
- получение разведывательной информации путем перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также по побочным излучениям и за счет специального внедрения технических средств перехвата информации;
- осуществление несанкционированного доступа к информационным ресурсам (путем использования программно-аппаратных средств прорыва систем защиты информационных и телекоммуникационных систем противника) с последующим их искажением, уничтожением или хищением, либо нарушение нормального функционирования этих систем;
- формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения;

- получение интересующей информации путем перехвата и обработки открытой информации, передаваемой по незащищенным каналам связи, циркулирующей в информационных системах, а также публикуемой в открытой печати и средствах массовой информации.

В качестве основных объектов воздействия в ходе информационных операций выступают:

- сети связи и информационно-вычислительные сети, используемые государственными организациями при выполнении своих управленческих функций;
- военная информационная инфраструктура, решающая задачи управления войсками;
- информационные и управляющие структуры банков, транспортных и промышленных предприятий;
- средства массовой информации (в первую очередь – электронные).

Ряд специалистов отмечает, что применение информационного оружия это информационная технология, включающая в себя /30/:

- анализ способов и механизмов активизации у конкретной системы – противника, заложенных в нее программ самоуничтожения;
- поиск программы самоуничтожения;
- разработка конкретного информационного оружия;
- применение информационного оружия по заданному объекту.

Поскольку информационная война связана с вопросами информации и коммуникаций, то это есть борьба за знания - за то, кому известны ответы на вопросы: что, когда, где, почему и насколько надежным считает отдельно взятая страна и ее армия свои знания о себе и своих противниках. При этом средства ведения информационной войны или «информационное оружие» есть само использование информации и информационных технологий для воздействия на военные и гражданские системы с целью достижения информационного превосходства над противником.

Согласно опубликованным материалам, ряд специалистов дают такое определение информационным операциям. Информационная операция – это

комплекс взаимосвязанных по цели, месту и времени мероприятий и акций, направленных на инициализацию и управление процессами манипулирования информацией, с целью достижения и удержания информационного превосходства путем воздействия на информационные процессы в информационных системах противника. При этом информационные системы рассматриваются в широком смысле, т.е. не только автоматические и автоматизированные технические системы, но и государство и общество, которые тоже рассматриваются как информационные системы.

Информационные операции есть основа ведения информационной войны. Информационные операции являются самостоятельным видом оперативного обеспечения, который реализует на поле боя концепцию информационной войны. По целям и задачам информационные операции подразделяются на *информационное обеспечение*, *специальные информационные операции* и, собственно, *информационное противоборство*. При этом по характеру решаемых задач информационные операции могут быть *оборонительными* и *наступательными*.

Наступательные информационные операции включают в себя следующие мероприятия по достижению и удержанию информационного превосходства:

- оперативная безопасность;
- дезинформация;
- психологические операции;
- радиоэлектронное противоборство;
- физическое разрушение и уничтожение объектов информационной инфраструктуры;
- атаки на компьютерные сети противника.

Целью наступательных информационных операций является достижение и удержание информационного превосходства в ходе информационной войны.

Оборонительные информационные операции включают следующие мероприятия по обеспечению безопасности собственных информационных ресурсов:

- оперативная безопасность;
- физическая защита объектов информационной инфраструктуры;
- контрпропаганда;
- контрдезинформация;
- контрразведка;
- радиоэлектронная борьба.

Целью оборонительных информационных операций является обеспечение выполнения целевых задач информационными и управляющими системами в условиях ведения информационной войны, а также обеспечение сохранности информационных ресурсов и предотвращения утечки, искажения, утраты или хищения информации в результате несанкционированного доступа к ней со стороны противника.

Ряд экспертов подчеркивает, что эффективность сдерживания проецирования силы и других стратегических концепций в большой степени зависит от способности США влиять на восприятие и решения правительства других стран. Во время кризисов информационные операции могут помочь сдержать противника от проведения акций, приносящих ущерб США и их союзникам.

Следовательно, заключают специалисты, на *национально-стратегических и военно-стратегических уровнях* информационные операции как в мирное время, так и информационные боевые действия в кризисные или конфликтные периоды требуют высокой степени координации между правительственными структурами, включая министерство обороны и разведсообщество.

2.4. Определение информационного воздействия и информационного оружия

2.4.1. Обеспечивающее и атакующее информационное оружие

Возможности средств ведения информационной войны все время возрастают с ростом возможностей и распространением микропроцессоров, высокоскоростных систем передачи данных и информационных технологий в целом. По словам одного американского военного, сегодня унция кремния может сделать больше, чем килограмм урана.

Согласно ряду исследований информационное воздействие или информационное нападение представляет собой наступательную составляющую информационной войны и реализуется посредством наступательных информационных операций.

Информационное оружие - это совокупность специально организованной информации, информационных технологий, позволяющая целенаправленно изменять (уничтожать, искажать), копировать, блокировать информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование носителей информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей, применяемая в ходе информационной борьбы для достижения поставленных целей.

Средства, используемые в качестве информационного оружия, называются средствами информационного воздействия (СИВ), а для нашего случая – это средства специального программно-математического воздействия (ССПМВ).

Под средством специального программно-математического воздействия понимается некоторая самостоятельная программа (набор инструкций), которая способна выполнить любое непустое подмножество перечисленных ниже функций /28/.

1. Скрывать признаки своего присутствия в программно-аппаратной среде системы.

2. Обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти.

3. Разрушать (искажать произвольным образом) код программ в оперативной памяти.

4. Сохранять фрагменты информации из оперативной памяти в некоторой области внешней памяти прямого доступа (локальной и удаленной).

5. Искажать, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

6. Подавлять информационный обмен в телекоммуникационных сетях, фальсифицировать информацию в каналах государственного и военного управления.

7. Нейтрализовывать работу тестовых программ и систем защиты информационных ресурсов.

При этом под *самодублированием* понимается процесс воспроизведения своего собственного кода в оперативной или внешней памяти системы.

Ассоциирование с другой программой - интеграция своего кода, либо его части в код другой программы таким образом, чтобы при некоторых условиях управление передавалось на код программы с потенциально опасными последствиями.

По цели использования информационное оружие делят на *обеспечивающее* и *атакующее*.

Обеспечивающим называется информационное оружие, с помощью которого оказываются информационные воздействия на средства защиты информации атакуемой системы.

В состав обеспечивающего информационного оружия входят:

средства компьютерной разведки;

средства преодоления системы защиты.

Успешное применение обеспечивающего информационного оружия позволяет осуществлять деструктивные воздействия на хранимую, обрабатываемую и передаваемую в системе информацию с использованием атакующего информационного оружия.

Атакующим называется информационное оружие, с помощью которого осуществляется воздействие на хранимую, обрабатываемую и передаваемую в системе информацию, нарушающее применяемые информационные технологии.

В составе атакующего информационного оружия выделяют четыре основных вида средств информационных воздействий:

средства нарушения конфиденциальности информации;

средства нарушения целостности информации;

средства нарушения доступности информации;

средства психологических воздействий на абонентов информационной системы.

Применение атакующего информационного оружия направлено на срыв выполнения информационной системой целевых задач.

По способу реализации информационное оружие можно разделить на три больших класса:

математическое (алгоритмическое);

программное;

аппаратное.

Информационное оружие, относящееся к разным классам, может применяться совместно, а также некоторые виды информационного оружия могут нести в себе черты нескольких классов.

Специфика данной работы состоит в том, что, рассматривая все три класса информационного оружия, основной акцент делается на защиту от алгоритмического и программного информационного оружия.

К *алгоритмическому* информационному оружию будем относить:

алгоритмы, использующие сочетание санкционированных действий для осуществления несанкционированного доступа к информационным ресурсам;

алгоритмы применения санкционированного (легального) программного обеспечения и программные средства несанкционированного доступа для осуществления незаконного доступа к информационным ресурсам.

К *программному* информационному оружию будем относить программы с потенциально опасными последствиями своей работы для информационных ресурсов системы.

Средства специального программно-математического воздействия подразделяются на следующие классы: *компьютерные вирусы, средства несанкционированного доступа* и *программные закладки*.

2.4.2. Виды атакующего и обеспечивающего информационного оружия

В настоящее время известен широкий спектр ССПМВ, который включает в себя компьютерные вирусы, «троянских коней», сетевых червей и др. Все они перечислены ниже с описанием основных характеристик.

Компьютерный вирус (КВ) - это программа, обладающая способностью к скрытому размножению в среде используемой операционной системы путем включения в исполняемые или хранящиеся программы своей, возможно модифицированной копии, которая сохраняет способность к дальнейшему размножению.

Первые исследования саморазмножающихся искусственных конструкций проводились в середине нынешнего столетия. В работах фон Неймана, Винера и других авторов дано определение и проведен математический анализ конечных автоматов, в том числе и самовоспроизводящихся. Термин "компьютерный вирус" появился позднее, официально считается, что его впервые употребил сотрудник Лехайского университета (США) Ф. Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США.

Заражая программы, вирус может распространяться по компьютерной системе или сети обмена информацией, используя полномочия пользователей для заражения их же программ.

Рисунок 16 Классификация средств информационно-технического воздействия

Для использования компьютерных вирусов в качестве программного модуля системы информационного воздействия принципиальное значение имеют следующие классификационные признаки вирусов /28/:

- объект воздействия (заражения);
- способ заражения объекта;
- принцип маскировки;
- деструктивные возможности.

Особенностью КВ является его ненаправленность на конкретные программы и также то, что основным свойством является самодублирование вируса. Разрушение информации вирусом не направлено на конкретного рода программы и встречается не более чем у 10% такого рода программ.

Таким образом, КВ способны размножаться, внедряться в программы, передаваться по линиям связи, сетям обмена информацией, выводить из строя системы управления и т.п.

Средства несанкционированного доступа (СНСД) - это класс программ с потенциально опасными последствиями, обязательно выполняющий функции 3-5, 7.

К СНСД относится всевозможное штатное программное обеспечение системы, которое противник может использовать для нарушения целостности операционной системы или вычислительной среды. Часто этот тип программного обеспечения используется для анализа систем защиты, с целью их преодоления и реализации НСД к информационным ресурсам системы.

Программные закладки (ПЗ) - класс программ с потенциально опасными последствиями, обязательно выполняющий функции 3-5.

Отличительный признак между средствами несанкционированного доступа и программными закладками - это наличие для первых и отсутствие для вторых функции преодоления защиты.

Выделяют несколько видов ПЗ: троянская программа, логическая бомба, логический люк, программная ловушка, программный червь.

Троянская программа - программа, имеющая законный доступ к системе, но выполняющая и скрытые (необъявленные) функции.

Логическая бомба - программа, осуществляющая злоумышленные действия при выполнении ряда определенных логических условий.

В качестве примера логических бомб можно назвать программные закладные устройства, заранее внедряемые в информационно-управляющие центры военной инфраструктуры, чтобы по сигналу или в установленное время привести их в действие.

Логический люк - механизм внутри операционной системы (программного обеспечения), позволяющий программе злоумышленника получить привилегированную функцию или режим работы (которые ему не были разрешены).

Логическими люками могут быть различного рода ошибки, сознательно вводимые злоумышленниками в программное обеспечение объекта.

Программная ловушка - программа, использующая ошибки или неоднозначности в программном обеспечении.

Программный червь - программа, маскирующаяся под системные средства поиска свободных вычислительных ресурсов в сети.

Сетевым червем называется компьютерный вирус, обладающий свойством самостоятельного распространения в системе и заражающий ее элементы, функциональные сегменты либо систему целиком.

Универсальность, скрытность, многовариантность форм программно-аппаратной реализации, радикальность воздействия, достаточный выбор времени и места применения, наконец, экономичность делают информационное оружие чрезвычайно опасным: оно легко маскируется под средство защиты и даже позволяет вести наступательные действия анонимно.

2.4.3. Особенности и основные характеристики атакующего информационного оружия

Существует ряд особенностей, определяющих качественное отличие информационного оружия от других видов вооружений. К ним относятся:

- универсальность;
- скрытность;
- экономическая эффективность;
- возможность применения для решения широкого круга задач;
- масштабность применения;
- обладание эффектом “цепной реакции”;
- сложность осуществления международного контроля за разработкой и применением.

Универсальность. Виды информационного оружия и способы его применения не зависят от климатических и географических особенностей возможных театров военных действий, состояния инфраструктуры (например, состояния дорог и мостов) и т.п.

Скрытность. При подготовке к агрессии одного государства против другого (с которым имеется общая граница) с применением традиционных средств необходимо:

- иметь мощный экономический потенциал;
- провести мобилизацию;
- создать группировку войск, способную выполнить поставленные задачи;
- нанести внезапный сокрушительный удар по противнику.

Перечисленные условия противоречат друг другу: возможности современной разведки таковы, что практически невозможно скрыть от предполагаемого противника процессы мобилизации и концентрации войск в приграничных районах. Следовательно, противник в ответ также начнет мобилизацию и концентрацию войск, и внезапного удара не получится. В то же время, для нанесения внезапного сокрушительного удара армии мирного времени недостаточно, а содержание в мирное время армии военного времени приведет к разорению государства, подрыву его экономики.

Применение информационного оружия позволяет снять указанные противоречия.

Схему вступления в войну государства, обладающего информационным оружием, можно обобщенно представить следующим образом:

- скрытая подготовка и внезапное проведение широкомасштабных долговременных информационных воздействий на систему противника. Атаки осуществляются на системы различного назначения (государственные, военные, управления транспортом, системы финансовых учреждений, системы энергообеспечения и т.п.) с целью лишения противостоящей стороны возможности принятия управленческих решений. Одновременно ведется психологическая война с использованием информационных воздействий население;

- армия мирного времени сосредотачивается на границе, переформировывается в первый стратегический эшелон и начинает захват территории противника. Одновременно объявляется мобилизация, действующая армия доукомплектовывается, формируются второй и

последующие стратегические эшелоны, которые завершают захват территории противника.

При отсутствии общей границы между противоборствующими сторонами захват территории противника может осуществляться подразделениями быстрого реагирования.

Отметим еще две особенности представленной схемы вступления государства в войну:

а) сложность оперативного определения истинного агрессора для принятия контрмер;

б) отсутствие, в общем случае, необходимости наличия общей границы между противоборствующими сторонами.

Экономическая эффективность. По предварительным оценкам, разработка и применение информационного оружия требуют, по сравнению с другими видами вооружений, существенно меньших затрат. Очевидно, что разработка и размножение средств информационного воздействия значительно дешевле создания и серийного производства традиционных видов вооружения (бронетанковой техники, ракетно-космической техники и др.).

Возможность применения информационного оружия для решения широкого круга задач. Информационное оружие может быть использовано не только в первом внезапном ударе, но и для решения стратегических, оперативно-тактических и тактических задач на поле боя. Например, информационное оружие может применяться для осуществления воздействий на средства связи и управления батальоном, ротой и взводом, психологических и физических воздействий на отдельных субъектов.

Масштабность применения. С использованием информационного оружия возможно осуществление воздействий на стационарные и мобильные элементы системы наземного, морского, воздушного и космического базирования.

Обладание эффектом “цепной реакции”. Воздействия на единичный элемент системы могут привести к выводу из строя других элементов, сегментов и системы целиком.

<u>Сложность осуществления международного контроля.</u> Факты производства и испытаний информационного оружия, а также используемые для этого технические и программные средства могут быть надежно скрыты от разведок других государств, различных международных организаций, их контролирующих органов.

Приведенные характеристики позволяют говорить об информационном оружии, как о качественно новом виде вооружений.

2.5. Распределенные атаки с отказом в обслуживании – наиболее характерный и наиболее опасный тип информационной атаки на компьютерные сети

Один из многочисленных видов удаленных атак на компьютерные системы известен как «атака с отказом в обслуживании» (Denial-of-Service, DoS). Данный тип нападения имеет целью не допустить доступ законных пользователей к ресурсам информационной системы. Традиционные атаки отказа в обслуживании используют ошибки в программном обеспечении, связанные с переполнением буфера, истощения ресурсов системы или эксплуатируют дефекты системы, в результате чего система «валится» и некоторое время необходимо на ее восстановление.

Летом 1999 года был зарегистрирован новый тип нападения на информационные системы с использованием сети Интернет. Он получил название «распределенная атака с отказом в обслуживании» (Distributed Denial of Service, DDoS). Ряд известных интернет-сайтов был успешно атакован с использованием этого типа нападения.

Распределенная атака с отказом в обслуживании использует множество вычислительных машин, работающих совместно, и воздействующих на сеть или участок сети, выбранный в качестве мишени. Мало что можно сделать, если информационная система стала мишенью для DDoS атаки. Природа этих нападений порождает так много дополнительного трафика в сети, что сеть оказывается перегруженной, и нет возможности заблокировать враждебные пакеты данных.

Ввиду повышенной опасности данный вид атаки на компьютерные системы в течение длительного времени являлся предметом исследования

многих лабораторий, занимающихся вопросами обеспечения защиты информации. Одно из наиболее детальных исследований, проведенных в Национальной лаборатории Лоуренса Ливермора Министерства энергетики США, было опубликовано в феврале 2000 года.

Большинство из существующих сегодня средств организации DDoS-атак основано на одной и той же базовой концепции и топологии. Подчеркнем, что эти инструменты не используются для захвата данных или проникновения в компьютерную систему. Они используются исключительно для разрушения нормального трафика в районе узла-мишени.

Данные нападения чрезвычайно трудно проследить в силу реализованных в инструментах приемах маскировки их деятельности, о чем мы расскажем подробнее чуть ниже. Ряд утилит использует шифрование с целью скрыть их коммуникации, а также изменяют их исходные адреса, что позволяет скрыть их истинное местоположение.

Как правило, средства организации DDoS-атак управляются удаленно. Если администратор сайта, подвергшегося нападению, сможет проследить адреса агентов, то для выхода на инициатора нападения ему необходимо будет также проследить трафик до узла-руководителя, и только после этого он сможет выйти на нападающего.

DDoS-атаки включают две стадии. Как правило, противник затрачивает значительное время при подготовке к проведению первой стадии нападения.

Рисунок 17 Первая фаза атаки

Эта стадия нападения заключается в поиске и компрометации как можно большего количества компьютеров. Нападающий нуждается в большом количестве компьютеров, чтобы затем сгенерировать мощные потоки фиктивных пакетов данных, необходимых для «затопления» выбранной мишени.

Рисунок 18 Вторая фаза DDoS-атаки

Таким образом, нападающий должен найти множество компьютерных систем со слабой защитой, чтобы скрытно проникнуть в них и установить необходимый DDoS-инструментарий, а также скрыть присутствие этих средств.

Вторая стадия этого нападения не может быть реализована до тех пор, пока не будет скомпрометировано достаточно много машин для формирования мощного потока ложных пакетов.

Именно вторая стадия - фактическое осуществление нападения с отказом в обслуживании. Компрометированные системы порождают атакующий трафик в сети с целью заблокировать нормальную работу целевого сайта или подсети. Сами эти скомпрометированные системы рассматриваются вторичными жертвами нападения.

Порожденный трафик использует TCP-протокол. Цель, на которую обрушивается этот поток, не может сразу обработать все поступающие пакеты, и распределяет под их последующую обработку некоторый ресурс. В конечном счете, это приводит к полному истощению ресурсов и блокировке системы, что и является целью атаки. Во множестве случаев вообще не имеет значения, как обрабатываются пакеты, поскольку объем пакетов настолько большой, что сама сеть переполняется порожденным трафиком, что не позволяет проходить законному трафику.

Архитектура распределенной атаки с отказом в обслуживании состоит из четырех уровней. Компрометированные системы играют роль «руководителей» групп «агентов» и самих агентов. Агенты - это собственно те компьютеры, где порождается атакующий поток пакетов. Один или более руководителей управляют этими агентами. Руководители поддерживают список всех агентов. Руководители также сигнализируют агентам, когда начать нападение и определяют метод нападения. Нападающий управляет одним или более руководителями, а каждый агент может ответить на запрос больше чем одному руководителю. Существует общее название для скомпрометированных в ходе подготовки DDoS-атаки компьютеров – «зомби».

Рисунок 19 Структура распределенной атаки

Наиболее важный аспект распределенных нападений - то, что нападающий нуждается в компрометированных компьютерных системах для реализации нападения. Если Интернет, как сообщество, будет уверено, что каждая из его подсетей безопасна, то не будет места для злоумышленников, размещающих свои инструменты в плохо поддерживаемых системах.

2.6. Системы обнаружения информационных атак на компьютерные сети – оборонительное информационное оружие

По мнению ряда российских и зарубежных специалистов, системы обнаружения вторжений в компьютерные сети сегодня являются одним из рубежей обороны в киберпространстве. Сама технология обнаружения вторжения достаточно молода и динамична. Сегодня происходит активное формирование рынка систем - одни производители поглощают других. В силу весьма динамичных процессов любая информация о системах обнаружения вторжений быстро устаревает, что делает весьма затруднительным подготовку сравнительного анализа технических характеристик систем этого класса. Так, представленный компанией Staniford-Chen обзор, включающий краткое описание 42 продуктов, связанных с обнаружением вторжения, уже серьезно устарел, так как произошло достаточно много изменений с момента его публикации (зима 1997-1998 года). Другой список продуктов расположен в Интернет (на сайте SANS/NSA), что делает его более достоверным, поскольку он постоянно модифицируется и дополняется.[6]

Обнаружение вторжений остается областью активных исследований уже в течение двух десятилетий. Считается, что начало этому направлению было положено в 1980 году изданием статьи Джеймса Андерсона «Мониторинг угроз компьютерной безопасности»[7]. Несколькими годами позже (в 1987) это направление было развито публикацией оригинальной статьи «О модели

---

[6] Stocksdale, Gregory. (National Security Agency). *SANS/NSA Intrusion Detection Tools Inventory*. WWW: <URL: http://www.sans.org/NSA/idtools.htm>.

[7] Anderson, James P. *Computer Security Threat Monitoring and Surveillance*. Fort Washington, PA: James P. Anderson Co..

обнаружения вторжения» Дороти Деннинг[8]. Эта статья обеспечила методологическую основу, которая вдохновила многих исследователей и заложила основу для создания коммерческих продуктов в области обнаружения вторжений.

2.6.1. Обзор характеристик экспериментальных систем обнаружения информационных атак

Исследования по обнаружению вторжения, выполненные в начале 90-ых годов, породили целый ряд новых инструментальных средств[9]. Однако большинство из них были разработаны студентами только с целью исследовать базовые концепции теоретического подхода и после того, как авторы заканчивали обучение, эти инструментальные средства более не поддерживались. Вместе с тем они серьезно повлияли на выбор направления последующих исследований и разработок. Ранние разработки в основном базировались на применении централизованной архитектуры систем обнаружения вторжений, но в силу взрывного роста количества телекоммуникационных сетей разного назначения, более поздние усилия были сконцентрированы на системах с сетевой архитектурой.

Описанные ниже средства отражают направление активных исследований в области обнаружения вторжений.

Первый два продукта: EMERALD и NetSTAT, сформировались на базе сходных подходов. Третий инструмент – Bro, является уникальным продуктом для изучения проблемы проникновения в сеть с использованием попыток перегрузки или дезинформации системы обнаружения вторжения.

EMERALD

EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) - самый современный инструмент в своем классе, разработанный компанией SRI. Эта линия инструментальных средств создавалась для исследования проблем в обнаружении вторжения, связанные как с обнаружением отклонений от нормального пользовательского поведения (аномалии), так и определение характерных «образов» вторжения

---

[8] Denning, Dorothy E. (SRI International). “An Intrusion Detection Model.” *IEEE Transactions on Software Engineering (SE-13)*, 2 (February 1987): 222-232.

[9] Mukherjee, Biswanath; Heberlein, L.Todd; & Levitt, Karl N. (University of California, Davis). “Network Intrusion Detection.” *IEEE Network 8*, 3 (May/June 1994): 26-41. WWW: <URL: http://seclab.cs.ucdavis.edu/papers.html>.

(сигнатуры). Первые работы SRI в области обнаружения вторжения начались в 1983 году, когда был разработан уникальный статистический алгоритм, способный различить различия в пользовательском поведении[10].

Несколько позже реализация подсистемы анализа сигнатур вторжения была дополнена экспертной системой P-BEST[11]. Результаты исследований были реализованы в одной из ранних версий системы обнаружения вторжения компании SRI - IDES[12]. Данная система способна контролировать действия пользователей, подключенных к нескольким серверам, в реальном масштабе времени. Основываясь на опыте, полученном в результате проведенных исследований, в 1992 – 1994 годах был создан уже коммерческий продукт NIDES[13]. Подобно IDES, этот инструмент был предназначен для защиты отдельных серверов (host-based), и использовал экспертную систему P-BEST. Однако создатели системы пошли несколько дальше, добавив к системе компонент «Resolver», который способен объединять результаты статистического анализа и анализа сигнатур. Интерфейс пользователя в NIDES был также существенное усовершенствование по сравнению с интерфейсом пользователя в IDES.

Следующей системой, созданной этой командой разработчиков, стала система EMERALD. Она основывается на результатах ранних экспериментов с системами IDES/NIDES, но на сей раз сосредотачивается на обеспечении безопасности сетевых сегментов (network-based). Главная цель, для которой и разрабатывался этот продукт, состоит в том, чтобы решать проблемы обнаружения вторжений в больших гетерогенных сетях. Такие среды более трудны для контроля и анализа в силу распределенного характера поступающей информации.

---

[10] Anderson, Debra, et al. (SRI International). *Detecting Unusual Program Behavior Using the Statistical Component of the NextGeneration Intrusion Detection Expert System (NIDES)* (SRICSL-95-06). Menlo Park, CA: Computer Science Laboratory, SRI International, May 1995. WWW: <URL:http://www.sdl.sri.com/nides/index5.html>.

[11] Lindqvist, Ulf & Porras, Phillip A. “Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST).” *Proceedings of the 1999 IEEE Symposium on Security and Privacy.* Oakland, CA, May 9-12, 1999. WWW: <URL: http://www2.csl.sri.com/emerald/pbest-sp99-cr.pdf>.

[12] Lunt, Teresa F., et al. (SRI International). *A Real-Time Intrusion Detection Expert System (IDES).* WWW: <URL: http://www2.csl.sri.com/nides.index5.html>.

[13] Anderson, Debra; Frivold, Thane; & Valdes, Alfonso. (SRI International). *Next-Generation Intrusion Detection Expert System (NIDES), A Summary* (SRI-CSL-95-07). Menlo Park, CA: Computer Science Laboratory, SRI International, May 1995. WWW: <URL: http://www.sdl.sri.com/nides.index5.html>.

EMERALD объединяет пользователей в совокупность независимо управляемых доменов. Каждый домен обеспечивает необходимый набор сетевых сервисов. В каждом домене реализуется индивидуальная политика безопасности, причем отдельные домены могут иметь доверенные отношения с другими доменами. В этом контексте ориентация на одно централизованное хранилище для централизованного хранения и обработки поступающей информации ведет к существенной деградацией эффективности системы в целом, что и послужило основным мотивом в создании системы EMERALD, для которой характерен лозунг «разделяй и властвуй».

Иерархический подход обеспечивает три уровня анализа, выполненного тройственной системой мониторов: мониторы сервисов, мониторы домена и мониторы окружения. Эти мониторы имеют общую базовую архитектуру, набор анализаторов профилировщика (для обнаружения аномалий), анализаторов сигнатуры (для анализа сигнатуры), и resolver-компонента, которая интегрирует результаты, сгенерированные от анализаторов двух предыдущих уровней. Каждый модуль содержит объекты ресурсов, что обеспечивает библиотеку с перестраиваемой конфигурацией информации, позволяющей настраивать компоненты модуля к конкретному приложению. Сами ресурсы могут многократно использоваться в нескольких мониторах EMERALD. На самом низком уровне, мониторы сервисов поддерживают обнаружение вторжения для индивидуальных компонентов и сетевых услуг в пределах одного домена, анализируют данные (файлы регистрации действий, событий и т.д.), выполняют анализ локальных сигнатур и статистические исследования. Мониторы домена интегрируют информацию от сервисных мониторов, с целью обеспечить более детальное представление вторжения в масштабах всего домена, в то время как мониторы окружения выполняют анализ междоменной области, чтобы оценить угрозы, исходящие от этой части сети. Наличие возможности организовывать виртуальные каналы связи на основе подписки позволяет различным мониторам сервисов связываться друг с другом.

Предшествующая работа с NIDES продемонстрировала, что статистические методы могли быть эффективны как с пользователями, так и с прикладными программами. Однако контроль прикладных программ

(например, анонимный ftp), был особенно эффективен, так как для анализа требовалось меньшее количество прикладных профилей. Именно поэтому в EMERALD была реализована методика профилирования, обобщающая понятие «профиля анализа», в которой управление профиля отделено от анализа.

Относительно анализа сигнатуры. Анализаторы сигнатуры сервисного уровня контролируют компоненты домена с целью обнаружения заранее описанных последовательностей действий, приводящих к нештатным ситуациям. Анализатор сигнатуры в мониторах более высокого уровня фильтрует эту информацию, чтобы оценить – существует ли нападение более широкого уровня. В дополнение к интегрированию следствий статистического анализа и анализа сигнатуры, решающая компонента (resolver) обеспечивает ряд дополнительных функций, которые позволяют встраивать в среду EMERALD анализаторы, разработанные сторонними фирмами.

Работы по созданию системы EMERALD еще не завершены, вместе с тем, это одно из перспективных направлений создания систем обнаружения вторжений нового поколения. Поскольку противник становится все более искушенным в организации вторжений, следует ожидать, что он будет стремиться рассеивать следы своего присутствия по всей сети, сводя к минимуму возможность обнаружения его присутствия. В таких ситуациях способность собирать, обобщать и анализировать информацию, исходящую от разнообразных источников в реальном времени становится главным свойством системы обнаружения вторжений.

По мнению ряда экспертов, гибкость масштабируемой архитектуры EMERALD, ее способность расширять функциональные возможности с помощью дополнения внешних инструментальных средств, делает EMERALD предшественником будущих инструментальных средств обнаружения вторжения. Однако управление и поддержка инфраструктуры системы и ее информационной основы в виде базы знаний для экспертной системы может потребовать существенных усилий и затрат.

NetStat

NetStat последний продукт из линии инструментальных средств "STAT", созданных в калифорнийском университете в Санта-Барбаре. Исследования по проекту STAT, начатые в начале 90-ых сосредоточены на использовании анализа состояний системы и процессов перехода в них системы с целью обнаружения вторжений в реальном масштабе времени.[14] Подход основан на предпосылке, что некоторые последовательности действий, описывающие неправомочное действие и однозначно указывающие нарушителя, переводят систему из начального санкционированного состояния в другое - несанкционированное.

Большинство централизованных систем обнаружения вторжения в категории аномалии анализируют доказательство вторжения в контрольном следе на компьютере. Однако в подходе STAT контрольная информация следа преобразована через «аудит следа анализатора», который фильтрует и обобщает информацию, собранную на уровне аудита следа. Данные абстракции, которые являются более подходящими для анализа, называются «сигнатурами» и являются самым важным элементом в подходе STAT. Последовательность действий, описанная сигнатурой, перемещает систему через ряд состояний, каждое из которых все ближе подводит систему к несанкционированному состоянию. Последовательности вторжения определены посредством переходов между состояниями, которые зафиксированы в наборах продукционных правил.

Первоначально метод был реализован в UNIX-системе USTAT[14], предназначенной для защиты отдельных серверов. Основными блоками USTAT являются:

- препроцессор;
- база знаний (который включил базу фактов и базу правил);
- блок вывода;
- решатель;

Препроцессор фильтрует и упорядочивает данные в форму, которая выполняет роль независимого контрольного файла системы.

[14] Kemmerer, Richard A., et al. (University of California, Santa Barbara). *STAT Projects.* WWW: <URL: http://www.cs.ucsb.edu/~kemm/netstat.html/projects.html>

База правил, как часть базы знаний, хранит правила перехода между состояниями, которые указывают предопределенные последовательности вторжения, в то время как база фактов хранит описание динамически изменяющихся состояний системы относительно возможных текущих вторжений.

Во вновь полученной информации, интегрированной препроцессором с описанием текущего состояния системы, согласно определению в базе фактов, блок вывода идентифицирует любые существенные изменения в состоянии и обновляет базу фактов.

Блок вывода также уведомляет решатель о возможных нарушениях защиты. Решатель в свою очередь или уведомляет администратора безопасности сайта о ситуации, или инициализирует действие на его собственное усмотрение. Одно преимущество данного подхода состоит в том, что нападение может быть выявлено и ему будет организовано противодействие еще до достижения системой скомпрометированного состояния.

Данный подход на основе описания состояний использует таблицу блока вывода, для отслеживания каждого возможного вторжения, что позволяет USTAT идентифицировать скоординированное нападение, исходящее из множества источников. Это может быть сделано после того, как последовательности нападения определены, не через последовательность действий нападающего, а через последовательность переходов между состояниями системы. Таким образом, если два нападения приводят в одно и тоже состояние системы, каждое из их последующих действий может быть отражено как ветвление в предыдущей последовательности состояний. Это разветвление осуществляется путем дублирования строк в таблице блока вывода, каждая строка которой, представляет различные последовательности нападения.

NSTAT[15] является естественным преемником USTAT. Система NSTAT ориентирована на поддержку обнаружения вторжений в сети серверов, у которых единая распределенная файловая система. В этом случае, действия

[15] Kemmerer, Richard A. (University of California, Santa Barbara). *NSTAT: A Model-Based Real-Time Network Intrusion Detection System* (TRCS97-18). November 1997.WWW: <URL:http://www.cs.ucsb.edu/~kemm/netstat.html/documents.html>

типа монтирования каталогов на одном сервере, могут влиять на другие машины в сети. Наличие одной централизованной системы позволяет эффективно обнаруживать нападения в случае, когда задействовано несколько серверов. В этом случае локальные системы обнаружения на серверах преобразовывают контрольные данные в формат NSTAT и объединяют их для анализа в один файл.

В настоящее время система NetStat[16] продолжает развиваться. Вносится ряд существенных изменений в архитектуру системы, что приводит к переориентации с обеспечения безопасности отдельных серверов на обеспечение безопасности сетевых сегментов. NetStat включает набор зондов, которые отвечают за обнаружение и оценку вторжений в тех подсетях, в которых они функционируют. Каждый зонд обеспечен фильтром данных с перестраиваемой конфигурацией, блоком вывода и решателем. Зонды могут действовать автономно. Если обнаружены компоненты вторжения, то информация о событии может быть отправлена другим заинтересованным зондам, которые подпишутся на информацию о подобных событиях, это позволит получать более полное понимание схемы вторжения. Этим способом могут быть идентифицированы разные подсети, которые участвуют в осуществлении вторжения.

Зонды связаны с анализатором - автономным инструментом, который поддерживает порождение и управление зондами. Анализатор состоит из базы фактов, база данных сценариев вторжения, основанных на состоянии системы, блока анализа и диспетчера программы конфигурации. Анализатор определяет, для которого события должны быть проверены данные, где они должны быть проверены, какая сетевая информация о топологии требуется, и др. Для выполнения этих действий используется информация об использовании сетевых ресурсов, которая располагается вместе с базой данных сценария. Эта информация затем передается составителю программы конфигурации, который в свою очередь генерирует конфигурацию зондов.

Bro

[16] Vigna, Giovanni & Kemmerer, Richard A. (University of California, Santa Barbara). “NetSTAT: A Network-Based Intrusion Detection Approach.” *Proceedings of the 14th Annual Computer Security Applications Conference.* Scottsdale, AZ, Dec. 1998 [online]. Available WWW: <URL: http://www.cs.ucsb.edu/~kemm/netstat.html/documents.html>.

Bro - исследовательский инструмент, разрабатываемый Национальной лабораторией им. Лоуренса Ливермора Министерства энергетики США. Система строится для исследования проблем, связанных с отказоустойчивостью систем обнаружения вторжения, то есть, для анализа, какие характеристики делают систему обнаружения вторжения способной к сопротивлению атакам против себя. Цели проекта Bro [17] включают:

- ***контроль перегрузки***. Способность обрабатывать большие объемы передачи данных без того, чтобы снижать пропускную способность. Нарушитель может использовать механизм перегрузки сети посторонними пакетами, для вывода из строя системы обнаружения вторжения. Такая ситуация может привести к тому, что система обнаружения вторжения будет вынуждена пропускать некоторые пакеты, к которым сеть уязвима.

- ***уведомление в реальном масштабе времени.*** Оно необходимо, для обеспечения своевременного информирования и подготовки ответных действий.

- ***механизм разделения***. Разделение фильтрации данных, идентификации событий и политики реагирования на события, обеспечивает более совершенный программный дизайн, простую эксплуатацию и обслуживание.

- ***масштабируемость системы***. Большое количество известных нападений, вместе с выявлением новых уязвимостей требует, чтобы система имела возможность быстро добавить новые сценарии нападения к ее внутренней библиотеке сценариев.

- ***способность противостоять нападениям***. Сложные сценарии вторжения непременно включают элементы воздействия и на систему обнаружения вторжений. Систсема должна противостоять подобным действиям.

Bro имеет иерархическую архитектуру с тремя уровнями функций. На самом низком уровне Bro использует утилиту libpcap для извлечения из сети пакетов с данными. Этот блок делает независимыми основные блоки анализа

[17] Paxson, Vern. (Lawrence Berkeley National Laboratory). “Bro: A System for Detecting Network Intruders in Real-Time,” *Proceedings of 7th USENIX Security Symposium.* San Antonio, TX, January 1998. WWW: <URL: http:// www.aciri.org/vern/papers.html>.

по обнаружению вторжения Bro от технических особенностей телекоммуникационной сети, в которой развернута система. Это также позволяет отклонять существенную долю пакетов на низком уровне. Таким образом libpcap, к примеру, может перехватывать все пакеты, связанные с прикладными протоколами (например, ftp, telnet и др.).

Следующий уровень - уровень события, выполняет проверки целостности по заголовкам пакетов. Если заголовок плохо сформирован, то будет сгенерировано событие о возможной проблеме. После этого запускается процедура проверки, чтобы определить, было ли полное содержание пакета зарегистрировано (обычно, если полный пакет был проанализирован), если только информация заголовка пакета была зарегистрирована (обычно, если только флажки TCP были проанализированы), или если ничто не было зарегистрировано (если никакая обработка не была сделана).

События, сгенерированные в результате этого процесса размещаются в очереди, которая опрашивается интерпретатором сценария политики. Сам сценарий постоянно находится на третьем уровне иерархии. Интерпретатор сценария политики написан на внутреннем языке Bro, который поддерживает строгую типизацию. Интерпретатор связывает значения случая с кодом для обработки этого случая и затем интерпретирует код.

Выполнение кода может закончиться генерацией дальнейших событий, регистрации уведомления в реальном масштабе времени или регистрации данных. Чтобы добавить новую функцию к возможностям к Bro, надо подготовить описание образа, идентифицирующего событие, и написать соответствующие обработчики событий, чтобы расширить функциональные возможности интерпретатора сценария политики. В настоящий момент Bro контролирует четыре прикладных сервиса: finger, ftp, portmapper и telnet.

Bro работает под несколькими вариантами ОС UNIX и используется как часть системы защиты Национальной лаборатории. Начиная с 1998 года, результатом функционирования Bro стало формирование 85 сообщений об инцидентах, переданных в CIAC и CERT/CC. Разработчики особо подчеркивают хорошие данные по производительности системы при обработке высокоскоростных потоков информации. Bro не испытывает

проблем с потерей пакетов в сети FDDI на скорости 25 Мбит/с, при пиковой производительностью до 200 пакетов в секунду.

2.6.2. Коммерческие системы обнаружения информационных атак

Коммерческие программы, описанные ниже, только небольшая часть всего множества продуктов, присутствующих на рынке[18, 6, 19]. Опубликован ряд отчетов, содержащих сравнительную оценку коммерческих продуктов[20, 21, 22, 23, 24]. Выбранные для описания могут рассматриваться в качестве классических образцов.

В отличие от экспериментальных программ, рассмотренных выше, коммерческие программы практически не имеют доступного объективного описания достоинств и недостатков особенно в части тестовых испытаний систем, что сильно затрудняет выбор нужной потребителю программы.

Для решения этой проблемы в настоящее время ведется разработка единого стандарта на тестирование систем обнаружения вторжений[25].

CMDST

Компьютерная система обнаружения неправильного употребления (CMDST) была первоначально разработана корпорацией Science Applications International[26, 27], однако теперь поддерживается и продается ODS Networks

---

[18] Sobirey, Michael. *Michael Sobirey's ID Systems Page*. WWW: <URL: http://www-rnks.informatik.tucottbus.de/~sobirey/ids.html>

[19] Information Assurance Technology Analysis Center. *Information Assurance Tools Report.* WWW: <URL: http://www.iatac.dtic.mil/iatools.htm>.

[20] Newman, David; Giorgis, Tadesse; & Yavari-Issalou, Farhad. *Intrusion Detection Systems: Suspicious Finds.* WWW: <URL: http://www.data.com/lab_tests/intrusion.html>

[21] Newman, David; Giorgis, Tadesse; & Yavari-Issalou, Farhad. *Intrusion Detection Systems: Suspicious Finds—II* . WWW: <URL: http://www.data.com/lab_tests/intrusion2.html>

[22] Newman, David; Giorgis, Tadesse; & Yavari-Issalou, Farhad. *Intrusion Detection Systems: Suspicious Finds—III* WWW: <URL: http://www.data.com/lab_tests/intrusion3.html>

[23] Scambray, Joel; McClure, Stuart; & Broderick, John. (InfoWorld Media Group Inc.). "Network Intrusion-Detection Solutions." *InfoWorld 20,* 18 (May 4, 1998). WWW: <URL: http://www.infoworld.com/cgi-bin/displayArchive.pl?/98/18/intrusa.dat.htm>.

[24] Phillips, Ken. (*PC Week*). *One if by Net, Two if by OS* . WWW: <URL:http://www.zdnet.com/products/stories/reviews/0,4161,389071,00.html>

[25] MIT Lincoln Laboratory. *DARPA Intrusion Detection Evaluation*. WWW: <URL: http://www.ll.mit.edu/IST/ideval/index.html>.

[26] Van Ryan, Jane. *SAIC's Center for Information Security Technology Releases CMDS Verson 3.5* .WWW: <URL: http://www.saic.com/news/may98/news05-15-98.html>.

[27] Proctor, Paul E. (SAIC). *Computer Misuse Detection System(CMDS) Concepts.* WWW: <URL: http://cpits-web04.saic.com/satt.nsf/externalbycat>.

Inc. [28]. Это – система, предназначенная для обеспечения безопасности серверов, которая ведет мониторинг иерархической сети машин. Система поддерживает статистическую и сигнатурную категории обнаружения и может генерировать отчеты о возможных тенденциях развития вторжения.

В категории анализа аномалий CMDS использует статистический анализ, чтобы идентифицировать образы поведения, которые отклоняются от нормальной пользовательской практики. Статистика формируется из таких категорий как:

- времена входа в систему/выхода из системы;
- запуск на выполнение прикладных программ;
- количество открытых файлов, измененных или удаленных;
- использование прав администратора;
- каталоги, используемые наиболее часто.

Профили пользовательского поведения обновляются каждый час работы системы. Они используются для проведения исследований по выявлению сомнительного поведения в каждой из трех категорий (вхождение в сет, выполнение программ и ознакомление с информацией). Вычисляются отклонения от ожидаемого (в течение часа) поведения, и, если отклонения выше порогового значения, то генерируется предупреждение.

Распознавание сигнатур поддержано экспертной системой CLIPS[29]. Факты, полученные из описания событий, имена, использованных объектов, и т.д. используются для представления правил в CLIPS.

CMDS определяет сигнатуры нападения на UNIX системы, связанные, например, с неудавшейся попыткой установления суперпользовательских полномочий, неудачей входа в систему, активностью отсутствующих пользователей и критической модификацией файлов. Каждое из подобных событий имеет эквивалентный набор определенных сигнатур и для операционной системы Windows NT.

---

[28] ODS Networks, Inc. *CDMS: Computer Misuse Detection System*. WWW: <URL: http://www.ods.com/security/products/cmds.shtml>

[29] Riley, Gary. *CLIPS: A Tool for Building Expert Systems*. WWW: <URL: http://www.ghg.net/clips/CLIPS.html>

NetProwler

Выпускаемая в настоящее время система NetProwler[30, 31, 32] связана с системой Intruder Alert от компании Axent. Компонент Intruder Alert поддерживает обнаружение вторжения на основе защиты серверов, в то время как NetProwler (ранее именовавшийся ID-Track от компании Internet Tools, Inc) поддерживает обнаружение вторжений в сегментах сетей. Основу NetProwler составляет то, что Axent называет процессом «динамического анализа полной сигнатуры». Этот метод обеспечивает средства для интеграции небольших порций информации, которая извлекается из сети, в более сложные события, что позволяет проверять события на совпадение с предопределенными сигнатурами в реальном масштабе времени, а также формировать новые сигнатуры. NetProwler имеет библиотеку сигнатур для широкого разнообразия операционных систем и различных типов нападений, что позволяет пользователям самим строить профили сигнатур, используя мастер определения сигнатуры. Таким образом, пользователи могут характеризовать нападения, которые составлены из отдельных событий, повторяющихся событий или целого ряда событий. Сигнатура нападения имеет четыре элемента: примитив поиска (образец строки), примитив значения (значение или диапазон значений), сохраненное ключевое слово (имя протокола) и операционная система или приложение, связанное с нападением.

NetProwler также поддерживает и возможность автоматизированного ответа. Он включает регистрацию сеанса, завершение сеанса, отправление по электронной почте событий на пульт администратора, информирование о событиях персонала через электронную почту или пейджер и ряд других средств.

NetRanger

---

[30] AXENT Technologies, Inc. *NetProwler—Advanced Network Intrusion Detection*. WWW: <URL: http://www.axent.com/iti/netprowler/idtk_ds_word_1.html>

[31] AXENT Technologies, Inc. *Netprowler*. WWW: <URL: http://www.axent.com/product/netprowler/default.htm>

[32] AXENT Technologies, Inc. *Netprowler—II* . WWW: <URL: http://www.axent.com/product/netprowler/npbrochure.htm>

NetRanger[33, 34, 35, 36] от Cisco Systems - система обнаружения вторжения в сетевых сегментах. С ноября 1999 года NetRanger известен на рынке под названием Cisco Secure Intrusion Detection System. Программа работает в реальном времени и масштабируема к уровню информационной системы. Система NetRanger формируется из датчиков и одного или более директоров, которые связаны системой почтовой связи. Каждый из датчиков развернут на базе аппаратной платформы Cisco, однако Директор реализован на основе программного обеспечения.

Датчики размещаются в стратегических точках сети и контролируют проходящий сетевой трафик. Датчики могут анализировать все заголовки и содержание каждого пакета, а также сопоставлять выбранные пакеты с образцом. Датчики используют экспертную систему на основе продукционных правил для определения тип нападения.

В системе существует три категории описания нападения: именованные нападения (то есть, нападает с определенным названием), основные нападения (то есть, поименованное нападение, которое породили множество других событий) и экстраординарные нападения (нападение с очень сложными сигнатурами). Для обеспечения совместимости с большинством существующих сетевых стандартов NetRanger дает пользователю возможность самостоятельной настройки сигнатур.

В случае фиксации факта нападения, датчик имеет возможность инициировать ряд действий, которые позволяют включить процесс сигнализации, просто регистрировать критичное событие, уничтожить сеанс или полностью разорвать сетевое соединение.

Директор обеспечивает централизованную поддержку управления для системы NetRanger. Это включает удаленную инсталляцию новых сигнатур в датчики, сбор и анализ данных защиты.

Состояние датчиков может быть проверено через цветовое кодирование. Объекты в системе (машины, прикладные программы, процессы и т.д.)

---

[33] Cisco. *NetRanger*.WWW: <URL: http:// www.cisco.com/warp/public/778/security/netranger/>
[34] Cisco. *The NetRanger Intrusion Detection System*. WWW: <URL: http://www.cisco.com/warp/public/778/security/netranger/prodlit/netra_ov.htm>
[35] Cisco. *NetRanger Intrusion Detection System*. WWW: <URL: http://www.cisco.com/warp/public/778/security/netranger/netra_ds.htm>

имеют различные состояния, отражающиеся на консоли администратора в виде строк текст или пиктограмм, при этом состояние каждого устройства представлено различным цветом. Нормальные состояния показываются зеленым, пограничные состояния - желтым, в то время как критические состояния – красным цветом. Датчики управляются через директора (с использованием инструмента nrConfigure на основе java). Директор уведомляет персонал о событии через электронную почту.

Centrax

До недавнего времени компания Centrax продавала программу под названием Entrax. Однако в марте 1999 года Centrax была куплена компанией Cybersafe. Корпорация Cybersafe сделала некоторые существенные технические изменения в Entrax и переименовала это Centrax [37, 38, 39].

Первоначально система Entrax была ориентирована на обеспечении безопасности отдельных серверов. Однако текущая версия Centrax включает как контроль событий в сегменте сети, так и на обеспечении безопасности отдельных серверов: модернизации, которая, возможно, была произведена под влиянием текущей популярности первого подхода.

Centrax включает два главных компонента: *пульт управления* и *целевой агент*. Они аналогичны директорам и датчикам в NetRanger. Однако целевой агент может быть одного из двух типов: первый для сбора информации на основе централизованной архитектуры, другой – для сбора информации на основе сетевой архитектуры. Целевые агенты постоянно находятся на машинах, которые они контролируют (например, индивидуальные PC, файл-серверы или серверы печати) и передают информацию для обработки на пульт управления.

Для повышения эффективности сетевой целевой агент (второй тип) реализован на автономной машине. Агенты первого типа поддерживают более чем 170 сигнатур (для вирусов, троянских программ, просмотра

---

[36] Cisco. *NetRanger—General Concepts*. WWW:<URL: http://www.cisco.com/warp/public/778/security/netranger/netra_qp.htm>
[37] CyberSafe Corporation. *Centrax FAQ's*. WWW: <URL: http://www.centraxcorp.com/faq.html>
[38] CyberSafe Corporation. *Centrax: New Features & Enhancements in Centrax 2.2*. WWW: <URL: http:// www.centraxcorp.com/centrax22.html>
[39] CyberSafe Corporation. *Centrax FAQ's* .WWW: <URL: http://www.centraxcorp.com/faq.html>

объекта и изменения пароля), в то время как агенты на основе сети поддерживают только 40 сигнатур.

Агенты на основе централизованного анализа могут обнаруживать и реагировать на угрозы в местном масштабе в реальном времени. Каждая угроза может иметь ее собственный образец ответа, типа завершения подключения к атакованной машине.

Пульт управления служит для администратора системы консолью для связи с системой обнаружения вторжений. Он состоит из нескольких блоков. *Целевой администратор* загружает политику сбора и аудита для целевых агентов, *администратор оценки* исследует серверы на предмет выявления уязвимости защиты, а *аварийный администратор* отображает информацию относительно обнаруженных угроз и может ответить на эти угрозы, например, путем разрыва сеанса связи.

Пульт управления функционирует на Windows NT, в то время как целевые агенты реализованы или на Windows NT или на ОС Solaris. Сетевой целевой агент реализован под Windows NT.

RealSecure

RealSecure [40, 41, 42, 24] от Internet Security Systems – еще одно средство обнаружения вторжения в реальном времени. Она использует трехуровневую архитектуру, состоящую из модуля распознавания для обнаружения в сегменте сети, модуля распознавания для отдельных серверов и модуля администратора. Сетевой модуль распознавания выполняется на специализированных рабочих станциях, чтобы обеспечить обнаружение вторжения и ответ в сети. Каждый сетевой модуль распознавания контролирует трафик пакетов, проходящий по определенному сетевому сегменту, на предмет наличия сигнатур нападения. Когда сетевой модуль обнаруживает неправомочное действие, он может ответить, разрывая подключение, посылая электронную почту или сообщение на пейджер, делая запись сеанса, повторно конфигурируя выбранные межсетевые экраны или

---

[40] Internet Security Systems. *Real Secure*. WWW: <URL: http://www.iss.net/prod/realsecure.pdf>
[41] Internet Security Systems. *RealSecure System Requirements*. WWW: <URL: http://www.iss.net/reqspec/reqDisplay.php3?pageToDisplay=RS%20sys%20reqs>
[42] Internet Security Systems. *RealSecure Attack Signatures*. WWW: <URL:http://www.iss.net/reqspec/linkDisplay.php3?pageToDisplay=RS%20a.s.%20from%20DB>

выполняя другие, определяемые пользователем, действия. Кроме того, сетевой модуль передает сигнал тревоги к модулю администратора или стороннему пульту управления для продолжения программы мероприятий и мониторинга ситуации.

Модуль распознавания для серверов - дополнение к сетевому модулю распознавания. Он анализирует ведущие файлы регистрации с целью выявить нападение, определяет, было ли нападение успешным или нет и предоставляет некоторую другую информацию, не доступную в реальном масштабе времени. Каждый такой модуль установлен на рабочей станции или сервере и полностью исследует файлы регистрации этой системы по контрольным образцам нарушений защиты. Модули этого типа предотвращают дальнейшие вторжения, завершая пользовательские процессы и приостанавливая учетные записи пользователя. Модуль может посылать сигнал тревоги, регистрационные события и выполнять другие, определяемые пользователем, действия.

Все модули распознавания соединены и конфигурируются административным модулем, который контролирует состояние любой комбинации модулей распознавания для UNIX и NT. Как результат – достижение всесторонней защиты, легкость конфигурированная и управления с единственной консоли. Административный модуль работает с любыми блоками распознавания и как сменный модуль доступен для ряда архитектур сети и операционных систем.

2.6.3. Общедоступные системы обнаружения компьютерных атак

Есть ряд свободно распространяемых общедоступных систем, которые могут использоваться для обнаружения вторжения. Ниже рассмотрены два из них: Shadow и Network Flight Recorder, которые сопровождаются объединенными усилиями военно-морского Центра сухопутных операций США, компанией Network Flight Recorder, Агентством национальной безопасности США и Институтом SANS[43]. Эти системы вряд ли будут иметь тот же уровень поддержки как и коммерческие системы, так что требуется более высокий уровень подготовки специалистов для работы с ними. Однако многим, чтобы лучше понять и оценить принципы работы систем

[43] Stocksdale, Greg. *CIDER Documents.* WWW: <URL: http://www.nswc.navy.mil/ISSEC/CID/>

обнаружения вторжения, их возможности и ограничения такие системы будет очень интересны, поскольку доступны в исходных кодах. Кроме того, рассмотрена и утилита Tripwire [44] - инструмент который, подобно Network Flight Recorder, входит в состав как в общественных версию, так и в коммерческие.

Shadow

Система Shadow[45, 46] использует так называемые станции датчиков и анализирующие станции. Датчики обычно располагаются в важных точках сети, типа внешней стороны межсетевых экранов, в то время как станция анализа расположена внутри защищенного сегмента сети. Датчики извлекают заголовки пакетов и сохраняют их в файле. Эта информация читается ежечасно анализирующей станцией, которая выполняет операции фильтрации и генерирует следующий журнал. Философия Shadow такова, что предупредительные сообщения не должны генерироваться, когда события уже идентифицированы и есть стратегия реагирования. Этот принцип был взят из опыта работы с другими системами обнаружения вторжения, в которых множество предупреждений были ложными тревогами, отвлекали и раздражали пользователей.

Станция датчиков использует утилиту libpcap, разработанную Lawrence Berkeley Laboratories Network Research Group[47], для извлечения пакетов. Станция не делает предобработки данных, таким образом предотвращая вторгшегося от проверки, что сделано с его пакетами. Главная функция анализа обеспечивается модулем tcpdump[47], через который определяются фильтры пакетов. Однако некоторые вторжения достаточно трудно обнаружить с фильтрами tcpdump, особенно те, которые основываются на редком зондировании сети. Для этих типов событий, Shadow включает инструмент на основе perl - one_day_pat.pl. Этот инструмент позволяет просматривать события для событий вторжения низкой частоты, которые

---

[44] Tripwire Security Systems, Inc. *The History of Tripwire*. WWW: <URL: http://www.tripwiresecurity.com/ products/history.html>

[45] Irwin, Vicki; Northcutt, Stephen; & Ralph, Bill. (Naval Surface Warfare Center). *Building a Network Monitoring and Analysis Capability*—Step by Step. WWW: <URL:http://www.nswc.navy.mil/ISSEC/CID/step.htm>

[46] Northcutt, Stephen. (Naval Surface Warfare Center, Dahlgren).
"Intrusion Detection: Shadow Style—Step by Step Guide." *SANS* Institute Report (November 1988).

[47] Floyd, Sally, et al. (Lawrence Berkeley National Laboratory). *LBNL's Network Research Group*. FTP: <URL: http://ftp.ee.lbl.gov/>

могут быть зарегистрированы больше чем в одном журнале. Фильтры могут быть простые или являться совокупностью ряда простых фильтров. Пример простого фильтра – tcp_dest_port_23. Этот простой фильтр выбирает пакеты протокола TCP и портом адресата 23 (то есть, telnet). Анализирующая станция использует Web-интерфейс для отображения информации от датчиков или отображения результатов фильтрации на необработанных данных.

Shadow функционирует на многих UNIX-системах, включая FreeBSD и Linux.

Network Flight Recorder

Network Flight Recorder (NFR) - система обнаружения вторжения, которая была изначально доступна как в коммерческой, так и в общедоступной версии. Последняя была свободно доступна еще совсем недавно[48, 49, 50]. NFR объясняет причины для изменения в политике распространения продукта: NFR прекратил доступ к старому исходному тексту версии, потому, что свободное программное обеспечение не было столь же эффективно как коммерческое изделие, а пользователи могли принять его за коммерческий продукт.

Вместе с тем, NFR по-прежнему планирует делать коммерческий продукт доступным для изучения, хотя, очевидно, уже не в исходных кодах.

Подобно Shadow, NFR использует несколько измененную версию libpcap для извлечения случайных пакетов из сети (эта версия может, кроме заголовков извлекать также и тело пакета). База данных и модуль анализа обычно функционирует на той же самой платформе вне межсетевых экранов. Однако копии NFR могут также быть размещены в стратегических внутренних точках, чтобы обнаружить потенциальные угрозы, исходящие от внутренних пользователей сети.

---

[48] Network Flight Recorder, Inc. *Step-by-Step Network Monitoring Using NFR.* WWW: <URL: http://www.nswc.navy.mil/ISSEC/CID/nfr.htm>

[49] Ranum, Marcus J., et al. (Network Flight Recorder, Inc.). *Implementing a Generalized Tool for Network Monitoring*. WWW: <URL: http://www.nfr.net/forum/publications/LISA-97.htm>

[50] Network Flight Recorder, Inc. *The Network Flight Recorder in Action!* WWW: <URL: http://www.nfr.net/products/technology.html>

NFR включает законченный язык программирования, именуемый N, который предназначен для анализа пакетов. Фильтры написаны на этом языке, компилируются в байт-код и интерпретируются модулем выполнения.

Функции генерации предупреждений и отчетов используются для извлечения данных после операции фильтрации и формирования выходных форм. Функция сигнализации может посылать информацию о событии через электронную почту или факс. Функция записи объединяет данные в форматы, требуемые различными модулями анализа выходных форм.

Tripwire

Tripwire - инструмент оценки целостности файла, который был первоначально разработан в Университете г. Пурду, США. Подобно NFR, эта программа входит как в общедоступные пакеты программ, так и в коммерческие версии. Общедоступная версия доступна в исходных кодах для систем UNIX. Tripwire отличается от большинства других инструментальных средств обнаружения вторжения тем, что обнаруживает изменения в файловой системе уже проверенной системы, а не выполняет поиск подозрительных действий.

Tripwire вычисляет контрольные суммы или криптографические подписи файлов. Если такие подписи были вычислены в условиях, когда файловая система находится в безопасности, и были сохранены таким способом, что они не могли быть изменены (например, хранились автономно вне сети на неперезаписываемом носителе), они могут быть использованы для сравнения с сигнатурами, вычисленными в последствии, с тем, чтобы определить возможные изменения. Tripwire может быть сконфигурирована таким образом, чтобы сообщать о всех изменениях в проверенной файловой системе администратору. Программа может быть сконфигурирована так, чтобы выполнять проверки целостности регулярно в намеченные интервалы и обеспечивать администраторов систем информацией, на основании которой они должны осуществить восстановление системы, если вмешательство произошло. Конечно, восстановление требует, чтобы соответствующие копии материала, который был скомпрометирован быть постоянно доступны.

Tripwire может обеспечивать восстановление наряду с обнаружением вторжения - особенность несвойственная большинству систем обнаружения

вторжения. Подход Tripwire независим от типа события, однако, эта программа не будет обнаруживать вторжение, которое не изменяет проверенные файлы. Кроме этого, запуск Tripwire вне расписания, полезен для оценки ущерба после возможного вторжения.

Tripwire входит, и в коммерческие и бесплатные версии. Текущий коммерческий выпуск - версия 2.X для ряда платформ UNIX и Windows NT 4.0. Бинарная версия 2.0 для Red Hat Linux 5.1 и 5.2 доступна бесплатно. Версия 1.3 доступна в исходных кодах и представляет состояние программы на момент 1992 года.

Согласно заявлению разработчика, все версии, начиная с 2.0 коммерческой редакции включают:

- *скрытое криптографическое подписывание* - программное обеспечение Tripwire для UNIX использует криптографическую технологию электронной подписи. Подписание базы данных Tripwire и файлов политики поддерживает целостность этих критических файлов.

- *усовершенствованный язык политики* – в новых версиях язык политики Tripwire был расширен, чтобы добавить гибкости в определение правил.

- *сообщения электронной почты* - программное обеспечение Tripwire для UNIX посылает сообщения через электронную почту соответствующему администратору системы.

2.6.4. Системы обнаружения компьютерных атак для государственных учреждений США

Различия между коммерческими системами и системами, предназначенными для государственных организаций

Первичные требования для программ обнаружения вторжения заключаются в том, что они должны делать видимым подозрительное сетевое действие, обеспечивать предупреждение о таком действии и предлагать варианты остановки таких действий, если это возможно. На первый взгляд коммерческие и правительственные требования одни и те же, однако, они существенно отличаются по возможностям и акцентам внимания.

В феврале 1999 года Министерство энергетики США, Совет национальной безопасности и Управление политики в области науки и техники Администрации США организовали проведение симпозиума под названием «Обнаружение враждебного программного кода, вторжений и аномального поведения». На симпозиуме присутствовали представители как коммерческого так и государственного секторов. В принятом на симпозиуме документе был отмечен ряд требований для программ обнаружения вторжения, которые не должны быть реализованы разработчиками коммерческих продуктов:

- усовершенствование методов обнаружения вторжений со стороны хорошо подготовленных агентов спецслужб иностранных государства;
- более внимательная идентификация действий пользователей;
- объективные оценки характеристик программ обнаружения вторжения.

Согласно заявлениям ряда экспертов, выступивших на конференции, как коммерческие, так и правительственные организации требуют, чтобы системы обнаружения вторжения обнаруживали вторжения и обеспечивали отображение данных об этих событиях, но возможности и акцент внимания для этих требований различны. Бизнесмены заинтересованы в защите их сетей и информации только для создания прибыли. Компании активно покупают программы обнаружения вторжения, поскольку они достаточно ясно осознают угрозу для их бизнеса от современных сетевых технологий, способных привести к потере данных или программ, составляющих определенную долю капитализации компаний.

Подчеркивается, что подобно бизнесменам, федеральное правительство заинтересовано в защите собственных сетей, однако первичное требование для него не в создании прибыли, а в защите национальной безопасности. Это очень важное различие правительственных и коммерческих требований обнаружения вторжения. Для правительства, прежде всего, требуется обеспечить обнаружение вторжений в государственные информационные сети со стороны спецслужб иностранных государств. Все эксперты, принявшие участие в симпозиуме в феврале 1999 года согласились с тем, что

ресурсы и возможности противника, поддержанного иностранным государством, определенно превысят возможности лучших методов программ обнаружения вторжения.

Другое важное различие между коммерческими и правительственными требованиями - акценты внимания.

Бизнесмены сосредотачиваются на получении общего описания подозрительного действия с тем, чтобы получить возможность его прекратить, для правительственных же организаций важно также и выяснить мотивы, которыми руководствовался нарушитель. В некоторых ситуациях, правительство может избирательно перехватывать информацию с целью разведки или исполнения постановления суда. Коммерческие программные продукты ни сегодня, ни в ближайшее время не будут интегрироваться со специализированными программными комплексами перехвата информации (типа Carnivore).

Одним из утвержденных на симпозиуме 1999 года положением было то, что производители коммерческих продуктов не будут разрабатывать объективные оценки программ обнаружения вторжения. В настоящее время, нет никаких стандартов для оценки программ этого класса. Это может удовлетворить бизнесменов, но правительственные организации, основной задачей которых является обеспечение защиты национальной безопасность, должны знать, что подобная программа делает и как она работает.

Другая проблема состоит в том, что коммерческие программы обнаружения вторжения могут быть куплены любым. Это ведет к тому, что потенциальный нарушитель, узнав, какие системы используются в государственных организациях, смог бы купить такой же продукт. И досконально изучив ее архитектуру, сможет выяснить ее уязвимые места. Этот риск может быть уменьшен, если используется только программное обеспечение, специально разработанное для государственных организаций и не попадающих в продажу.

Сегодня в США разработаны правительственные требования к обнаружению вторжения, которым существующие коммерческие программы обнаружения вторжения не удовлетворяют. Все это послужило поводом к

разработке группы специализированных продуктов обнаружения вторжений для государственных организаций.

CIDDS

CIDDS, (Common Intrusion Detection Director System, также известная как CID Director), - специализированная аппаратно/программная/операционная среда, разрабатываемая по программе создания средств обнаружения вторжений (IDT) Центра информационной войны военно-воздушных сил США (Air Force Information Warfare Center, AFIWC). AFIWC - структура, ответственная в ВВС США за разработку средств обнаружения вторжений для сетей ВВС США. В состав AFIWC входит Служба компьютерной безопасности Воздушных сил (AFCERT) которая ответственна за разработку ежедневных операций по администрированию и обеспечению защиты информационных сетей, включая и программу обнаружения вторжений.

CIDDS получает данные о подключениях и расшифровки стенограммы работы в реальном масштабе времени от машины автоматизированного измерителя инцидентов защиты (Automated Security Incident Measurement, ASIM) системы датчиков, а также и другие инструментальные средства обнаружения вторжения. Средства обеспечивают возможность анализа собранных данных как автоматическими средствами, так и с привлечением экспертов-аналитиков.

Программное обеспечение CID Director состоит из набора откомпилированных С и С ++ программ, откомпилированных программ на Java, сценариев и SQL запросов базы данных Oracle. Director хранит информацию в локальной базе данных Oracle и с помощью дружественного графического интерфейса пользователя, позволяет пользователю устанавливать корреляцию, изучать, и анализировать индикаторы потенциально опасных действий, злонамеренных или неправомочных событий, встречающихся на сетях Военно-воздушных сил США.

Методы анализа данных включают:

- обнаружение потенциально опасных, злонамеренных или неправомочных действий, которые происходят длительные периоды времени;
- обнаружение тех действий, которые имеют целью определенные машины или типы сетей;
- обнаружение тех действий, которые проходят транзитом или задействуют несколько сетей;
- анализ тенденций и глобальных целей.

CIDDS также включает возможность воспроизвести данные подключений в реальном масштабе времени для анализа последовательностей нажатия клавиш.

CIDDS обеспечивает ASIM систему централизованным хранением данных и способностью анализа. Director получает данные от различных датчиков, которые контролируют и сообщают состояние всех сетей ВВС. Эти сети могут быть гомогенными или гетерогенными, обслуживая различные миссии ВВС. CIDDS – есть центральная база данных и точка анализа для всех этих сетевых систем.

Планы будущего развития системы включают установку ряда систем CID Director на различных уровнях во всех структурах ВВС. Все эти системы будут отправлять основную информацию в единую базу данных в AFCERT.

Каждая машина CID Director является зависимой от системы датчиков ASIM, сообщающих к этому для точности и своевременности данных, это получает и процессы.

Программное обеспечение ASIM датчика состоит из откомпилированного кода С и программ на языке Java. Сценариев для оболочки UNIX (Bourne) и файлы конфигурации, которые вместе фиксируют, фильтруют и анализируют сеть. ASIM датчик - по существу утилита перехвата разнородных пакетов данных и их анализатор. Программное обеспечение ASIM датчика ведет мониторинг трафика протокола ip, tcp, udp, icmp. Далее он анализирует этот трафик, чтобы идентифицировать подозрительные действия. Есть два режима работы для ASIM датчика: 1) пакетный режим и 2) режим реального время. В типичной ASIM инсталляции

системного программного обеспечения датчика (для нормальных операций контроля сети), оба режима включены по умолчанию.

ASIM в реальном масштабе времени использует тот же самый программный модуль, что и для пакетного режима, чтобы собрать сетевой трафик. ASIM в реальном масштабе времени идентифицирует строки и услуги, которые могли указывать на попытки неправомочного доступа в момент их происхождения и немедленно порождает аварийный процесс в сервере датчика, а также посылает предупреждение в реальном масштабе времени администратору. Предупреждения в реальном масштабе времени обычно содержат основную информацию относительно определенного действия. Дополнительная информация может быть получена из расшифровки стенограммы, которая являются отчетами нажатия клавиш для обнаруженного предупреждения.

ASIM датчик пакетного режима собирает сетевой трафик за некоторый период времени с перестраиваемой продолжительностью, обычно 24 часа. После обобщения данных, они анализируются программным обеспечением, с целью идентифицировать индикаторы подозрительного действия. Программное обеспечение датчика ASIM генерирует расшифровки стенограммы собранных данных для идентифицированного подключения, которое могло указывать, что кто-то сделал попытку или выполнил неправомочное действие. Данные могут быть просмотрены как локально, так и переданы в центральный офис (AFIWC/AFCERT) для наблюдения и анализа.

Каждый день данные, собранные датчиками ASIM шифруются на сайтах, сертифицированных AFCERT и передаются в головную систему ASIM (AFIWC/AFCERT) для анализа специалистом-аналитиком. Аналитик определяет, является ли идентифицированное действие злонамеренным, неправомочным или нормаль уполномоченное действие.

Таким образом, поведенный анализ показывает, что в области создания систем обнаружения вторжений в настоящее время характерен переход к созданию систем, основанных на обнаружении вторжений в сетевые сегменты.

Следует отметить, что для американского рынка характерна ситуация, когда программные продукты для коммерческого применения сильно отличаются от тех продуктов, которые рекомендованы для использования в государственных учреждениях. Это – общая тенденция в области информационных технологий – для государственных учреждений должны использоваться только специально созданные безопасные информационные технологии, недоступные на рынке.

Характерным свойством последних является ориентация не на автоматические алгоритмы распознавания признаков вторжений, а на экспертов-аналитиков, ежедневно оценивающих передаваемые данные.

2.7. Перспективные системы обнаружения компьютерных атак на основе мобильных программ-агентов

Одной из наиболее перспективных технологий противодействия информационному оружию в компьютерных сетях является использование мобильных интеллектуальных программ-агентов.

Начиная с сентября 1997 года в США Национальным институтом стандартов и технологии (NIST), совместно с рядом фирм, при финансовой поддержке Агентства национальной безопасности реализуется проект, призванный оценить перспективу использования технологии мобильных программ-агентов для обеспечения безопасности компьютерных систем.

Целью проекта является исследование приемов и способов использования технологии мобильных агентов для улучшения характеристик программного обеспечения информационной безопасности, а также исследование путей, позволяющих обезопасить саму технологию мобильных агентов.

В последнее время работы по проекту сосредоточены на разработке технологии управления полномочиями мобильных агентов на основе цифровой подписи и цифровых сертификатов, что тесно связано с проводимыми NIST работами по формированию национальной инфраструктуры обеспечения работы криптосистем с открытым ключом (Public Key Infrastructure, PKI), а также на возможности применения

технологии мобильных агентов для улучшения характеристик систем обнаружения вторжения в компьютерные сети.

Системы обнаружения вторжения сегодня уже достаточно широко распространены в корпоративных информационных системах и компьютерных сетях. Оценки показывают, что рынок инструментальных средств СОВ достиг в 2000 году почти 150 миллионов долларов США. Обнаружение вторжения в компьютерные сети и информационные системы компаний уже далеко не новое направление научных исследований. Сегодня это уже достаточно хорошо освоенная коммерческая область с рядом серьезных конкурентов типа IBM, Cisco и Network Associates.

Вместе с тем, по признанию ряда экспертов, существующие СОВ достаточно часто срабатывают в пустую, к тому же не обнаруживают все известные атаки на информационные ресурсы компаний. В этом отношении текущее состояние разработок СОВ похоже на недавнее положение дел в области антивирусного программного обеспечения. Ранние версии антивирусов также излишне беспокоили пользователя всякий раз, когда он создавал новые файлы или стирал старые. Однако в последние годы антивирусное программное обеспечение было существенно усовершенствовано. Сегодняшний пользователь практически не обращает внимания на то, что на его компьютере функционирует антивирусное программное обеспечение. При этом, как показывает практика, большинство из них уверены, что антивирус обнаружит все известные (а зачастую и новые) вирусы. Этим же путем сегодня идут и разработчики систем обнаружения вторжений.

В силу того, что обнаружение вторжения стало зрелой технологией и областью промышленных интересов, сегодня практически все простейшие проблемы в ней успешно решены. В последнее время в этой области исследований не было найдено существенных прорывных решений. Вместо этого, разработчики систем подобного рода совершенствуют главным образом существующие методы обнаружения вторжения.

В этой связи многие эксперты отмечают, что традиционные направления исследований в этой области в ближайшее время будут иметь все меньшее значение. Будущее работы по совершенствованию приемов

обнаружения вторжения, как ожидается, сосредоточатся на относительно неисследованных областях типа:

- механизмы ответа на нападение;
- архитектуры сильно распределенных систем обнаружения вторжения;
- стандарты взаимодействия компонентов системы при обнаружении вторжения;
- новые парадигмы обнаружения вторжения.

2.7.1. Технология мобильных агентов

К числу перспективных направлений исследований в области создания систем обнаружения вторжений относится и применение мобильных программ-агентов.

Системы обнаружения вторжения на основе мобильных агентов - одна из новых парадигм создания систем данного класса. Мобильные агенты - специфический тип программного обеспечения, который имеет возможность перемещаться от одного компьютера к другому. Программный агент может быть определен следующим образом[51]: « … программный объект, который функционирует непрерывно и автономно в специфической среде … способный выполнять действия гибким и интеллектуальным способом в ответ на изменения среды … идеально, если агент, функционирующий непрерывно, …был бы способен учиться на опыте. Кроме того, существуют агенты, которые взаимодействуют с другими агентами и процессами, при этом они способны общаться и сотрудничать с ними, а при необходимости - перемещаться от одного компьютера к другому».

Мобильные агенты являются одной из передовых тем исследований в области информационных технологий в течение ряда лет. Однако результаты этих исследований, главным образом, оставались в пределах лабораторий и не были широко использованы. Вместе с тем, интенсификация работ по созданию Web-приложений имела ключевое значение для взрывного роста заинтересованности к области исследований свойств мобильных агентов, что

[51] Jeffrey M. Bradshaw, “An Introduction to Software Agents,” In Jeffrey M. Bradshaw, editor, *Software Agents*, chapter 1. AAAI Press/The MIT Press, 1997.

связано с возможностью создания на их основе распределенных приложений для работы в Интернет. Стала широко применяться процедура запуска на выполнение мобильных агентов через Web-браузеры для сбора информации и взаимодействия с любым узлом в сети (технология «ноуботов»). Фирмы IBM и General Magic являются инициаторами работ в этом направлении интерактивных систем[52, 53]. Параллельно, в 1994 году Агентство перспективных исследований и разработок Министерства обороны США (ARPA) поддержало программу «Распределение знаний» (Knowledge Sharing). В результате ее реализации был разработан язык KQML[54], который до настоящего времени остается одним из наиболее жизнеспособных языков взаимодействия агентов (Agent Communication Languages, ACLS).

Область исследования мобильных агентов была пересмотрена в период 1995-1996 годов, когда Sun Microsystems был разработан язык программирования Java. Хотя Java и являлся просто одним из новых интерпретируемых языков программирования, он специально разрабатывался для организации взаимодействия сетевых приложений и предоставления технологии мобильного, платформнонезависимого программного кода. Язык Java обеспечил некоторую независимость системы, в язык были включены конструкции, позволяющие обеспечить приемлемый уровень безопасности.

В течение того же периода, были представлены многочисленные предложения по использованию мобильных агентов. Например, система Lava [55,56], разработанная в Государственном университете штата Северная Каролина (США). Разработчики этой системы сосредоточились на решении проблема защиты информации, поэтому в системе была реализована простая, но эффективная политика защиты для апплетов Java. Mitre Corporation[57, 58],

---

[52] Chess, D., B. Grosof, C. Harrison, D. Levine, C. Parris, G. Tsudik, “Itinerant Agents for Mobile Computing,” IBM Research Report, RC 20010, March 1995. <URL:http://www.research.ibm.com/massdist>.

[53] Harrison, C.G., D.M. Chess, A. Kershenbaum, “Mobile Agents: Are they a good idea?,” IBM Research Report, March 1995.

[54] Finin, T., R. Fritzson, D. McKay, and R. McEntire. “KQML as an Agent Communication Language,” Proceedings of the Third International Conference on Information and Knowledge Management (CIKM ’94), ACM Press, Nov. 1994.

[55] Wu, S.F., M. S. Davis, J. N. Hansoty, J. J. Yuill, S. Farthing, J. S. Webster, X. Hu. “LAVA: Secure Delegation of Mobile Applets,” Technical Report 96/42, Center for Advanced Computing and Communication, North Carolina State Univ., Raleigh, NC, October 1996.

[56] Hansoty, Jatin N., “LAVA: Secure Delegation of Mobile Applets,” Master’s Thesis North Carolina State Univ., 1997. <URL: http://shang.csc.ncsu.edu:80/lava.html >

[57] Farmer, W.M., J.D. Guttman, and V. Swarup, “Security for Mobile Agents: Authentication and State Appraisal,” Proceedings of the 4th European Symposium on Research in Computer Security (ESORICS ’96), pp. 118-130, September1996.

также проводившая работы в этой области, разработала механизмы аутентификации и определения таксономии событий в области защиты информации с использованием Java.

Важное наблюдение на основе анализа большинства работ в области мобильного кода в ранний период ее развития, сделанное многими исследователями, касается полной открытости подобных систем. Практически все возможные проблемы защиты в полной мере реализовались в системе с полностью открытой архитектурой, что привело к возникновению максимально возможного числа угроз. На основе этого наблюдения в то время некоторые исследователи сделали вывод о том, что использование парадигмы мобильных агентов не является целесообразным там, где всегда имелись угрозы безопасности, которым невозможно противостоять при полной открытости системы.

Частично в силу этих выводов, частично в силу хорошо разрекламированных нападений хакеров на ряд ранних Java-систем, нерешенные проблемы обеспечения защиты информации препятствовали широкому распространению технологии мобильных агентов.

Эти соображения особенно чувствительны для систем обнаружения вторжения, так, что в итоге большинство исследователей в этой области сконцентрировались на создании структуры, необходимой для обеспечения защиты мобильных агентов.

Многоагентные системы имеют ряд характеристик, которые дают им возможность расширить технологию обнаружения вторжения. Агентная технология и приложения на ее основе походит на сообщество самонастраивающихся и интеллектуальных особей. Классы особей имеют специализированные цели, и каждый индивидуум может работать независимо от других. Каждый индивидуум общается и обменивается информацией с другими.

Эта парадигма остро контрастирует с традиционной парадигмой программирования, где главный логический модуль управляет набором подчиненных. Подчиненные модули не имеют никакой самостоятельности и

---

[58] Farmer, W.M., J.D. Guttman, and V. Swarup, “Security for Mobile Agents: Issues and Requirements,” Proceedings: National Information Systems Security Conference, pp. 591-597, October 1996. <URL: http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper033/>

исполняют только то, что диктует главный логический модуль. Разновидности традиционного подхода включают множественные модули. В этом случае может не существовать центральный контроллер, а каждый модуль может взаимодействовать с другими модулями, чтобы исполнить задание. Однако если один модуль прекращает функционировать, другие модули не достаточно интеллектуальны (или не имеют полномочий) чтобы самостоятельно решить поставленную задачу. Эта традиционная распределенная парадигма программирования работает достаточно хорошо, когда компоненты отчасти дублируют друг друга по функциональным возможностям. Даже при использовании избыточных компонентов, противник может отключить сравнительно малое число резервных копий функциональных блоков. Агентная технология - значительный контраст этому подходу, так как она пытается дать каждому агенту понимание среды наряду с его полномочиями, чтобы независимо принимать решения.

Мобильные агенты по своей природе *автономные, коллективные, самоорганизующиеся и мобильные*. Эти особенности не отражены в традиционных распределенных программах и дают возможность СОВ реализовать полностью новые подходы для обнаружения вторжения, некоторые из которого основаны *на аналогиях, найденных в природе и в обществе*.

Представьте совокупность мобильных агентов как колонию пчел. Каждая пчела имеет способность лететь к цветам и подбирать пыльцу точно так же как мобильный агент может двигаться среди компьютеров и обрабатывать данные. Пчелы не имеют потребности нести большие цветы домой. Точно так же агент может избегать необходимости передавать данные по факту обнаружения вторжения в центральный архив.

Другая аналогия может представить совокупность мобильных агентов, выполняющих работу в составе СОВ, как колонию муравьев. В случае гибели одного или нескольких сотен рабочих колония продолжает функционировать. Кроме того, муравьи могут переместиться далеко за пределы колонии, когда они видят убывание пищи. Многоагентная система может быть создана с подобным механизмом сопротивления нападению, так как агенты самонастраивающиеся и мобильные, а уничтожение нескольких не влияет на функционирование системы в целом.

Многоагентная система также может рассматриваться как множество охранников. Сотрудники отдела безопасности компании не хотят нести расходы на размещение охранников в каждой комнате офиса. Вместо этого, они делают обход каждой комнаты, периодически проверяя наличие признаков вторжения. Аналогично и многоагентная система дает возможность периодически проверять компьютеры с целью выявления проблем защиты без необходимости устанавливать программное обеспечение проверки на каждом компьютере.

Это - только несколько примеров того, как сообщества самонастраивающихся мобильных агентов могут приносить пользу технологии обнаружения вторжения. Подвижность - важный аспект, но одного его не достаточно. Многоагентная система должна быть способной использовать автономность и работать во взаимодействии с другими агентами. Эти особенности позволяют предложить новые парадигмы обнаружения вторжения.

2.7.2. Основные проекты в области систем обнаружения вторжений на основе мобильных агентов

Наиболее интенсивные работы по исследованию свойств мобильных агентов для создания систем обнаружения вторжения на основе мобильных агентов (Mobile Agent Intrusion Detection Systems, MAIDS) в компьютерные сети проводятся в настоящее время в ряде лабораторий США и Японии. Среди наиболее известных организаций университет штата Айдахо, университет штата Нью-Мексика, Армейская научно-исследовательская лаборатория Министерства обороны США, Государственный университет штата Айова, а также Агентство содействия информационным технологиям в Японии.

Самонастраивающиеся агенты для обнаружения вторжения

Самонастраивающиеся агенты для обнаружения вторжения (The Autonomous Agents for Intrusion Detection (AAFID), разработанные в университете г Пурду[59], используются в традиционной системе обнаружения

[59] Jai Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, E. H. Spafford, and Diego Zamboni, “An Architecture for Intrusion Detection using Autonomous Agents,” Department of Computer Sciences, Purdue University; Coast TR 98-05, 1998. <URL: http://www.cs.purdue.edu/coast/coast-library.html>

вторжений на основе агентов главным образом как средство для преобразования множества компонентов обнаружения вторжения в совокупность простых программных объектов, которые могут быть легко реконфигурированы.

AAFID используют иерархию агентов. В корне иерархии - мониторы, которые обеспечивают глобальный контроль и управление. Они же выполняют анализ информации, поступающей от узлов более низких уровней. В листьях иерархии - агенты, которые собирают информацию о событиях. Агенты постоянно находятся во взаимосвязи со специальными базовыми агентами, именуемыми «приемопередатчиками». Приемопередатчики выполняют роль локальных мониторов по контролю и управлению агентами, а также для анализа и обработки потока информации, полученной от этих агентов, с целью его сокращения для передачи агентам-мониторам более высокого уровня. Агенты статические и вводятся в систему путем загрузки с приемопередатчика, однако они могут быть заменены в процессе реконфигурации.

Hummingbird

В университете штата Айдахо разработан проект Hummingbird[60]. Это - один из наиболее амбициозных проектов распределенной системы обнаружения вторжения из доступных в настоящее время.

Система Hummingbird - это распределенная система для сбора и управления данными о нештатном использовании компьютерных систем. Хотя система использует некоторую агентную технологию, однако, в ней агенты не адаптивные и не мобильные. В системе распределен только сбор данных, а контроль и управление остается централизованным. Акцент сделан на защищенном распределении данных среди серверов сети, имеющих различные уровни защиты. Предполагаются также и инструментальные средства, алгоритмы, методы сжатия данных и технология визуализации информации в системах мобильных агентов.

---

[60] Frincke, D., Don Tobin, Jesse McConnell, Jamie Marconi, Dean Polla, “A Framework for Cooperative Intrusion Detection,” Proceedings of the 21st National Information Systems Security Conference, pp. 361-373, October 1998. <URL:http://csrc.nist.gov/nissc/1998/papers.html>

В Hummingbird не реализовано принципиально новых механизмов для защиты собственной структуры. Вместо этого в проекте используется система Kerberos[61].

Агенты Java для метообучения

В проекте «Агенты Java для метообучения» (JAM)[62] Колумбийского университета (штат Нью-Йорк) метод метообучения применяется для извлечения распределенных данных посредством применения интеллектуальных агентов. Интеллектуальные агенты используют методы искусственного интеллекта для моделирования знаний и рассуждений, а также поведения в многоагентных сообществах. Проект имеет два ключевых компонента: локальные агенты обнаружения несанкционированных действий, которые изучают, как обнаружить действия такого рода и обеспечить услуги обнаружения вторжения в пределах отдельной информационной системы; и защищенной, интегрированной системы метообучения, которая объединяет коллективные знания, приобретенные индивидуальными локальными агентами. Извлечение данных, подобно нейронным сетям и другим приложениям, обучающимся централизованно, не допускает совместного использования знания агентами. Подход на основе метообучения пытается преодолеть это ограничение, интегрируя множество отдельно обученных классификаторов, реализованных как отдаленные агенты.

Интеллектуальные агенты для обнаружения вторжения

Этот проект, реализуемый в Государственном университете штата Айова[63], реализует систему обнаружения вторжений, основанную на технологии интеллектуальных агентов, подобной использованной в проекте JAM. Подвижность агентов позволяет различным типам интеллектуальных

---

[61] B. Clifford Neuman and Theodore Ts'o. “Kerberos: An Authentication Service for Computer Networks, ” IEEE Communications, 32 (9), pp. 33-38, September 1994. <URL http://nii.isi.edu/publications/kerberos-neuman-tso.html >

[62] W. Lee, S.J. Stolfo, and K. Mok, “A Data Mining Framework for Building Intrusion Detection Models,” Proceedings of the IEEE Symposium on Security and Privacy, 1999. <URL: http://www.cs.columbia.edu/~sal/JAM/PROJECT/>

агентов (называемых в проекте «сборщики данных»), которые используют алгоритмы классификатора, передвигаться среди точек сбора информации и раскрывать подозрительные действия.

Алгоритм агента - стандартные алгоритмы идентификации последовательностей. Структура иерархическая с информационным хранилищем в корне, уборщиками данных в листьях и агентами-классификаторами между ними. Агент-классификатор специализируется на определенной категории вторжения и способен к сотрудничеству с агентами другой категории, чтобы решить, насколько серьезен уровень подозрительных действий. При перемещении вычислительного алгоритма (то есть, агента-классификатора) к каждой точке сбора данных, позволяет избежать дорогостоящего перемещения информации к обобщающему модулю. Результаты работы обеспечивают хороший базис для последующих исследований, так как подход дает возможность определить агентов обнаружения вторжения для индивидуальной системы и подсистемы.

Программа исследования перспективных телекоммуникаций и распределения информации

Работа, выполняемая вооруженными силами США по программе перспективных телекоммуникаций и распределения информации (the Advanced Telecommunications/Information distribution Research Program, ATIRP)[64, 65, 66], адресована не обнаружению вторжения, а выявлению уязвимых мест в компьютерных систем с использованием мобильных агентов. Однако модули оценки уязвимости могут быть легко заменены модулями обнаружения вторжения, что позволяет создать простую систему обнаружения вторжения. Центральный диспетчер запускает агентов к одному или нескольким целевым узлам, чтобы проверить на известные уязвимости и

---

[63] Guy Helmer, Johnny S. K. Wong, Vasant Honavar, and Les Miller. “Intelligent Agents for Intrusion Detection.” Proceedings, IEEE Information Technology Conference, Syracuse, NY, pp. 121-124, September 1998. <URL: http://www.cs.iastate.edu/~ghelmer/ieee-1998.ps>

[64] Michael Conner, Chirag Patel, Mike Little, “Genetic Algorithm/Artificial Life Evolution of Security Vulnerability Agents,” Army Research Laboratory Federal Laboratory 3rd Annual Symposium on Advanced Telecommunications & Information Distribution Research Program (ATIRP), February 1999.

[65] Jacobs, S., D. Dumas, W. Booth, M. Little, “Security Architecture for Intelligent Agent Based Vulnerability Analysis,” Proceedings: 3rd Annual Fedlab Symposium on Advanced Telecommunications/Information Distribution Research Program, pp. 447-451, February 1999, College Park, MD.

[66] Barrett, Michael, W. Booth, M. Conner, D. Dumas, M. Gaughan, S, Jacobs, M. Little, “Intelligent Agents System Requirements and Architecture,” Report to ATIRP, p. 5, October 1998.

сообщить обратно результаты проверки. Агенты составляются динамически с использованием генетического алгоритма, который непрерывно пытается максимизировать вероятность обнаружения существующих уязвимостей. Генетический пул, от которого агенты развиваются, состоит из кодовых фрагментов, которые соответствуют методике обнаружения и разработаны таким образом, что способны взаимодействовать с другими фрагментами. Структура имеет определенные возможности защиты, основанные на криптогафических сигнатурах и электронных сертификатах. Идентичные или подобные возможности требуются и для системы обнаружения вторжений. Исходная система должна была бы быть расширена, чтобы управлять системой обнаружения вторжений, так как связь между агентами более чувствительна в обнаружении вторжения, чем при сканировании уязвимостей.

Система обнаружения вторжения на основе агентов

Агентство содействия информационным технологиям (Information-technology Promotion Agency, IPA) Японии, разрабатывает систему обнаружения вторжений, названную «Система обнаружения вторжения на основе агентов» (Intrusion Detection Agent system, IDA)[67].

Система IDA относится к категории многохостовых систем обнаружения вторжений. Вместо анализа действий всех пользователей, IDA наблюдает за определенными событиями, которые могут касаться вторжений, и обозначаемых в системе как «метки, оставленные подозреваемым злоумышленником» (Marks Left by Suspected Intruder, MLSI). Если MLSI найдена, то IDA собирает дополнительную информацию, связанную с этой MLSI, анализирует ее и решает: произошло или нет вторжение.

Система IDA основывается на использовании мобильных агентов, для определения злоумышленников среди множества серверов, вовлеченных в операцию вторжения и сбора информации. Структура системы иерархическая с центральным менеджером в корне и множеством различных

[67] M.Asaka, S.Okazawa, A.Taguchi, and S.Goto, "A Method of Tracing Intruders by Use of Mobile Agents," INET'99, June 1999.

агентов в листьях. Датчиком является агент, который постоянно находится в узле с целью поиска MLSIS. О факте обнаружения такой информации датчик уведомляет менеджера, который посылает агента-инспектора на инспектируемый сервер. Агент-инспектор инициализирует собирающего информацию агента для сбора дополнительной информации, связанной с инспектируемым сервером, перед перемещением на любой другой узел сети, идентифицированный как подозреваемый. Менеджер собирает и интегрирует результаты от собирающего информацию агента. Возможное дублирование, связанное с тем, что несколько датчиков обнаруживают одно и то же событие вторжения в системе решено через «доску объявлений» в каждом проверенном сервере.

Вместе с тем технология обеспечивает ценные дополнения к текущим возможностям систем обнаружения вторжений. Хотя препятствия на пути создания практических систем на основе мобильных агентов достаточно высоки, способность перемещать программу выполнения от одной аппаратной базовой системы до другой – весьма ценное свойство. В конечном счете, когда проблемы, связанные с обеспечением защиты, производительности, безопасной технологий функционирования и барьеры стандартов, которые подавляют развитие технологии мобильных агентов, будут решены, технологии на основе агентов ждет широкое применение.

2.8. Системы контроля и перехвата информации в глобальных информационных сетях

В настоящее время происходит изменение роли коммуникаций, вызванное ростом стоимости нематериальных активов, а также выходом на рынок новых высокотехнологичных компаний. Наряду с этим происходит создание все более изощренных технологий воздействия на аудиторию, которые становятся все более доступными. Так под влиянием процессов глобализации Интернет становится важнейшим каналом для влияния на поведение и восприятие людей.

Как пишет А.А. Мухин в своей книге «Информационная война в России», в последние несколько лет в российском сегменте сети Интернет появилось множество проектов, содержание которых может быть охарактеризовано как «сетевой компромат». Дело дошло до того, что в 1999

году даже был проведен круглый стол основной темой которого было обсуждение перспективы превращения Интернета в России в арену для политических манипуляций.

Наиболее значимым событием в сфере «сетевого компромата» по словам А.А. Мухина, стало появление серии сайтов под общим названием «Коготь». Материал сайтов содержал главным образом сведения о ряде известных российских политиков, бизнесменов и чиновников, содержал материалы прослушивания их телефонов, расшифровки пейджерных сообщений и др. Как отмечает автор, появление компромата в сети взбудоражило общество еще и потому, что все материалы были анонимные, а выяснить авторство не удалось. В случае с печатными средствами массовой информации и телевидением источник информации, так или иначе, выявить удавалось, Интернет же в России оказался на практике идеальной средой для распространения анонимной информации самого различного содержания.

В последнее время передача информации через Интернет стала необходимой и неотъемлемой частью организации коммуникаций как в государственном, так и в частном секторе современного общества. Коммуникации посредством Интернет сегодня уже может конкурировать с обычным телефоном. Вместе с тем стало очевидным, что она все чаще эксплуатируется преступниками и террористами, деятельность которых угрожает не только безопасности отдельных граждан, но и национальной безопасности целых государств. В этом случае, контролируемый судебными властями перехват такой информации техническими средствами может стать мощным инструментом в противостоянии подобным угрозам.

Сегодня Интернет - это мировая компьютерная сеть, объединяющая сотни тысяч локальных, государственных, корпоративных, общественных, образовательных и иных сетей. Численность пользователей Интернет растет очень быстро. Специалисты утверждают, что динамика развития интернет-услуг в мире предвещает великие перемены в распространении массовой информации[1].

Быстрый рост числа пользователей Интернета заставляет субъектов политической жизни всерьез задуматься о них, как о части потенциальной аудитории. Буквально за последние несколько лет в Интернет были

представлены практически все ведущие СМИ. Кроме того, в сети представлены правительства и парламенты большинства стран.

В настоящее время Интернет предоставляет различную информацию 24 часа в сутки, спрос на которую пытаются удовлетворить многочисленные проекты, среди которых есть как интернет-версии традиционных СМИ, так и чисто сетевые СМИ, возникшие благодаря возможностям Интернета.

Сегодня уже просто невозможно представить себе ни одного крупного информационного агентства или СМИ, будь то телевизионный канал, газета или радиостанция, не имеющего своего представительства в Интернете.

Преимущества Интернет-СМИ обусловлены специфическими способами, приемами и формой подачи в них информации. С другой стороны и негативных моментов в распространении информации через Интернет-СМИ более чем достаточно.

В последние годы Интернет становится активным участником практически всех политических скандалов, исполняя роль удобной информационной площадки для «вброса» в общество компромата, дезинформации и т.п. При этом заинтересованные лица используют в своих целях одно из главнейших свойств Интернета - его глобальность. На сегодняшний день разместить в Сети сайт, содержащий материал фактически любого характера, например, в США или в любой другой стране очень просто: достаточно оплатить регистрацию доменного имени через Интернет по кредитной карточке, «закачать» на удаленный сервер соответствующую информацию - и создатели сайта становятся фактически недосягаемыми для национальных правоохранительных органов. Таким образом, заинтересованные субъекты уходят от юридической ответственности, а распространяемая ими информация становиться весьма действенным средством для достижения поставленных, в первую очередь политических, целей.

Анализ зарубежного опыта использования информационных ресурсов убедительно свидетельствует о возрастающей роли Интернет-СМИ, как одного из средств информационно-психологического воздействия сторон друг на друга, а также на международное общественное мнение.

Так, в период проведения странами НАТО т.н. миротворческой операции в Боснии и Герцеговине на соответствующих сайтах постоянно размещалась информация, нацеленная на формирование позитивного образа США и НАТО в урегулировании боснийской проблемы[1]. С началом операции «Союзная сила» в Интернет было размещено свыше 300 тысяч сообщений, так или иначе затрагивающих проблему Косово[2]. По оценкам аналитиков, большинство из них были созданы непосредственно или при содействии западных специалистов по компьютерным технологиям и связи с общественностью.

Соответственно, возможности сети также активно используются противостоящими сторонами на различных этапах внутренних вооруженных конфликтов. Как было отмечено выше, специфика создания и функционирования Интернет-СМИ, делает возможным использование ресурсов сети деструктивными силами для проведения негативного информационно-психологического воздействия.

В середине 90-х годов для правительств ряда государств стало очевидным, что оставлять без должного внимания ситуацию, складывающуюся в области распространения информации через Интернет просто невозможно – невнимание к этому вопросу угрожает национальной безопасности.

Понимание проблемы и решение каким-либо путем повлиять на ситуацию привело к формированию и исполнению спецслужбами рядя стран организационно-технических программ по созданию средств и методов контроля национальных сегментов глобальной сети Интернет.

Ниже мы рассмотрим ряд таких программ на примере создания системы Carnivore в США, системы «временный почтовый ящик» в Японии.

2.8.1. Система Carnivore – средство кибернетической разведки

Федеральное бюро расследований США разработало инструмент, названный Carnivore (прямой перевод этого слова – “плотоядное растение”), который призван облегчить перехват электронных коммуникаций программно-техническими средствами. Carnivore – аппаратно-программный комплекс относящийся к классу «снифферов IP-пакетов», который может перехватывать и выборочно записывать трафик от определенного

абонентского пункта в компьютерной сети к которой он подключен. Пакеты могут выбираться на основании IP-адреса или, в случае электронной почты, на названии имени пользователя в полях TO и FROM. В отдельных случаях, пакеты могут быть выбраны на основании их содержания. Перехваченные пакеты могут быть зарегистрированы полностью (полнотекстовый режим) или регистрация может быть ограничена только адресной частью (режим по ключевым словам) включающей IP-адрес и имя пользователя. ФБР полагает, что Carnivore позволит ограничить объем информации, которую оно вынуждено собирать при проведении следственных мероприятий, за счет гораздо более точного ее поиска, чем в случае, когда используются для этих целей коммерческие инструментальные средства или, когда поставщик услуг Интернет проводит мероприятия по сбору информации по его просьбе. Существует и ряд других подобных программ, например Omnivore и Etherpeek.

В официальном заявлении представителей ФБР и Министерства юстиции США говорится, что система Carnivore призвана противостоять терроризму, шпионажу, попыткам применения информационного оружия, распространению порнографии, разным видам мошенничества и другим уголовным преступлениям с использованием Интернет. Сотрудники этих ведомств гарантировали, что инструмент не будет использоваться с целью преднамеренного или произвольного перехвата частной информации. Однако многие американцы обеспокоены тем, что электронное подслушивание может стать угрозой конституционным правам частной жизни и свободы слова.

В отсутствии детальной информации о системе Carnivore возникло множество слухов относительно возможностей системы и приемам его использования следственными органами. Ряд членов Конгресса США подвергли сомнению законность создания и применения таких инструментальных средств. Беспокойства были незначительно смягчены после того, как Министр юстиции США Джанет Рино заявила, что «…когда мы внедряем новую технологию, когда мы применяем Конституцию, я хочу удостовериться, что мы применяем это непротиворечивым, сбалансированным и адекватным способом…».

Вопросы, поднятые правительством США были сформулированы следующим образом:

1. Carnivore представляет технологию, которая сохраняет или нарушает баланс между интересами секретности и законными интересами следствия?

2. Необходимы ли дополнительные законодательные акты для использования таких инструментальных средств?

3. Действительно ли беспокойства граждан справедливы?

Чтобы обеспечить технически обоснованные выводы по этим вопросам, Министерство юстиции США вынуждено было ходатайствовать перед академическими и частными организациями о проведении независимой экспертизы системы Carnivore. На это предложение откликнулись одиннадцать организаций, из числа которых был выбран Исследовательского института информационных систем (IIT Research Institute). Как заявили представители Министерства юстиции, выбор основывался на лучшем техническом мастерстве, предложенной высоко профессиональной методологией и приемлемым графиком проведения работ.

Однако сразу после того, как стал известен персональный состав комиссии, которая должна была провести экспертизу системы Carnivore, страсти в обществе накалились с новой силой. Стало известно, что большинство членов комиссии так или иначе связаны с рядом правительственных учреждений и ведомств. Так один из членов комиссии работал на Агентство национальной безопасности в 80-х, затем продолжил разрабатывать компьютеризированную поисковую технологию для ФБР. Другой член комиссии служила в течение четырех лет юристом в Министерстве юстиции США. Несколько других экспертов предварительно работали над проектами для Налогового управления США. При этом на неоднократные запросы ряда неправительственных организаций о проведении подобной экспертизы ранее ФБР отвечало отказом.

Кроме того, высказывались большие сомнения, что всего за шесть недель имея бюджет в 175 тысяч долларов возможно провести серьезное и независимое тестирование столь сложной системы как Carnivore. Все это поставило под сомнение объективность проводимого исследования.

Однако, несмотря на подобные заявления, в ноябре 2000 года специалистами Исследовательского института информационных систем (IIT Research Institute) и Иллинойского технологического института (The Illinois Institute of Technology) был подготовлен отчет по результатам проведенного исследования основных характеристик системы Carnivore. Исследование проводилось по контракту с Министерством юстиции США.

В ходе изучения основных характеристик системы Carnivore, специалистам предстояло ответить на следующие основные вопросы:

- обеспечивается ли доступ только к той информации, которая определена в постановлении суда;
- вносятся ли дополнительные технические или программные уязвимые места в систему обеспечения защиты информации, установленную у поставщика услуг доступа к Интернет, к сети которого подключена система Carnivore;
- существует ли риск неавторизованного сбора информации случайно или преднамеренно как сотрудниками ФБР, так и другим персоналом;
- адекватна ли защита информации возможным рискам по ее утрате.

Кроме того, специалисты IITRI рассмотрели обращения большого числа заинтересованных организаций и граждан, обеспокоенных применением системы. Экспертами IITRI изучались полученные доказательства, исследовались материалы на ряде сайтов Интернет.

Эксперты IITRI решили, что отчет должен также раскрывать:

- все потенциальные возможности системы, независимо от предназначенного использования;
- управляемость и подконтрольность Министерству юстиции и судам всех этапов процесса, проводимого ФБР;
- обеспечение отказоустойчивости и целостности данных;
- роли, фактические и потенциальные, других сторон и систем; например, поставщика услуг доступа к сети Интернет или возможные альтернативные способы ее применения;

- функции Carnivore в пределах набора подобных программ

При этом оценка должна включать, не только сведения о том, как используется Carnivore, но также и ее технические возможности. Эксперты IITRI оценивали только восприятие распоряжений суда оперативным работником, выполняющего постановление суда как команду на запуск программного обеспечения сбора данных, возможной минимизации собранной информации, а также обработку и пост-обработку полученных данных. Вопросы конституционности перехватов подобного типа, а также анализ доверия к исполнителям постановления суда остались вне этой оценки.

Между тем следует отметить, что исследование Carnivore, выполненное специалистами IITRI, есть только единичный снимок развития системы. Carnivore постоянно совершенствуется, повышая свою производительность, расширяя возможности и сохраняя темп с развитием Интернет и законодательных норм.

Carnivore - это система предназначенная для санкционированного судом наблюдения за электронными коммуникациями. Она используется, когда другие средства (например, когда ISP обеспечивают, требуемые данные) не выполняют потребности следователей или в силу ограничений, наложенных судом. Carnivore может использоваться для получения полнотекстового содержания линии связи или только адресной информации (то есть, ключевых слов). Считается, что сотрудники, реализующие постановление суда, следуют строгой, детальной процедуре, чтобы получить постановление суда на применение системы, а само наблюдение выполняется под руководством суда, вынесшего постановление.

Как и во всех других видах технического наблюдения, ФБР применяет строгое разделение ответственности при использовании Carnivore. Следователь устанавливает необходимость и юридическую обоснованность наблюдения. Отдельная группа технически обученных агентов устанавливает оборудование и конфигурирует его, чтобы ограничить сбор информации в соответствии с постановлением суда. Мотивы следователя состоят в том, чтобы раскрыть или предотвратить преступления, вместе с тем технические агенты мотивируются политикой ФБР и процедурами, гарантирующими, что

перехват информации строго придерживается предписания суда и будет допустим в суде как доказательство.

В ответ на вопросы Министерства юстиции США эксперты IITRI заключили следующее.

1. Когда Carnivore используется правильно, согласно порядку применения, она обеспечивает следователей только той информацией, которая должна быть доступной по постановлению суда. Когда Carnivore используется для перехвата по ключевым словам, то собирается информация из полей TO и FROM сообщения, а также указывается длина сообщения и длины индивидуального поля в пределах тех сообщений, возможно превышающих разрешенный судом объем собираемых данных.

2. Функционирование Carnivore не вносит дополнительный эксплуатационный риск или риск защиты для сети провайдера, где она установлена.

3. Carnivore уменьшает, но не устраняет риск преднамеренного и неумышленного неправомочного приобретения информации персоналом ФБР путем использования аппаратно-программных средств, однако серьезно затруднен риск приобретения информации людьми, не являющимися персоналом ФБР.

4. В то время как порядок функционирования или действия кажутся нормальными, Carnivore не обеспечивает защиты, особенно функции контроля, соразмерные с уровнем рисков.

2.8.2. Система «Временный почтовый ящик»

В статье Тошимару Огура, размещенной в Интернет 13 ноября 2000 года, говорится, что Мизухо Фукушима (член Государственного Совета, Социальная Демократическая Партия) инициировал слушания по проблеме проведения операций перехвата электронной корреспонденции, проводимых Национальным департаментом полиции (NPD) Японии в офисе самого Фукушимы. В слушании, официальный представитель NPD объяснил, что его департамент будет просить о предоставлении финансирования в следующем бюджетном году (начинающемся в апреле 2001) разработки так называемого "Временного почтового ящика" ("Temporary Mail Box") -

устройства, которое будет использоваться для перехвата электронной почты в японском сегменте Интернет. До проведения этих слушаний NPD никогда не объяснял подробности этого проекта.

Из комментариев представителя NPD в слушаниях можно сделать вывод о том, что рассматриваемое устройство ("Временный почтовый ящик") будет иметь функцию, очень похожую на функцию системы Carnivore в США или специального программного обеспечения RIP в Великобритании.

Данные сотрудниками NPD объяснения позволяют в общих чертах понять принцип работы системы, который заключается в использовании оборудования для временного хранения электронной почты на почтовом сервере провайдера. Процедура использования системы может выглядеть следующим образом.

1. Судебный исполнитель предъявляет поставщику услуг Интернет постановление суда о проведении мероприятий в отношении некоторого субъекта.

2. Поставщик услуг Интернет использует маршрутизацию приема почты, чтобы перехватить сообщения, предназначенные для объекта внимания судебного исполнителя.

3. Следователь получает перехваченную почту, размещенную на накопителе. Это не подразумевает дублирования в почтовом ящике или накопителе, переданном следствию. Для почтовых сообщений устанавливается два адреса: реальный потребитель и судебный исполнитель. Вместе с тем представители NPD отказались объяснять подробности операции при слушаниях.

4. Большинство из описанных операций может быть выполнено штатным персоналом провайдера.

Представитель NPD заявил, что на текущий момент имеется две проблемы:

- мероприятия на серверах провайдера создают неудобства для поставщика услуг;
- имеется вероятность того, что подозреваемый может выявить проводимые мероприятия.

"Временный почтовый ящик" является электронным устройством для перехвата электронной почты, предназначенным для NPD, с полным программным обеспечением и фиксированными параметрами настройки.

Согласно объяснению NPD, использование "Временного почтового ящика" подчинено следующему алгоритму.

1. NPD предоставляет устройство поставщику услуг Интернет, услугами которого пользуется подозреваемый.

2. Поставщик услуг физически подключает устройство к своей сети.

3. Судебный исполнитель использует устройство.

4. Устройство отфильтровывает входящую и исходящую почту для подозреваемого от всего трафика почты поставщика услуг.

5. NPD возвращает устройство от поставщика услуг после окончания установленного постановлением суда срока прослушивания.

Необходимое финансирование для реализации проекта внедрения системы "Временного почтового ящика" в течение 2001 года составит 140 миллионов иен (1.4 миллион долларов) при том, что одно устройство стоит 8.75 миллионов иен.

Полиция Токио планирует развернуть два устройства, а другие пятнадцать районных управлений полиции будут иметь по одному устройству. Бюджет включает стоимость разработки. После того, как бюджет будет одобрен, NPD должен будет опубликовать информацию относительно "Временного почтового ящика" и его базовой архитектуре.

В конце слушания М.Фукушима просил NPD раскрыть большее количество подробностей устройства типа исходного текста программного обеспечения, устройства для ввода и вывода информации, оправдывающих стоимость устройства в 8.75 миллионов иен. Однако до настоящего времени NPD не сказал ничто больше, кроме вышеупомянутого.

2.8.3. Прогноз развития ситуации в вопросе контроля глобальных сетей

В целом по обозначенной проблеме можно сделать следующие выводы.

Правительства ряда стран осознали угрозу, исходящую от бесконтрольности информационных ресурсов Интернет, которая в ряде случаев может рассматриваться как угроза национальной безопасности страны.

Спецслужбы этих государств разрабатывают и повсеместно внедряют технические средства и системы, позволяющие контролировать национальные сегменты глобальной сети, при этом подобные системы обладают и возможностями выявления факта применения информационного оружия. Такие системы строятся, как правило, на одних и тех же принципах.

Внедрение подобных систем вызывает волну негодования среди населения, причем опасения, как правило, схожие для населения большинства стран. Информационные кампании, вызванные этими опасениями, заставляют руководство спецслужб давать приемлемые разъяснения (вплоть до подготовки «независимого» экспертного заключения по характеристикам системы), обосновывающие легитимность применения систем этого класса. В ряде случаев власти не затрудняют себя подобными объяснениями, сославшись на государственную тайну.

В ближайшее время следует ожидать резкого ужесточения контроля над информационными ресурсами, вплоть до введения виртуальных государственных границ в киберпространстве, о чем уже сообщали ряд информационных агентств.

Такая ситуация показывает, что в настоящее время формируется новая сфера национальных интересов государства в области контроля над информационными ресурсами. Ужесточение контроля в этой сфере неминуемо приведет к эскалации информационного противоборства в виртуальном киберпространстве.

2.9. Системы контроля электронных платежей и проблема борьбы с легализацией незаконных финансовых средств международными террористическими организациями

По мнения ряда экспертов, сколь бы ни были эффективны действия отдельных стран, по контролю за киберпространством, попытки эффективно

бороться с преступниками, которые действуют в ставшем действительно глобальным Интернете, в рамках одного отдельного взятого государства, обречены на неудачу[68].

Взломщики и мошенники, проникавшие в компьютеры одной страны с территории другой, к тому же нередко использующие и компьютеры третьих государств, чаще всего оказываются вне зоны юрисдикции и спецслужб пострадавшей стороны. Фактически, возможность отслеживать и идентифицировать нарушителей по всему миру в последние годы приобрела решающее значение для предупреждения, расследования и раскрытия сетевых преступлений.

Спецслужбы ряда стран, занимающиеся расследованием деятельности наркоторговцев, преступлений в сфере финансов и секс-бизнеса, в течение последних лет создают собственные системы контроля за киберпространством. Именно эта виртуальная сфера жизнедеятельности общества с каждым годом все больше привлекает криминал. Сегодня криминал активно использует современные технологии: при помощи сотовых и спутниковых телефонов оговариваются сделки, пересылают секретные послания по электронной почте, свободно путешествуют и имеют множество банковских счетов в лучших финансовых организациях по всему миру.

В последние месяцы продолжает резко сокращаться число гражданских свобод, связанных с беспрепятственным распространением и получением информации. Под давлением США в ряде стран спешно корректируется законодательство, как-либо связанное с противодействием терроризму.

Согласно последним законодательным инициативам Белого дома, к террору приравнены и преступления в области высоких технологий. Для выявления террористов ФБР активно задействует различные системы контроля, в том числе электронные. Сегодня все чаще звучат такие названия как «Carnivore» (система контроля электронных коммуникаций и перехвата сообщений), «Echelon» (глобальная система радиоэлектронной разведки) и др.

---

[68] В. Хозиков Информационное оружие. – СПб: Издательский дом «Нева», М: Издательство «ОЛМА-ПРЕСС», 2003. – 480 с. (Серия «Досье»)

Из всего потока информации важнейшей является информация финансовая. Именно здесь сосредоточена настоящая сила. Своевременная информация о финансовых потоках может быть весьма ценной. Оставить без контроля столь значительный кусок глобального информационного пространства для США было бы просто невозможно. Поэтому, еще в 1998 году экспертами корпорации RAND было проведено исследование, результаты которого должны были лечь в основу создания новой системы контроля за финансовыми потоками в системах электронных платежей.

Электронные платежи – сравнительно недавно появившийся класс инструментов на основе платежных систем, поддерживающих электронную передачу наличных средств. Передача наличности в системах этого класса может осуществляться с использованием глобальных сетей типа Internet или с помощью физического перемещения высоко номинальных смарт-карт с записанным значением наличной суммы денег. Новые технологии оплаты предназначены в основном для замены наличных денег в розничной торговле, а также в сделках уровня потребителя.

В силу эффективность и простоты, с которой они заменяют наличность, системы электронных платежей несут в себе и новые вызовы юридическому сопровождению сделок. Существующие технологии, которые реализованы в таких системах, позволяют комбинировать скорость передачи наличности, присущей существующим банковским системам телеграфного перевода, и анонимность валютных вкладов. В результате возникают проблемы, которые должны быть разрешены в процессе развития систем этого класса, позволяющие гарантировать обнаружение и предотвращение проведения операций по отмыванию денег, а также других нелегальных финансовых сделок.

В 1990 году в рамках Интерпола была создана первая Рабочая группа по преступлениям в сфере информационных технологии, в которую вошли представители полиций ряда европейских стран (в настоящее время это Австрия, Бельгия, Великобритания, Германия, Дания, Испания, Италия, Нидерланды, Норвегия, Португалия, Швейцария, Швеция, Финляндия и Франция). Ежегодно члены рабочей группы проводят три встречи, участвуют в подготовке ряда информационных и справочных изданий по расследованию электронных преступлений, проводят тренировочные занятия для полицейских.

Кроме того, под эгидой рабочей группы создана система раннего предупреждения компьютерных преступлений, сотрудники которой находятся на дежурстве двадцать четыре часа и стараются координировать действия киберполицейских в разных странах.

В октябре 1995 года на 64-й сессии Генеральной Ассамблеи Интерпола была принята следующая рекомендация:

«Проблема борьбы с преступностью, связанной с незаконным использованием компьютеров, должна решаться в одинаковой степени в африканском, американском и азиатском регионах и каждым членом Интерпола в этих регионах, с оказанием возможной помощи Генеральным секретариатом на региональном уровне.

Создать Координационный комитет в составе небольшой группы экспертов из различных регионов для координации и реализации всех региональных инициатив, стимулирования единообразия в методах расследования международных компьютерных преступлений. Поручить Генеральному секретариату внести соответствующие положения по достижению этих целей в ближайшее время»[69].

Спустя несколько лет по образцу Европейской Рабочей группы были сформированы аналогичные организации и в других регионах мира: в 1998 году в Африке, куда вошли представители ЮАР, Зимбабве, Намибии, Танзании, Уганды, Ботсваны, Занзибара, Свазиленда, Лесото и Руанды; в 2000 году в Азиатско-Тихоокеанском регионе (Австралия, Китай, Индия, Япония, Непал, Шри-Ланка) и в Америке (США, Канада, Чили, Аргентина, Колумбия, Ямайка, Багамы).

В 1998 году сотрудники одного из специализированных подразделений Департамента торговли США совместно с экспертами корпорации RAND провели ряд исследований с целью анализа и выявления возможных путей использования современных систем электронных платежей для осуществления операций по отмыванию незаконных финансовых средств.

Системы электронных платежей оказались в сфере интереса Белого дома, Конгресса Соединенных Штатов и ряда других структур. В июле 1997

---

[69] Выписка из резолюции Генеральной Ассамблеи Интерпола, 4-10 октября 1995 г. (http://newasp.omskreg.ru/bekryash/app1.htm)

года, Президент представил доклад относительно Глобальной информационной инфраструктуры (GII), озаглавленный «Основа глобальной электронной торговли» часть которого непосредственно адресована значению систем электронных платежей.

Системы электронной оплаты также удостоились самого пристального внимания и на международном уровне. Многосторонние обсуждения и изучения были предприняты рабочими группами по противодействию отмыванию незаконных средств (FATF) «большой семерки». В июне 1996 года, была добавлена новая рекомендация за № 13 к Рекомендациям FATF. Она констатирует, что «…все страны должен обратить особое внимание на схемы отмывания денег, свойственные новым или развивающимся технологиям и предпринимать меры, если необходимо, для предотвращения их использования в подобных схемах…».

Классические кредитные или дебетовые карты позволяют их владельцам купить товары и услуги без использования наличных денег, но неизменно вовлекают посредническое финансовое учреждение или эмитента кредитной карты. Напротив, основная характеристика многих современных систем электронных платежей связано с устранением регулирующего третьего лица (например, банка) при передаче денежных средств между двумя (или более) объектами. Возможность передачи наличности через информационные сети без посредничества значительно понижает затраты на совершение сделок. Как результат - экономическая конкурентоспособность и эффективность расширяют пространство сетевого обеспечения, что позволяет значительно расширить круг пользователей подобных услуг, которые в свою очередь требуют новые типы инструментов оплаты.

Глобальные масштабы подобных систем и тот факт, что передача наличности может иметь место с высокой скоростью и степенью анонимности, которая препятствует надлежащему контролю правительственными структурами, является серьезным поводом для беспокойства правительств ряда стран.

2.9.1. Проблема легализации незаконных финансовых средств международными террористическими организациями

Легализация незаконных финансовых средств или «отмывание денег» - это нелегальная деятельность, посредством которой легализуются преступные доходы. Это функция свойственна практически всем действиям по созданию прибыли преступными сообществами. Так Уголовный кодекс США содержит больше 100 статей, нарушения которых относится к категории преступлений, связанных с отмыванием денег. Эти нарушения охватывают области деятельности от торговли наркотиками и финансового мошенничества, до похищения и шпионажа.

Большинству финансовых транзакций свойственен некоторый след, однозначно привязывающий сумму к конкретной персоне. Преступники избегают использовать традиционные платежные системы типа чеков, кредитных карточек, и т.д., именно в силу наличия этого следа. Они предпочитают использовать наличность потому, что это анонимно. Физическая наличность, однако, имеет весьма существенные неудобства. Прежде всего - это большой объем и масса. Например, 44 фунта кокаина, стоящего 1 миллион долларов, эквивалентен 256 фунтам наличности суммой в 1 миллион долларов. Наличность больше чем шесть раз превышает вес наркотиков. Существующие платежные системы и наличность - это большие проблемы для преступников. И гораздо больше они для больших межнациональных групп организованной преступности. Законодательное регулирование и банковский контроль увеличили их затраты и риски, связанные с отмыванием средств.

Физическое перемещение больших сумм наличности – самая большая проблема для тех, кто занимается отмыванием денег. Чтобы лучше понимать потенциал для злоупотребления системами электронных платежей с целью отмывания денег, приведем краткое объяснение того, как преступники "узаконивают" наличность через традиционный процесс отмывания денег.

Размещение, *иерархическое представление* и *интеграция* - термины, обычно используемые, чтобы описать три стадии, через которые легализуются преступные доходы.

Размещение. Размещение - первая стадия в процессе отмывания денег. Именно в течение стадии размещения физическая валюта вводится в

финансовую систему, и нелегальные доходы наиболее уязвимы к обнаружению. Когда незаконные суммы денег успешно депонированы в финансовом учреждении, размещение произошло. Законодательно установлено несколько типов транзакций, о которых работники банка должны информировать правоохранительные органы. Преступнику требуется скрывать свои действия, в силу чего им необходимо либо полностью обойти законную финансовую систему, либо нарушить установленные правила. Соответственно, официальные лица, следящие за соблюдением законов, работающие в сотрудничестве с финансовой сферой, находятся в уникальной позиции, способствующей пресечению отмывания денег на этой стадии.

Иерархическое представление. Иерархическое представление описывает деятельность, предпринимаемую с целью затенить след, который оставляет вексель, оплаченный "грязными" деньгами. В течение стадии иерархического представления преступник может проводить ряд финансовых транзакций, чтобы создавать уровни между средствами и их незаконным источником. Например, ряд переводов денежных средств от банка к банку составил бы иерархическое представление. Подобные действия могут быть столь запутанными, что отследить маршрут денег становится очень сложно.

Интеграция. В течение это, конечной стадии в процессе отмывания, незаконные фонды объединяются с суммами денег от законных коммерческих действий, поскольку они вводят в экономику. Таким образом, незаконные средства приобретают законность. Интеграция незаконных сумм денег в законную экономику очень трудно обнаружить, если контрольный след не был установлен в течение стадий иерархического представления или размещения.

2.9.2. Схемы легализации незаконных финансовых средств международными террористическими организациями

Схемы отмывания денег могут сильно изменяться по характеру и сложности. Они могут вовлекать любой число посредников и использовать традиционные и нетрадиционные платежные системы. В большой степени, возможности и характер операции отмывания денег ограничены только творческим потенциалом лиц, их проводящих. Международные наркоторговцы могут использовать множество различных методов

отмывания денег и схем, каждая из которых специально создавалась, чтобы выполнить определенные задачи и достичь определенной цели.

Передовые компьютерные технологии и технологии связи в настоящее время обычно используются, чтобы увеличить эффективность и защиту связанных с наркотиками действий по отмыванию денег. Примеры, которые следуют ниже - базовые схемы, предназначены для ознакомления читателей с несколькими простыми методами для перемещения незаконных средств.

Пример 1: Перемещение средств, полученных незаконным путем в США, в третью страну для использования в местной экономике.

1. Продажа наркотиков осуществляется в США (наличность - привилегированная форма расчетов за эти транзакции.).

2. Наличность от одной или множества точек продаж накапливается в бандитском притоне для обработки.

3. Наличность передается для пересылки из страны. Чтобы избежать внимания со стороны правоохранительных органов или банка, наличность может быть разделена на суммы меньше минимально контролируемой суммы (например, 10000 долларов США) и "размыта" (для этой цели привлекается большое количество индивидуумов, чтобы сделать небольшие по сумме депозиты) или структурируется (суммы передаются порциями ниже федеральных требований информирования).

4. Средства пересылаются посредством перевода американским отправителем своему иностранному коллеге.

5. В третьей стране переводы выплачиваются уже в национальной валюте.

Пример 2: Перемещение отмытых денег из США в третью страну.

1. Деньги от продажи наркотиков в США переводятся в платежные поручения.

2. Платежные поручения отправляются в третью страну экспресс-почтой.

3. Американские платежные поручения продаются валютному маклеру за национальную валюту страны.

2.9.3. Системы электронных платежей

В настоящее время существуют и разрабатываются системы электронных платежей нескольких видов. Между тем, сегодня доминируют два универсальных типа систем: системы на основе смарт-карт, хранящих сумму наличности, и платежные системы на основе сети Internet. Последние разработки показывают, что эти два типа систем останутся доминирующими и в ближайшие годы.

В настоящее время наблюдается значительный прогресс в разработке стандартов систем электронных платежей. Однако, вопросы финансового взаимодействия (взаиморасчет), и связанные с ними проблемы ответственности между компаниями-эмитентами в различных странах, являются сегодня существенным препятствием на пути продвижения платежных систем этого типа.

Некоторые особенности систем электронных платежей, такие как возможность передачи наличных средств на одном уровне от человека к человеку, при условии анонимности плательщика предлагают клиенту услуги со свойствами гибкости и удобства в обращении с наличностью вместе с расширенной способностью провести закупки на почти глобальном пространстве.

Ниже описываются четыре основных типа построения систем электронных платежей:

1. Модель на основе торговой компании, выполняющей функции эмитента карточек. В этой модели эмитент смарт-карт и продавец товаров – одна и та же компания.

2. Модель на основе банка-эмитента. Торговая компания и эмитент карт в этой модели различные стороны. Транзакции осуществляются через традиционные финансовые системы.

3. Модель, в которой эмитент – небанковская компания. Пользователи покупают электронную наличность у эмитентов, используя традиционные деньги, и тратят электронную наличность в компаниях-участниках системы. Эмитент впоследствии выплачивает электронную наличность фирме-продавцу

4. Одноранговая модель. Банк или небанковское учреждение выступает в качестве передаточного звена между потребителями. Точка контакта между традиционной системой платежей и электронной наличностью - начальная закупка электронной наличности у эмитента и выплата электронной наличности со стороны отдельных личностей или торговых фирм.

Все четыре модели позволяют легко добавлять наличные суммы или перемещать их между карточками с использованием различных средств.

2.9.4. Потенциальное использование систем электронных платежей для отмывания денег

Исследование, проведенное экспертами корпорации RAND, было сосредоточено на поиске и исследовании тех возможностей систем электронной оплаты, которые могут быть использованы для осуществления операций по отмыванию незаконных финансовых средств. По своей природе системы электронных платежей имеют потенциал, позволяющий решить одну из самых серьезных проблем для теневого бизнеса - физическое перемещение больших количеств наличности.

Глобализация многих существующих систем электронных платежей дает возможность преступникам использовать национальные различия в стандартах защиты и правилах надзора, чтобы скрыть движение незаконных средств.

Выполненные исследования идентифицировали множество особенностей транзакций в системах электронных платежей, которые правоохранительные органы должны внимательно изучить. Среди них - (1) отказ от посредничества; (2) банк или небанковское учреждение в качестве эмитента карт; (3) одноранговые транзакции; (4) операционная анонимность и (5) пределы номинирования и даты истечения срока действия карт.

Каждая из этих базисных особенностей ниже описана более подробно. С одной стороны эти базисные особенности делают системы электронных платежей привлекательными в качестве потенциальных средств, позволяющих уменьшить стоимости транзакции в торговле и способствовать увеличенной эффективности экономики, с другой - эти особенности определяют и те уязвимости, которые могут использоваться преступниками.

Отказ от посредничества. Исторически правоохранительная деятельность и регулирующие организации положились на посредничество банков и других регулируемых финансовых учреждений, чтобы обеспечить "точки перехвата", через который средства должны проходить и где возможно получить полный отчет об их происхождении.

Отказ от посредничества вовлекает передачу средств между объектами без промежуточного вовлечения третьего лица, подчиненного правительственному надзору (например, требования регистрации через банк). Если системы электронных платежей разрешают передачи средств без посредничества в неограниченных количествах, преступники могут использовать это как возможность избежать традиционных методов отслеживания перемещения денежных средств.

Банк и небанковское учреждения в качестве эмитента карт. Банки и небанковские учреждения могут быть подчинены различным правилам относительно их операций с системами электронных платежей. Это различие уже имеет место в нескольких странах, где небанковское учреждение эмитенты карт систем электронных платежей в настоящее время подчиненно набору правил, отличному от такового для банков. Простое расширение требований, сформированных ранее для традиционной платежной системы, к новому небанковскому учреждению-эмитенту карт может вызвать ряд претензий со стороны клиентов о возможных злоупотреблениях.

Однако новые системы построены по-другому и постоянно видоизменяются, так что принцип "один размер соответствует всему" не будет оптимальным.

Одноранговые передачи. Некоторые системы электронных платежей позволяют потребителям передавать значение одноранговый (и таким образом, без посредника) использование электронной "инкассаторской сумки", телефона, или Internet. Такая возможность возможно таит в себе прямой вызов правительственному надзору в системах электронных платежей. При отсутствии сведений или доказательств из других источников (например, физическое наблюдение), одноранговые передачи, вряд ли, могут быть обнаружены.

Операционная анонимность. В некоторых находящихся на стадии становления системах электронных платежей, точка введения средств в систему непрозрачна и тождество объекта, передающего их, весьма трудно определить. Фактически анонимность плательщика (тождество стороны, инициализирующей передачу наличности в систему электронных платежей) – основная характеристика некоторых предложенных систем. При передаче наличности в систему электронных платежей (например, через Internet или телефонную сеть) операционная анонимность могла бы стать почти непреодолимым барьером для обнаружения таких операций. В то время как варианты решения для этой проблемы были выдвинуты, они поднимают проблемы относительно сохранения тайны частных вкладов.

Пределы номинирования и даты истечения срока действия карт. Создатели систем электронных платежей, вероятно, ограничат максимальные суммы, которые могут быть сохранены на карточках, уменьшая тем самым риск мошенничества или других потерь. Как с кредитными карточками, эмитенты систем электронных платежей также вероятно установят пределы достоинства на основе потребностей, которые были бы определены рекламой и конъюнктурными факторами. Так недавние испытания потребителя систем электронных платежей указывают вероятные пределы потребителя приблизительно 1,000 $ - 3,000 $. Системы электронных платежей, между организациями, вероятно, будут иметь намного больший предел номинирования чем те, для индивидуальных клиентов, и будут широко различаться между фирмами.

Карты в системе электронных платежей могут быть запрограммированы так, чтобы прекращать свою работу после некоторого числа передач.

Чем больше электронные платежные системы подражают валюте, тем больше вероятность того, что записи о транзакции будут ограничены. Так в некоторых образцах, может фиксироваться только ограниченное число самых последних транзакций.

2.9.5. Некоторые примеры по использованию систем электронных платежей для отмывания денежных средств

Оба рассматриваемых примера основываются на использовании высокономинальных смарт-карт.

Сбыт наркотиков

В этом примере наркотики продаются пользователям в обмен на одноразовые карточки, номиналом, типично связываемых с транзакциями наркотиков - 20$, 50 $, или 100 $. Эти карточки собираются торговцем наркотиками и реализуются через подставную фирму в области розничной торговли. Эта фирма передает электронное значение карточек со своих терминалов в банк. Фирма получает некоторую плату за использование ее возможностей.

Как только средства введены в законную платежную систему, они перемещаются по всей цепочке стандартного процесса отмывания и вводятся в экономику третьей страны.

Два типа передачи наличности в системах электронных платежей

В этом примере средства, полученные от деятельности незаконного оборота наркотиков, и размещенные на смарт-карте могут быть переданы, по крайней мере, двумя простыми способами. Возможно наиболее предсказуемый способ движения средств - через физическое перемещение высоко номинальных карт, содержащие доходы незаконного оборота наркотиков. Из-за их небольшого размера эти карточки могут быть легко и надежно скрыты, и в конечном счете быть обналиченными через повторное депонирование, но уже в зарубежной стране.

Второй путь транспортировки средств вне досягаемости полномочий правоохранительных органов может состоять в передаче средств на карточке по телефону. И сотовые и обычные аналоговые телефоны легко взаимодействуют с различными сервисами, позволяющими выполнить подобные операции.

Как только фонды вводят платежную систему, они являются неотличимыми от фондов, полученных из законных источников.

Переводы денежных средств через системы на основе Интернет

В этом примере с низко номинальных карт значение передается на персональные компьютеры, которые передают это значение по Internet, используя все более и более доступные анонимные сервисы, чтобы скрыть пункты поступления незаконных средств. Получатель средств имеет

возможность объединить низкономинальные платежи и повторно интегрировать их в платежную систему.

Электронные деньги и всемирная паутина

Последний пример незаконного использования системы электронных платежей проводится под флагом милосердия, которое служит только прикрытием для получения денежных переводов в виде пожертвований. Фонды, изначально созданные как благотворительные, и честно выполнявшие свою миссию, вместе с тем могли выступать в качестве одного из звеньев цепочки по отмыванию преступных средств с использованием систем электронной оплаты.

В таких системах денежные средства могли быть переведены из электронных кошельков на компьютерах владельцев на банковский счет, а затем перечислены из одного финансового учреждения в другое, расположенное в произвольном месте планеты, законы которого наиболее благоприятны для инвестирования незаконных средств в реальную экономику.

2.9.6. Методы борьбы с легализацией незаконных финансовых средств международными террористическими организациями

Участники проведенного исследования, вне зависимости от их взглядов на отдельные вопросы, сошлись во мнении, что участие правительства необходимо. Оно требуется для начала диалога о том, как обеспечить соответствующее регулирование и организацию действий правоохранительных органов, необходимых для налаживания эффективной работы систем электронных платежей как действующих, так и находящихся в стадии проектирования. Сегодня правительство США, понимая роль и место систем электронных платежей в процессе формирования бюджета мировых террористических организаций, активно участвует в работах по предотвращению использования передовых технологий в финансовой сфере для финансирования преступного сообщества.

Анализ существующих и перспективных технологий и технических особенностей нового класса систем - первый шаг к пониманию применения в их отношении существующих правоприменительных норм, а также шаг на

пути формирования новых законодательных актов. Как известно, большинство систем электронной оплаты разрабатываются коммерческими фирмами. Наличие конкуренции в этой сфере позволяет организовать работы с привлечением самых совершенных информационных технологий. В этой связи желательно, чтобы правительство развернуло диалог с частным сектором по вопросу совершенствования нормативной и правовой базы по системам электронных платежей, включая обеспечение информационной безопасности в таких системах. Информация, полученная в результате проведенного исследования способствовала проведению тщательной оценке угроз безопасности, характерных для систем электронных платежей.

Какие выводы можно сделать после изучения материалов RAND по вопросу использования систем электронной оплаты для отмывания денег? Прежде всего – это то, что исследования показали существование широкой области проблем, связанных с обеспечением контроля в системах такого рода, а также связанных с обеспечением информационной безопасности. Существующая правоприменительная практика не всегда может эффективно решать вопросы, связанные с предотвращением использования систем электронных платежей для отмывания денег.

Необходимо широкое сотрудничество и совместные действия правительства и разработчиков систем электронных платежей, а также правительств ведущих государств с тем, чтобы перекрыть каналы легализации незаконных финансовых средств с использованием систем электронных платежей. Международное сотрудничество, практически, единственный действенный способ реально перекрыть такие потоки.

Сотрудничество в области стандартов, регулирующих прозрачность, и активный контроль за возможной эксплуатацией выявленных уязвимостей в интересах преступных группировок является ключевым фактором успешной защиты систем электронной оплаты от злоупотребления. Кроме того, сама проблема отмывания денег международная. Эффективная правоприменительная деятельность требуется, чтобы национальные правительства сотрудничали в урегулировании основных правил создания систем электронных платежей и операций с их применением.

Выполненное исследование послужило своеобразным полигоном, на котором прототипы подобных международных действий в рамках отработки политики функционирования систем электронных платежей были отработаны. В будущем планируется расширение средств и методов моделирования с целью включить международных участников, а также учесть более глубокое понимание вызовов, связанных с легализацией незаконных финансовых средств с использованием систем электронных платежей. Исследование высветило также важность согласования подходов к контролю за системами электронных платежей.

Пока еще преждевременно говорить о формировании проекта всестороннего регулирующего режима для систем электронных платежей, сегодня необходим расширенный и более глубокий диалог между компаниями-эмитентами кар, правительством и разработчиками систем поможет сформировать направление такого режима. Понимание проблем, поставленных в изложенном материале, поможет в продвижении общественных дебатов по организации надежной защиты системы электронных платежей и в определении необходимой роли для правительства в этом быстро растущем секторе Глобальной информационной инфраструктуры.

2.10. Информационное и технологическое превосходство – основа достижения «всеохватывающего господства» США в XXI веке

Американские военные эксперты отмечают, что основой достижения всеохватывающего господства в ближайшие десятилетия должны стать информационное и технологическое превосходство. Развитие «революции в военном деле» привела к тому, что в середине 90-х годов прошлого века была предпринята попытка интегрировать достижения в передовых отраслях науки и техники в военную науку, а также определить основное направление трансформации вооруженных сил США в следующем столетии. Попытка определить такое направление была предпринята в документе Комитета начальников штабов «Единая перспектива – 2010» (Joint Vision 2010), который является концептуальной основой ведения совместных операций и боевых действий будущего и отражает взгляды стратегов Пентагона на

проблемы ведения операций в эпоху становления информационного общества. Он определяет направления перспективного развития видов Вооруженных сил в условиях глобализации всего мира, делая упор на обеспечении их эффективного взаимодействия. В соответствии с документом «Единая перспектива – 2010», основной составляющей кардинального повышения боевых возможностей вооруженных сил является достижение информационного и технологического превосходства, которое преобразит современные понятия о маневре, ударе, защите и тыловом обеспечении и приведет к появлению новых оперативных концепций господствующего маневра, высокоточного сражения, целенаправленного тылового обеспечения и всеобъемлющей защиты. Реализация этих концепций, по мнению экспертов, даст возможность проводить решительные операции в любых условиях обстановки, то есть достичь качества, которое в документе «Единая перспектива – 2010» определяется как ***«всеохватывающее господство»***.

Если главная задача в реализации информационного превосходства США в общем ставится, как достижение в качестве национальной цели информационного доминирования по отношению к любой враждебной национальной или транснациональной общности то, в свою очередь, Министерство обороны США, нацеливаясь на создание мощной информационной системы для театра военных действий, полагает, что она сможет обеспечивать военных информацией такого уровня и качеств, которые не были доступны ранее.

Планируемые на уровень 2010 г. характеристики информационной системы для театра военных действий дадут потребителям возможность получить намного более качественную его визуализацию (как по времени, так и в пространстве) и обеспечить концентрацию усилий рассредоточенных подразделений на решаемых задачах. Интегрированная из коммуникационных сетей и сетей датчиков, программного обеспечения и организационных структур, информационная система предоставит:

- надежную и качественную связь для подразделений;
- оперативную информацию о ходе операции;
- точные и своевременные разведывательные данные о местоположении и действиях противника;

- каталог баз данных, относящихся к зоне операции и способностям противника, а также доступ к этим базам;
- точное положение дружественных сил и их боевой статус (в реальном времени);
- способность проведения операций на всем театре военных действий, выполняемых непрерывно с рассредоточенных мест проецирования силы;
- обработку в реальном времени информации, дающей общую картину ситуации, складывающейся на театре военных действий;
- встроенные способности самозащиты (с многоуровневой защитой доступа), позволяющие распределять информацию среди организаций, союзников, неправительственных организаций.

Информационные системы театра военных действий - это совокупность подсистем для сбора, обработки анализа, архивирования и распределения информации, которые, собственно, и призваны обеспечить достижение информационного превосходства над противником. При сосредоточении на имеющемся или потенциальном противнике информационные системы, собирающие данные, охватывают открытые источники, традиционную разведку, системы наблюдения и обнаружения. Собранные данные становятся информацией после их обработки и приведения к виду, удобному для пользования. Для удовлетворения специфических запросов потребителя такая информация может трансформироваться в разведывательную - в случае применения к ней целенаправленного анализа, интерпретации, сличения с относящейся к запросам другой информацией и общим информационным фоном.

В эпоху становления информационного общества во многом изменился и характер выполнения своих задач разведкой. Теперь, в качестве основной задачи, возложенной на разведывательные службы, кроме задачи опережающего оповещения высшего руководства страны о возможной агрессии, возложена и задача в достижении информационного превосходства над противником. В качестве развития средств ведения компьютерной разведки в последнее время упоминается виртуальная архитектура объединенной разведывательной информации (Joint Intelligence Virtual Architecture, JIVA). Она позволяет перераспределить технические и

программные ресурсы и формировать «виртуальную разведывательную рабочую среду», – особое подпространство в пространстве информационном. В нем осуществляется скоординированный просмотр, согласование, утверждение и распределение конечной разведывательной продукции.

Технологическое опережение в области информатизации США принимают как одну из главных предпосылок реализации своего информационного преимущества. В то же время военные аналитики США констатируют, что современные информационные технологии доступны любому, кто имеет финансовые возможности получить их. Постоянно увеличивающиеся распространение и доступность информации создают для потенциального противника (при растущей зависимости США от информации и информационных систем) предпосылки достижения временного или локализованного паритета в боевом пространстве или асимметричного преимущества. Быстрое внедрение перспективных технологий делает возможным неожиданное появление асимметричных угрожающих способностей у широкого круга потенциальных противников. Ожидается, что уровень интенсивности информационных операций, проводимых противником и в мирное время, повысится с эскалацией кризисной ситуации.

Планируется, что к 2010 г. вооруженные силы получат в распоряжение интегрированную архитектуру принятия решений, базирующуюся на искусственном интеллекте, нанотехнологиях, эффективном синтезе информации, многофункциональных процессорах со способностью поддерживать принятие решений в реальном времени, технологиях сжатия данных для повышения скорости обработки. При этом использование командованием информационных систем с подключением установок искусственного интеллекта, как операционных умножителей эффективности боевых действий, окажет влияние на доктрину, организацию и обучение вооруженных сил. В частности, моделирующие установки позволят в интегрированном и интерактивном режиме прогнозировать варианты действий, менять их тактику, принимать решения и действовать.

Приобретая эффективные наступательные (как правило, превентивные) и оборонительные информационные способности, США, естественно, стремятся не только защищать свои системы от «кибернетических атак», но и

быстро находить их источник и давать адекватный «ответ» на любом уровне действий, вплоть до его физического уничтожения.

2.11. Современные тенденции в области защиты информации и информационной борьбы

Сегодня российские и иностранные эксперты отмечают, что большинство современных средств обеспечения информационной безопасности не обладают достаточной эффективностью при организации противодействия специальным программно-математическим воздействиям. Более того сегодня практически не существует теоретических основ, средств и методов организации противодействия информационному нападению. Все существующие на настоящий момент теоретические наработки относятся к организации защиты информации от единичных случаев нарушения санкционированных прав доступа к информации.

Между тем исследования, проведенные за последние пять лет в России и за рубежом, показали, что качественно новый уровень защищенности сложных и многофункциональных автоматизированных систем может быть достигнут лишь за счет реализации адаптивного управления процессами защиты информации. При этом под "адаптивным управлением" понимается процесс целенаправленного изменения параметров и структуры системы защиты информации с целью поддержания требуемого уровня защищенности информационной системы /21/.

Об актуальности проблемы свидетельствует образование 21 октября 1998 г. «Альянса адаптивной безопасности сети», объединившего более 70 крупнейших мировых предприятий промышленности, работающих в области информационных технологий. Целью создания Альянса является повышение защищенности автоматизированных систем на основе разработки и внедрение технологий адаптивного управления.

Новый подход к обеспечению безопасности заставляет искать пути решения проблемы защиты информации в теориях, основные результаты которых лежат в междисциплинарной области. Среди них выделяют теорию эволюционных вычислений, теорию нейронных сетей, теорию нечетких

множеств и синергетику. Считается, что наиболее перспективным подходом к созданию систем защиты информации будущего является синергетический подход. Синергетический подход к исследованию процессов самоорганизации сопровождается отказом от традиционных методов редукционизма, когда сложные процессы пытаются свести к простым и элементарным, а тем самым игнорируется их сложность. В синергетике в противоположность кибернетике исследуются механизмы возникновения новых состояний, структур и форм в процессе самоорганизации, а не сохранение или поддержание форм старых. Именно поэтому она опирается на принцип положительной обратной связи, когда изменения, возникшие в системе, не подавляются или корректируются, а, наоборот, постепенно накапливаются и приводят к разрушению старой и возникновению новой системы, адекватной среде ее функционирования. Таким образом, самоорганизация выступает как источник эволюции систем, так как она служит началом процесса возникновения качественно новых и более сложных структур в развитии системы /21/.

2.11.1. Возможные направления совершенствования атакующего информационного оружия

Пересмотр основных направлений развития систем информационной безопасности вызвал ответную реакцию со стороны разработчиков средств атакующего информационного оружия или средств специального программно-математического воздействия.

Прежде всего, это отразилось на пересмотре основ тактики ведения боевых информационных действий.

Учитывая, что современные компьютерные сети обладают весьма значительной структурной устойчивостью, делается упор на отработку проведения массированных информационных атак, ставящих своей целью нарушить нормальное функционирование компьютерных сетей, путем блокирования доступа к информационным ресурсам.

Успешной реализации этого подхода способствует два обстоятельства:

- массовое распространение средств корпоративной электронной почты (MS Outlook, Lotus Notes), обладающих рядом существенных недостатков;

- массовое распространение систем управления функционированием сетей (HP Open View и др.), алгоритмы управления потоками в которых, также имеют серьезные недостатки.

Примерами успешного проведения атак с использованием уязвимостей указанных выше программ могут служить события, связанные с распространением вируса Melissa, когда на несколько дней были парализованы системы электронной почты многих компаний.

К сожалению, проблема макровирусов (к которым принадлежит и Melissa) в настоящее время не решена.

Сегодня уже разработан ряд алгоритмов, позволяющих писать вирусы, которые принципиально нельзя будет обнаружить ни одним из существующих способов ни сегодня, ни в ближайшем будущем.

Ряд специалистов отмечает[70], что вирус, написанный на виртуальной машине, требует очень много времени для анализа традиционными методами. Если такие вирусы распространяться, то вряд ли существующая антивирусная промышленность сможет с ними эффективно бороться. Это вполне закономерно. Вирусы рано или поздно должны были усложниться до той степени, когда несколько специалистов при помощи “ручного” анализа уже ничего не смогут сделать.

Наряду с проблемой массированных атак с использованием макровирусов и систем электронной почты, в последнее время получила огласку информация о работах в области создания “кибернетических организмов”.

Это небольшие (от 50 до 100 строк кода) программы, которые автоматически генерируются специальными пакетами программ с использованием алгоритмов генетической оптимизации, для минимизации длинны кода. Внедрение такой программы в автоматизированную систему управления воздушным движением позволит парализовать работу крупного авиационного узла всего за несколько десятков минут.

Программа по разработке этого вида СПМВ получила название CVCM (Computer Virus Countermeasures).

---

[70] Крис Касперски “Вирусы: вчера, сегодня, завтра” // BYTE Россия, № 6(10) 1999, с. 52-55.

При этом наиболее перспективным способом внедрения таких программ является способ дистанционного внедрения. При реализации этого способа используется дистанционное поражение автоматизированной системы путем наведения на нее вируса с помощью направленного электромагнитного поля, модулированного кодом вируса.

В ряде информационных источников, связанных с перспективной системой космической связи Teledesic, встречается термин «пакет вложения», который может рассматриваться именно как подобного рода «кибернетический организм».

Еще одним направлением в совершенствовании информационного оружия является создание сети интеллектуальных программ-агентов, на которые обычно возлагаются функции обеспечивающего информационного оружия. Одной из таких разработок является программа GenPage и Genetix[71, 72]. Системы таких программ-агентов положены в основу формирования виртуальной архитектуры объединенной разведывательной информации (Joint Intelligence Virtual Architecture, JIVA).

2.11.2. Компьютерное моделирование как вид информационного оружия

Как отмечалось выше, целью боевых информационных операций является достижение и удержание информационного превосходства. Достичь информационного превосходства над противником, это значит более полно промоделировать поведение противника в различных ситуациях, что дает возможность определить собственный алгоритм поведения и реализовать его. Полнее моделировать противника - значит в больших объемах собирать, хранить и обрабатывать информацию о противнике; это значит более полно изучить поведение противника – знать и понимать его историю, религию, быт /30/. Поэтому в последнее время появились публикации[73], в которых авторы утверждают, что компьютерное моделирование, направленное на прогнозирование развития социальных ситуаций, есть не что иное, как

[71] GenePage from Steinkrug Publications http://www.steinkrug.com
[72] ComputerWorld №8 (121), 10 марта 1998г.
[73] А.С. Овчинский. Информационно-психологическая сфера противодействия организованной преступности. // Информационное общество. № 1, 1997, с. 41-46.

информационное оружия. Учитывая высокую сложность математических моделей социума как мегасистемы[74], одним из перспективных направлений решения задач подобного уровня являются генетические алгоритмы.

2.12. Изменения в области защиты информации после терактов в США 11 сентября 2001 года

Потребность быть «все более и более открытыми», обеспечивать диалоговые решения для пользователей и клиентов все больше вовлекают в сферу бизнеса возможности глобальной сети Интернет. Это в свою очередь обязывает использовать инструменты и процедуры, нацеленные на защиту их информационной системы, такими способами и в такой степени, которые еще пару лет были просто фантастикой.

В дополнение к удовлетворению потребности в обеспечении защиты информации, сегодня компании должны эффективно управлять все более и более сложными информационными системами, на которые они теперь полагаются в своем бизнесе. У истоков, так называемой «новой экономики», информационные системы были намного менее сложными и имели дело, как правило, только с внутренними процессами корпораций. В случае же, если присутствовали внешние связи, то они были немногочисленными и поэтому легко контролировались. Более того, любая система почти всегда взаимодействовала только с такими же «закрытыми» структурами.

Все это позволяет говорить о том, что защита информации не является продуктом только нашего времени. Напротив, компьютеры уже давно и успешно используются в сфере обороны, промышленности и в финансовой сфере, где без защиты не обойтись. Важным отличием текущего момента является то, что сегодня большая часть решений в области информационных технологий все более и более используются в частном секторе экономики и дома. Это в свою очередь ставит и принципиально новые вопросы обеспечения этого потребительского сектора средствами и системами защиты информации и конфиденциальных данных от несанкционированного доступа.

---

[74] Handbook of System Science. European Systems Union/ Decleris M/ (ed), Athenai, 1991.

Ряд экспертов уверены, что надежная защита информации - одно из существенных требований, которое должно быть реализовано прежде, чем бизнес компании будет в значительной мере связан с Интернет. Информационная безопасность сегодня должна стать наиболее известным и важным компонентом в политике развития любой компании, ее технологической и организационной структуры.

По мнению российских и зарубежных экспертов рост потребностей в средствах защиты связан с целым рядом причин: от угрозы террористических актов в отношении важных объектов экономики, до активизации конкурентов, которые все чаще стали использовать средства несанкционированного получения информации из информационных систем оппонентов.

Интересно, но компьютерный бум 90-х годов прошлого века практически не затронул индустрию средств защиты информации. Во всяком случае, она развивалась гораздо медленнее, чем лавина интернет-проектов. Однако ничего не проходит бесследно и то, что создавалось «на скорую руку» в 90-х годах сегодня, спустя всего несколько лет, уже начинает ломаться. Более того, в 90-х годах еще не существовало такой угрозы как «международный высокотехнологичный терроризм», поэтому создаваемые системы и не рассчитывались на функционирование в условиях воздействия поражающих факторов хакеров-террористов.

Вот почему трагические события в США 11 сентября 2001 года стали точкой отсчета не только для целого ряда специальных служб и правоохранительных органов, но и для разработчиков информационных систем и производителей средств защиты информации.

Именно эти трагические события добавили остроты в необходимость решения накопившихся проблем в области защиты информации. Они во многом реанимировали дебаты о необходимости неотложных мер по нормализации ситуации с обеспечением защиты информации и информационной безопасностью в сфере бизнеса и заставили руководство ряда компаний по иному взглянуть на проблемы обеспечения устойчивости собственного бизнеса, обеспечения конфиденциальности, целостности и доступности информационных ресурсов.

В тот трагический день впервые мишенью террористов стали не военные объекты, а крупный центр мирового бизнеса. Вместе с трагизмом ситуации в целом, профессионалам невозможно было не отметить ряд важных моментов. Так, несмотря на громкие заявления американских коллег с нью-йоркской биржи об устойчивости функционирования информационной инфраструктуры, торги не проводились неделю, что практически спровоцировало панику в деловых кругах.

Вот как оценивается ситуация, сложившаяся в области защиты информации, американскими специалистами из Альянса безопасности Интернета (ISAlliance), Национальной ассоциации производителей (NAM) и экспертами RedSiren Technologies Inc.[75]

Целью проведенного опроса 227 специалистов в области информационной безопасности в ряде стран мира было выяснение ситуации в области информационной безопасности, сложившейся после трагических террористических нападений на Центр международной торговли и Пентагон в сентябре 2001 года.

В целом, результаты показывают, что большинство респондентов согласилось с тем, что информационная безопасность сегодня - ключевой вопрос и его значение непрерывно возрастает. Однако в то время как 88 процентов из опрошенных чувствовали, что информационная безопасность существенна в деле обеспечения устойчивости их бизнеса и деловой жизнеспособности, 30 процентов сообщили, что их критическая деловая информация все еще недостаточно защищена. Кроме того, 45 процентов рассказали, что они совсем не готовы иметь дело с проблемами в области информационной безопасности и угрозами кибертерроризма и в случае возможной атаки им скорее придется закрыть свой бизнес, чем восстанавливать его «с нуля».

Как считают специалисты, ответы указывают, что в то время как большинство организаций уже находится на правильных позициях и имеет четкое представление о важности компьютерной безопасности, существенный процент все еще испытывает недостаток в адекватном восприятии угрозы со стороны высшего руководства компаний, которое

[75] Global Computer Security Survey—Results Analysis. <URL: http//www.redsiren.com>

необходимо для реализации комплекса мероприятий в области защиты информации.

Несмотря на то, что огромное большинство опрошенных (91 процент) признает важность информационной безопасность, почти одна треть (30 процентов) говорит, что их компании в настоящее время все еще не могут быть соответственно оборудованы, чтобы иметь дело с нападением на их компьютерные сети. 40 процентов сообщили, что информационную безопасность считают сегодня более важной, чем до событий 11 сентября 2001 г. Почти две трети опрошенных (67 процентов) сообщили, что руководство их компаний сделало проблемы информационной безопасности приоритетными. Однако, все же существенная часть (39 процентов) сообщила о том, что их предложения по совершенствованию информационной безопасности не были восприняты руководством.

Интересно, что проблема кибертерроризма расколола опрошенных: 48 процентов из них ответили, что нападения 11 сентября 2001 сделали их “более заинтересованными” в противодействии кибертерроризму и его возможным воздействиям на ресурсы их организации, в то время как 48 процентов не сообщили ни о каком изменении в своих планах.

Результаты также показывают важность распределения ресурса в обеспечении адекватной безопасности. Немного меньше чем половина (47 процентов) опрошенных сообщила, что они уже имели необходимый ресурс и до событий 11 сентября. Равное им число опрошенных (также 47 процентов) сказало, что их компании увеличили расходы на информационную безопасность в сравнении с прошлым годом, в то же время 38 процентов опрошенных указало, что эта тенденция продолжится и в 2003 г.

Большинство респондентов сообщили, что они имели достаточную физическую и информационною безопасность, а также разработанную и введенную в действие политику безопасности компании и до событий 11 сентября 2001. В тоже время почти 40 процентов сообщили, что они предприняли ряд мер по усовершенствованию средств защиты по всем областям, включая информационную. Это отражает тенденцию, согласно которой теперь организации считают уже не приемлемыми ряд категорий

рисков, которые до печальных событий ими даже не рассматривались и принимались как несущественные.

Большинство опрошенных сообщили, по крайней мере, об одном нападении на их информационную систему в прошлом году; 25 процентов сообщили об 1-5 нападениях; 10 процентов рассказали уже о 6-20 нападениях и 17 процентов сообщили о больше чем 20 нападениях. Однако 18 процентов не знают сколько раз их организации, были атакованы.

Результаты проведенного анализа подтвердили понимание необходимости совершенствования подходов к решению задач в области информационную область безопасности. Они также подтвердили, что проблемы кибербезопасности и угрозы конфиденциальности определенно становятся более осязаемыми для высшего руководства компаний. Однако результаты также демонстрируют, что приоритет и уровень предпринимаемых мер все еще неадекватны угрозам.

Эксперты отмечают, что целями любого проекта в области защиты информации компании должны быть:

- активная эффективная защита;
- обеспечение конфиденциальности коммерческой информации;
- гарантии клиенту;
- повышение гражданской и уголовной ответственности за нарушения в сфере защиты информации.

Чтобы достичь этих целей, весь процесс обеспечения надежной защиты должен охватить стратегию компании и организационные аспекты, а также включать обучение персонала компании, чтобы увеличить понимание с их стороны рисков, связанных с использованием информационных систем.

Информационная безопасность должна быть определена как «важнейшая» деятельность среди всех приоритетов компании. Она должна затрагивать всю организацию и корпоративную культуру компании, изменяя ее стратегию, структуру, системы, навыки персонала. Именно за таким подходом и есть будущее в построении систем защиты информации. Только так можно создавать надежные и устойчивые информационные системы.

Информационная безопасность означает гораздо больше, чем простое добавление нескольких программно-аппаратных средств безопасности к уже существующим средствам: отправная точка должна создать рабочую среду, в которой имеется необходимое представление о важности защиты информации и существуют способы анализа уязвимости системы.

Первый шаг в осуществлении эффективной стратегии защиты информационной системы должен начинаться с формирования политики безопасности компании. Эта политика должна определять правила в использовании и управлении системой. Даже самые лучшие технические средства не могут гарантировать безопасность, если они не используются вне установленных регламентов. Цель политики безопасности собственно и состоит в том, чтобы продвинуть безопасное использование и управление информационными системами на уровень управления всей компанией.

Согласно данным, представленным IDC, товарооборот решений в области безопасности должен существенно возрасти, увеличившись с 2 миллиардов евро в 2000 году, до 7 миллиардов евро - в 2005 г. Также, согласно прогнозам IDC, наиболее стремительным будет рост в области систем авторизации, администрирования и аутентификации в ущерб использованию межсетевых экранов и антивирусных программ.

Такой уровень расходов оправдан тем фактом, что количество инцидентов в области безопасности драматично увеличилось в период с 1988 года до 2001 года. Статистические данные, о которых сообщает CERT (Computer Emergency Response Team), показывают, что в 1999 было зафиксировано 3 859 инцидентов, а в 2001 году уже 34 754!

Результаты обзора, опубликованного в апреле 2001 компанией Sirmi, показывают, что рост числа проектов в области создания систем интерактивной торговли и банковских услуг, приведет к росту популярности следующих технологий обеспечения защиты информации: протокол SSL (70 %), третья доверенная сторона (центры доверия) (60%) и протокол SET (28.3 %); использование этих технологий приведет к росту числа использования смарт-карт и электронных денег (оба пункта вместе - 15 %).

Опрос 600 компаний, проведенных компанией Sirmi, показал, что среди опрошенных для обеспечения безопасности коммуникаций с использованием

Интерент используются следующие решения: 65.2 % используют лишь пароли; межсетевые экраны используют только 47.3 % опрошенных; 15.1% аппаратно разделяют внутреннюю сеть компании и внешнюю сеть (создают «интранет»); методы криптографической защиты используют сегодня всего 8.4 % компаний.

Согласно исследованию, выполненному компанией Colt-Idc, процедуры безопасности для физической защиты оборудования реализованы в 32 % опрошенных компаний. Стандартная стратегия, используемая 81 % из них, состоит в том, чтобы «запереть» сервер, а также регистрировать вход/выход в систему и все соединения. Достаточно широко для аутентификации используются различные токены (36%) и смарт-карты (24 %). 20 % респондентов выбрали непрерывный контроль действий в системе, и только 3 % используют биометрические системы контроля доступа.

В целом общий вывод для всех приведенных результатов анализа в области информационной безопасности и защиты информации показывает, что сегодня большинству компаний все же не хватает систематического и комплексного подхода к решению проблем защиты информации. Сегодня же, как правило, эти проблемы решаются от случая к случаю, без четкой системы и программы действий и уже после того, как инцидент имел место.

Таким образом следует полагать, что в ближайшие годы ситуация в области информационной безопасности и защиты информации будет ухудшаться, будет сказываться отсутствие необходимого количества квалифицированного персонала, а огромное количество новых вирусов и выявленных уязвимостей в программах сделают работу администраторов чрезвычайно сложной. Проявят себя и технические недоработки многих систем, создававшихся на заре компьютерно-интернетного бума 90-х годов прошлого века, - сложность и отсутствие четкой структуры многих информационных систем, а также отсутствие подсистемы защиты информации, заложенной на этапе проектирования системы, приведут к лавине отказов подобных «коленных» разработок.

В этих условиях на рынке станет распространяться новая услуга – аутсорсинг безопасности. Высококвалифицированные специалисты в области информационной безопасности будут объединяться в компании

предоставляющие услуги в области безопасности сразу целому ряду компаний, при этом целый ряд угроз безопасности и связанные с ними риски будут сведены к минимуму за счет крупных капиталовложений заказчиков в инфраструктуру компании, предложившей услугу аутсорсинга безопасности. Такая ситуация во многом будет характерна как для частного так и для государственного сектора.

Рост числа и вероятности реализации угроз безопасности информации нового класса, а также все более и более строгие регламенты использования разворачиваемых средств защиты ясно продемонстрирует потребность в дополнительных инвестициях, нацеленных на защиту информации компании, осуществления четкого и эффективного плана управления защитой информации.

2.13. Трансформация подходов к ведению информационной войны в современных условиях. Первое и второе поколение методов информационной войны

Изменение подходов в проведении внешней политики государства повлияли на оценку роли информационного противоборства в будущих конфликтах. Сегодня ряд американских военных специалистов придерживаются точки зрения, согласно которой информационное противоборство понимается ими гораздо шире, чем просто вид обеспечения операций вооруженных сил путем нарушения процессов контроля и управления войсками, радиоэлектронного подавления и др.

Основные результаты исследований, проведенных специалистами RAND в конце девяностых годов, были изложены в отчетах MR-661-OSD «Strategic Information Warfare. A new face of War» (1996 г.), MR-963-OSD «The Day After … in the American Strategic Infrastructure» (1998 г.) и MR-964-OSD «Strategic Information Warfare Rising» (1998 г.).

В январе 1995 года RAND было поручено проведение ряда исследований в рамках мероприятий, проводимых Министерством обороны США с целью выявления национальных приоритетов в концепции информационного противоборства. Результат этих работ, который должен был служить в качестве подготовительного этапа к осмыслению роли и мест

информационного противоборства в национальной военной стратегии США, был изложен в отчете за номером MR-661-OSD.

Важным результатом исследований, как следствие осознания возможностей информационного оружия, стало появление термина «***strategic information warfare*** – стратегическое информационное противоборство», которое, согласно заявлениям авторов, определяется как «…использование государствами глобального информационного пространства и инфраструктуры для проведения стратегических военных операций и уменьшения воздействия на собственный информационный ресурс…». Появление такой терминологии существенным образом отличается от официальной трактовки информационного противоборства, закрепленной в директиве Министерства обороны США DOD TS 3600.1. (декабрь 1992 г.), которая трактует информационное противоборство в достаточно узком смысле.

Авторами отмечается, что изменения в общественно-политической жизни ряда государств, вызванные быстрыми темпами информатизации и интернетизации общества, ведут к пересмотру геополитических взглядов руководства этих стран, к возникновению новых стратегических интересов (в том числе и в информационной сфере), которые приводят к изменению политики, проводимой этими государствами. Учитывая, что, согласно Клаузевицу, война есть продолжение политики другими средствами, разрешение глобальных противоречий потребует новых средств и методов их разрешения – стратегического информационного противоборства. Подчеркивалось, что в настоящее время основные положения национальной военной стратегии США не адекватны тем угрозам, которые возникают в ходе стратегического информационного противоборства.

Ключевым понятием, введенным в отчете MR-964-OSD, является классификация стратегического противоборства на первое и второе поколение. При этом стратегическое информационное противоборство первого поколения рассматривается наряду с традиционными средствами противоборства (ядерными, химическими, биологическими и др.). Подчеркивается, что информационное противоборство первого поколения больше ориентировано на дезорганизацию деятельности систем управления и проводится скорее как обеспечение действий традиционных сил и средств.

Авторы отмечают, что такое восприятие информационного противоборства свойственно начальному этапу осмысления проблемы. В отчете стратегическое информационное противоборство первого поколения определено как «… одна из нескольких компонент будущего стратегического противоборства, применяемая совместно с другими инструментами достижения цели …».

Развитие понимания проблемы привело к введению понятия ***стратегического информационного противоборства второго поколения*** (2nd generation Strategic Information Warfare). В отчете это понятие определено как ***«… принципиально новый тип стратегического противоборства, вызванный к жизни информационной революцией, вводящий в круг возможных сфер противоборства информационное пространство и ряд других областей (прежде всего экономику) и растянуто во времени на недели, месяцы и годы …»***. Отмечается, что развитие и совершенствование подходов к ведению стратегического информационного противоборства второго поколения приведет к полному отказу от использования силы, поскольку скоординированные информационные акции просто не позволят применить ее. Авторы подчеркивают, что если последствия стратегического информационного противоборства первого поколения еще могут быть прогнозируемы с использованием существующих методик, то второе поколение противоборства на текущий момент весьма трудно формализуемо и существующие методики прогноза могут быть применены к анализу последствий весьма условно.

Среди наиболее серьезных по своим последствиям задач, которые решаются посредством ведения информационного противоборства второго поколения, эксперты выделяют следующие:

- создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию противника;
- манипулирование общественным сознанием и политической ориентацией социальных групп населения страны с целью создания политической напряженности и хаоса;
- дестабилизация политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигания

недоверия, подозрительности, обострения политической борьбы, провоцирование репрессий против оппозиции, провокация взаимоуничтожения;

- снижение уровня информационного обеспечения органов власти и управления, инспирация ошибочных управленческих решений;
- дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;
- провоцирование социальных, политических, национальных и религиозных столкновений;
- инициирование забастовок, массовых беспорядков и других акций экономического протеста;
- затруднение принятия органами управления важных решений;
- подрыв международного авторитета государства, его сотрудничества с другими странами;
- нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и в других сферах.

Таким образом, американские военные эксперты ко второй половине XX века значительно продвинулись в освоении информационной сферы как новой сферы противоборства. В ряде конфликтов была отработана первоначальная концепция ведения информационной войны. Были определены ее слабые звенья. Главным вопросом на повестке дня стоял вопрос о создании единой общегосударственной информационной стратегии, поскольку только в масштабах всего государства, с привлечением всех доступных средств возможно ведение эффективной информационной войны.

2.14. Операции на основе эффектов – третье поколение методов информационной войны

В июле-августе 2002 года в США прошли масштабные учения «Millennium Challenge 2002», к которым было привлечено более 13500 человек личного состава всех родов войск. Бюджет учений составил более 235 миллионов долларов. Цель учений – отработать связанность и

взаимодействие частей и подразделений всех родов войск вооруженных сил США, а также порядок взаимодействия с другими федеральными ведомствами в ходе проведения «быстрых решающих действий».

Как отмечают военные эксперты армии США, «быстрые решающие действия» (Rapid Decisive Operations, RDO) – форма военных действий для выполнения миссий армией США в следующем десятилетии. RDO сосредоточены, прежде всего, на оперативном уровне, однако понятие RDO имеет также стратегические и тактические значения. Подготовка к RDO является целенаправленной и непрерывной, сосредотачиваясь на действиях, позволяющих влиять на поведение противника и удерживать его от принятия тех или иных решений. В том случае, если сдерживание терпит неудачу, RDO обеспечивают способность к быстрому и решительному принуждению или нанесению поражения противнику с целью достичь стратегических целей без длительной кампании или масштабного наращивания сил. RDO может быть успешной как сама по себе, так и, если необходимо, подготовить условия для перехода к действиям в ходе масштабного регионального конфликта с применением тяжелого вооружения.

Основой быстрых решающих действий является сетевое противоборство (network-centric warfare, NCW). NCW представляет собой мощный набор концепций противоборства, которые позволяют вооруженным силам получить полное преимущество над противником, используя всю доступную информацию об окружающем пространстве, о противнике и о собственных силах.

Сетевое противоборство включает одновременные действия в *физической*, *информационной* и *познавательной* областях.

Физическая область. Физическая область - традиционная область войны. Это область объединяет традиционные сферы противоборства - землю, море, воздух и космическое пространство. Это область, в которой функционируют физические платформы вооружений и системы коммуникаций. Поэтому элементы этой области проще всего идентифицируемы. Боевая мощь в этой области традиционно измеряется эффектами физического поражения.

Информационная область. Информационная область - область, в

которой создается, обрабатывается и накапливается информация. Кроме того, это область, в которой функционируют системы командования, управления, связи, коммуникаций и разведки. В битве за информационное превосходство, информационная область – это область самой большой чувствительности. Существовавшие ранее подходы к оценке производительности информационных систем больше не достаточны, чтобы измерить качество информации необходимы новые оценки, позволяющие определить возможный «эффект» от использования информационных средств воздействия.

Познавательная область. Познавательная область - область мышления бойца и мирного населения. Это область, в которой формируются намерения командиров, доктрины, тактика, методы противоборства. Нематериальные активы лидерства, морали, сплоченности подразделений, уровень подготовки, опыта, понимания ситуации и общественного мнения - элементы этой области. По мнению американских военных экспертов, эффекты в этой области представляют самый большой вызов в текущем десятилетии.

Необходимость в пересмотре основ военной наук состоит в том, что, как отмечают военные эксперты Пентагона, изменившийся за последнее время характер угроз практически не оставил времени на принятие решений командирам всех уровней. Существовавшие ранее концепции противоборства и созданные на их основе вооруженные силы плохо приспособлены к противодействию угрозам нового времени. По мнению экспертов, сегодня уже нет возможности тратить месяцы или даже недели на разработку планов применения войск и их развертывание. Вместо этого необходимо применять силы уже в первые часы кризиса. При этом первыми будут применены те средства, которые воздействуют на цели, воздействие на которые способно произвести желательные эффекты и повлиять на дальнейшее поведение противника. Этот новый американский путь ведения войны, как считается, улучшит национальную безопасность США в 21-ом столетии.

По мнению экспертов, спустя десятилетие после окончания Холодной войны Соединенные Штаты столкнулись с драматическим изменением характера окружающей геополитической среды. Диапазон новых угроз, помимо традиционных государств-вероятных противников, включает

сегодня и негосударственные, транснациональные группы, точные границы которых трудно определить. Как отмечают эксперты, угрозы со стороны подобных сетевых структур в последнее время представляют существенную опасность национальным интересам США. Кроме этого, демографическая ситуация и растущее различие в богатстве и распределении ресурсов в глобализирующемся мире создают дополнительное давление, способствующее реализации угроз со стороны враждебных сетевых структур.

По мнению авторов концепции быстрых решающих действий, сегодня даже среди традиционных государственных игроков, различие между враждебностью и невраждебностью практически стерто, поскольку новые способности (типа вторжений в компьютерные сети) мешают точно определить, когда была пересечена линия враждебности.

Аналитики Пентагона отмечают, что, сегодня, несмотря на существенное технологическое, экономическое и военное превосходство, целый ряд региональных держав и межнациональных коалиций имеют потенциал, позволяющий угрожать национальным интересам США.

Считается, что потенциальные противники многое усвоили из недавних действий армии США в Югославии и адаптировались к новым условиям. В этих условиях противники будут искать возможности достичь цели прежде, чем США смогут ответить на вызов. При этом противник не будет пытаться наносить поражение американским силам в симметричной открытой конфронтации, а скорее будет пытаться наносить поражение американской воле, используя асимметричные нападения, блокирую возможность доступа и, если необходимо, втягивая их в длительный, вялотекущий и изматывающий конфликт. Считается также, что противник будет пытаться блокировать доступ американских сил к театру военных действий, используя широко доступные современные системы вооружений. Цель противника в этом случае будет состоять в том, чтобы заставить армию США сомневаться в своей способности победить в пределах приемлемых затрат. Противник будет пытаться противостоять высокотехнологичным способностям США маскировкой, хитростью и рассредоточением своих сил. Он также будет использовать сложные информационные действия, чтобы воздействовать на национальную и коалиционную волю к победе.

Американскими экспертами отмечается, что действия армии США в Сербии и Косово показали пример того, каким образом противник будет противостоять вооруженным силам США в возможных конфликтах нового века: действия распределенными малыми подразделениями, широкое применение мобильных систем ПВО и массовое использование маскировки, камуфляжа и укрытий, информационные действия сербов были направлены против воли к победе, а также на разрушение сложившейся коалиции. Ими признается, что американские войска были вынуждены прибегнуть к неоптимальным методам нападения в силу необходимости минимизировать собственные потери.

На этом фоне произошедшие глубокие изменения в информатике, биологии, космических исследованиях, а также в ряде других областей науки позволяют с принципиально новых позиций подойти к развитию военной науки. Парирование новых угроз, созданных новейшими технологиями, может быть весьма трудной задачей для вооруженных сил времен Холодной войны. Эксперты Пентагона подчеркивают, что сегодня мы входим в эру, в которой не может быть ясных линий между враждебным и невраждебным или политическим и военным действиями. Действия противника будут простираться далеко за пределы открытых военных действий и могут включить террористические акты и атаки на компьютерные сети. При этом исполнителей этих акций будет очень тяжело обнаружить. Даже после их обнаружения, они могут смешаться с мирным населением, делая очень сложным ответный удар. В этих условиях необходимо оперировать в континууме многомерного политического-военного-экономического-социального-инфраструктурного-информационного пространства, в котором как сами цели, так и интенсивность взаимодействий с потенциальными противниками могут быстро измениться.

В этой связи эксперты Пентагона отмечают, что существующие сегодня объединенные силы, с их подавляющим превосходством в обычном конфликте с равным по силе противником, не обладают средствами, с помощью которых возможно доминировать над новой оперативной средой. Американскими военными отмечается, что, начиная с падения Советского Союза, США изменили численность вооруженных сил времен Холодной войны и создали их уменьшенную копию. Однако, большинство доктрин

времен Холодной войны, принципы действий, планирование и строительство вооруженных сил остается неизменным. США удалось увеличить эффективность отдельных компонентов вооруженных сил с появлением преимуществ «революции в военном деле», но не удалось повысить эффективности применения военной силы в целом.

По мнению ряда экспертов, ограничения прежних сил включают существенную зависимость от мест базирования; недостаток сил для выполнения возросших требований; недостаточный уровень стратегической мобильности для быстрого развертывания мощных, но тяжелых сил; недостаточные дальности действия средств поражения и др. Кроме этого отмечается, что сегодня США имеют непревзойденную способность собирать информацию об окружающем пространстве, о противнике и о собственных вооруженных силах, но испытывают недостаток в совместном планировании и управлении, чтобы использовать эту информацию для достижения превосходства решения. Также отмечается, что армия США имея высокоточное оружие, которое способно поразить цель с большой точностью, испытывает недостаток в способности последовательно произвести желательный оперативный эффект и заставить противника принимать выгодные США решения. Сегодня армия должна быть готова к быстрому переходу от относительно мирного процесса противостояния до интенсивных боевых действий. При этом быстро и решительно достигать стратегических целей. Считается, что военная мощь США в соединении с другими инструментами национальной мощи, должна развивать способность ответить быстро и решительно и разрешать конфликты в возможно более короткое время. При этом США планируют делать это не теряя способность побеждать в случае развязывания крупномасштабного регионального конфликта с применением тяжелого вооружения.

Военные эксперты армии США считают, что для ответа на изменения, произошедшие в геостратегичесом пространстве в начале XXI века, США должны преобразовать путь, которым сегодня проводятся объединенные операции. Сегодня важно знать, как провести военные операции совместно с другими инструментами национальной мощи. Аналитиками отмечается, что базовыми характеристиками, которые описывают фундаментальные различия

между будущими и сегодняшними объединенными действиями является основа на знания и на эффекты.

Основа на знания. Владение превосходящим знанием позволит американским военным изменить будущие объединенные действия. Мощь сложных информационных систем будущего обеспечит возможность для беспрецедентного создания и обмена знанием в понимании врага, собственных способностей армии США, окружающей среды и боевого пространства. Улучшенное ситуативное понимание позволит достичь превосходства решения, уменьшить эксплуатационный риск и в несколько раз увеличить темп, связанность и эффективность действий. Считается, чем больше известно о противнике, окружающей среде и о самом себе, тем более точно можно направить собственные способности, чтобы произвести желательные эффекты.

Непрерывно обновляемое восприятие противника как сложной адаптивной системы позволит американским военным более точно координировать применение всего диапазона национальных способностей.

Основа на эффекты. Действия на основе эффектов (Effect-based Operations, EBO) – философия войны, которая сосредотачивается на получении желательного стратегического результата или "эффекта" в поведении врага, через применение полного диапазона военных и невоенных мер на тактическом, оперативном и стратегическом уровнях. "Эффект" - физический, функциональный или психологический результат, событие или последствие, которое следует за единичным действием или совокупностью действий. Действия на основе эффектов разработаны с целью объединить передовые концепции высокоточного удара, доминирующего маневра и информационных операций по всему боевому пространству, давая возможность создать эффекты и вызвать изменения в поведении противника.

Считается, что объединенные силы будущего, основанные на всестороннем понимании ситуации, обеспеченной совершенными системами наблюдения и разведки, будут способны лучше определять эффекты, которые создадут требуемые изменения в поведении противника, которые в свою очередь отвечают американским национальным интересам. Этому будет способствовать знания, которые помогут определить критические

точки инфраструктуры противника (center of gravity), их критические уязвимости и причинные связи.

Более ясное понимание причинных связей между средствами и производимыми ими эффектами, позволит выбирать именно те средства, которые производят желательные эффекты и избегать тех, которые создают эффекты нежеланные.

Наибольшее значение в ходе создания объединенных сил будущего отводится информационным операциям. По мнению экспертов Пентагона, информационная операция - информационный эквивалент маневра и огня. Информационная операция особенно эффективна, когда она реализуется в своей целевой области (в информационной сфере). Она также может использоваться и для поддержки огня и маневра в других сферах противоборства.

Информационные операции реализуются в двух главных областях информационных эффектов: *электронные эффекты и эффекты влияния*. Электронные эффекты достигаются, прежде всего, путем радиоэлектронной борьбы и нападений на компьютерные сети. Эффекты влияния достигаются путем психологических операций, дезинформации, связей с общественностью, оперативной безопасности и специальных информационных операций.

Информационная операция обладает уникальными характеристиками, позволяющими применять ее как в мирное, так и в военное время. Эти характеристики включают низкое сопутствующее разрушение физической инфраструктуры, низкие требования к развертыванию, относительно быстрый ответ на поставленную задачу, низкий уровень риска для персонала, потенциально большой эффект при малом усилии и целевой специфики.

Таким образом, отработанные в ходе учений «Millennium Challenge 2002» подходы к строительству объединенных вооруженных сил позволят администрации США с принципиально новых позиций подойти к проведению внешней политики США в XXI веке. Основой такой политики станет комплекс, прежде всего, невоенных мер, направленных на создание «эффектов», приводящих к изменению поведения конкретного субъекта международных отношений в выгодном для США направлении.

Это подтвердилось с началом агрессии против Ирака в 2003 году. Военно-воздушные силы США и Великобритании в ходе этой агрессии применили новый подход к проведению воздушной операции.

В соответствии с реализуемой армией США концепцией формирования армии XXI века, действия военно-воздушных сил коалиции планировалось на основе оперативного анализа обстановки в районе боевых действий и проводятся в виде «операций на основе эффектов» («effect-based operations»).

Основная цель проводимых операций заключается в том, чтобы парализовать действия вооруженных сил Ирака, а не уничтожить их. Планами предусматривалось, что авиация коалиции в первые дни кампании будет стремиться обходить или избегать ударов по статическим целям из числа городских строений и элементов инфраструктуры, значение которых не измениться в течение значительного времени и к их уничтожению можно будет вернуться с изменением обстановки. Для реализации этого замысла предполагалось резко увеличить процент использования высокоточного оружия. Так, представители американского командования заявляют, что в ходе первого дня боев использовано 90 % высокоточного оружия из общего числа примененных средств, в дальнейшем планируется применять не менее 90 % высокоточного оружия в густонаселенных районах и районах повышенной опасности (например, нефтяные поля). Во всех других случая при нанесении ударов авиацией будет применяться не менее 70 % высокоточного оружия.

Предполагалось, что в ходе планирования ракетно-бомбовых ударов военно-воздушные силы будут стремиться избегать целей среди объектов экономики и инфраструктуры Ирака, где это будет возможно исходя из боевой обстановки. Также планировалось избегать ударов по целям, представляющих историческую, религиозную и культурную ценность.

Такой подход к проведению воздушной операции заставляет американских военных во многом пересматривать принципы планирования воздушной операции, чтобы избежать или минимизировать жертвы среди гражданского населения и сопутствующее разрушение. Кроме этого, встает вопрос выбора боевых частей ракет и авиабомб, а также систем их наведения с тем, чтобы использовать минимально достаточные средства для

прекращения функций цели. Таким образом, по мнению экспертов военно-воздушных сил, теперь в ходе воздушной операции необходимо не только определить цель, но и выделить в ее структуре критические точки, удар по которым приведет к прекращению ее функционирования. Удары планируется наносить только для того, чтобы уничтожить ключевую часть зданий с минимальным сопутствующим разрушением.

По мнению военных экспертов Пентагона, реализация нового принципа проведения воздушных операций поставила перед военно-воздушными силами коалиции ряд проблемных вопросов, которые решались в ходе кампании.

1. Необходимость изменений в целеуказании, определении критических точек цели и выбор боеприпасов для ее уничтожения. Именно это, как считают эксперты, может стать ключом к успеху англо-американских сил по реализации их способности ограничивать сопутствующее разрушение и жертвы среди гражданского населения. Считается, что этот вопрос необходимо решать путем использования новых возможностей разведки при планировании и строго ограничить число целей, по которым будут наноситься удары. Эксперты подчеркивают, что теперь необходимо тщательно выбирать боеприпас соответствующей точности и поражающему эффекту оружия, именно для конкретной критической точке цели, чтобы уничтожить только функцию цели без ее полного уничтожения.

2. В ходе операции будет использоваться новое оружие и тактика действий. Эксперты отмечают, что если новые концепции планирования являются ключом к эффективности воздушных ударов на основе эффектов, то США, возможно недооценивают эффект от применения новых видов оружия, которые будут использоваться в ходе операции против Ирака. Учитывая предварительную рекламу 10 тонной авиабомбы МОАВА и импульсных авиабомб для поражения систем управления возможны непредсказуемые реакции населения Ирака.

3. Эксперты военно-воздушных сил считают, что уже ко второму дню конфликта план бомбометания из статического и заранее предопределенного массива превратиться в динамический, быстро меняющийся массив целей. Это будет вызвано обнаружением новых целей,

выявлением новых приемов действия армии Ирака, а также с учетом маневра сил и средств коалиции и противника.

4. Планируется, что первые дни войны позволят США и Великобритании получить необходимый опыт, который позволит скорректировать планы боевого применения авиации. Эксперты отмечают, что в этой войне даже небольшие проблемы или преимущества в эффективности американского и британского бомбометания и методов планирования будут вести к быстрым изменениям в ходе операции.

5. Ряд специалистов отмечают, что оценка повреждений боевой техники и сооружений и в этой кампании будет значительной проблемой. Именно объективная оценка нанесенных повреждений позволяет успешно планировать воздушные удары. Однако уровень технологий все еще не позволяет проводить оперативный анализ результатов огневого воздействия, жертв среди гражданского населения, а также сопутствующих разрушений.

6. Представители военно-воздушных сил отмечают, что США и Великобритания планируют наносить удары по объектам багдадского режима и чувствительным к времени целям, отражающим активное сопротивление армии Ирака, но не собираются бомбить страну в целом. Именно поэтому, как отмечают эксперты, США и Великобритания стремятся парализовать и уничтожить режим, а не разрушать страну. Считается, что наносить ракетно-бомбовые удары по населенным кварталам армия коалиции будет, если это активно угрожает личному составу и боевой техники коалиции.

7. Неуправляемое оружие также планируется применять в ограниченном количестве. Американское командование планирует применять неуправляемое оружие в пропорции не более 30 %, в случае если возникнет непосредственная угроза личному составу и технике армии коалиции. Планируется, что в населенных пунктах этот процент не превысит 10 %.

8. Иракское оружие массового поражения и ракеты. Эксперты Пентагона отмечают, что оружие массового поражения и средства его доставки, а также ракеты иракской армии являются целями первого приоритета при планировании ракетно-бомбовых ударов.

9. В текущей кампании со стороны иракской армии следует ожидать масштабного применения средств ассиметричного воздействия, также будут массово применяться различные средства психологической войны, включая использование заложников, преувеличение жертв среди мирного населения и др.

10. Боевые действия в городских условиях не будут представлять серьезную опасность для сил коалиции. Американские эксперты отмечают, что архитектура и застройка городов Ирака сегодня позволяет применять высокоточное оружие. Большинство административных зданий окружено значительной свободной территорией, огороженной забором, что позволят применять по этим целям управляемые ракет и авиабомбы без ущерба для гражданских строений.

В целом, исход антииракской кампании показал, что многие разработанные планы в условиях динамически изменяющейся обстановки не могут быть в полной мере эффективно реализованы.

Глава 3. Организация работ в области информационной войны в США и ряде других стран

3.1. Взгляды министерства обороны США на проблему разработки и применения информационного оружия

3.1.1. Формирование организационной структуры информационных войск США

С начала 90-х годов в США осуществляется формирование организационной структуры информационных войск Министерства обороны. В настоящее время каждый вид вооруженных сил США имеет свой собственный Центр информационной войны.

Для решения поставленных задач сегодня только в рамках Министерства обороны создано уже более 30 структур. Среди них можно выделить следующие (по областям компетенции).

Защита информационных систем:

- Объединенная рабочая группа по защите компьютерных сетей (Joint Task Force - Computer Network Defense);
- Космическое командование ВС США (US Space Command) (в август 2002 года объединено со стратегическим командованием);

- Национальный центр защиты инфраструктуры (National Infrastructure Protection Center).

Рабочие группы реагирования на компьютерные инциденты (CERT):

- Рабочая группа реагирования на компьютерные инциденты военно-воздушных сил США (Air Force Computer Emergency Response Team);
- Армейская рабочая группа реагирования на компьютерные инциденты (Army Computer Emergency Response Team);
- Рабочая группа реагирования на компьютерные инциденты военно-морских сил США (Navy Computer Incident Response Team);
- Рабочая группа реагирования на компьютерные инциденты транспортного агентства МО США (Defense Logistics Agency CERT)
- Рабочая группа реагирования на компьютерные инциденты АНБ (National Security Agency X Group);
- Рабочая группа реагирования на компьютерные инциденты университета Карнеги Меллона (Carnegie Mellon University CERT/CC).

Ведение информационного противоборства:

- Центр информационного противоборства ВВС США (Air Force Information Warfare Center);
- Пресс-службы сухопутных войск (Land Information Warfare Activity);
- Пресс-службы ВМС США (Naval Information Warfare Activity);
- Центр информационного противоборства флота ВМС США (Fleet Information Warfare Center);
- Центр технологии информационного противоборства (Information Operations Technology Center).

Расследование компьютерных преступлений:

- Отдел специальных расследований ВВС США (Air Force Office of Special Investigations);
- Директорат криминальных расследований армии США (US Army Criminal Investigation Directorate);

- Военная разведка армии США (US Army Military Intelligence);
- Служба криминальных расследований ВМС США (Naval Criminal Investigation Service);
- Служба криминальных расследований министерства обороны США (Defense Criminal Investigative Service).

Проведение операций в информационных сетях:

- Центр сетевых операций ВВС США (Air Force Network Operations Center);
- Армейский центр сетевых операций (Army Network Systems Operations Center);
- Компьютерное и телекоммуникационное командование ВМС США (Naval Computer and Telecommunications Command);
- Центр безопасности операций в глобальных сетях (Global Network Operations Security Center).

Обеспечение:

- Центр совместных операций против систем командования и управления (Joint Command and Control Warfare Center);
- Центр совместного использования электромагнитного спектра (Joint Spectrum Center);
- Компьютерная судебная лаборатория Минобороны США (DoD Computer Forensic Laboratory);
- Агентство перспективных оборонных исследований (Defense Advanced Research Projects Agency);
- Пункт управления совместными операциями по единому информационному обеспечению деятельности подразделений армии США (Joint C4ISR Battle Center)
- Армейская исследовательская лаборатория (Army Research Lab).

Разведка:

- Объединенный штаб J2 Комитета начальников штабов (Joint Staff-J2)

- Разведывательное управление министерства обороны США (Defense Intelligence Agency);
- Разведывательное агентство ВВС США (Air Intelligence Agency).

Прочие организации:

- Национальное агентство по аэронавтике и космонавтике (National Aeronautics and Space Agency);
- Объединенный центр оборонных исследований (Joint Warfare Analysis Center).

На уровне государства все работы по информационному противоборству координируются помощником Президента по защите критической инфраструктуры.

Первый Центр информационной войны AFIWC (Air Force Information Warfare Center) был создан в сентябре 1993 года в военно-воздушных силах США. Центр территориально расположен на авиабазе Kelly (штат Техас, г. Сан-Антонио). В положении о Центре его задачи определены так: “Центр AFIWC разрабатывает, поддерживает и развертывает средства борьбы с системами командования и оперативного управления противника, планирует их оперативное применение, а также обеспечивает их приобретение и испытания”.

В военно-морских силах США в августе 1994 года создан Центр информационной войны NIWA (Navy Information Warfare Activity). Основной задачей этого Центра является исследование наиболее важных аспектов информационной войны, способствующих разрешению будущих конфликтов с участием военно-морских сил США.

В сухопутных войсках США проблемы информационной войны решает Служба наземных информационных боевых действий ВС США LIWA (Land Information Warfare Activity). Место дислокации Службы: штат Вирджиния, форт Белвуар.

Руководство всей деятельностью, связанной с проблемами информационной войны, в США осуществляется Министерством обороны.

Ответственность за решение всех вопросов, связанных с информационным противоборством, возложена на Помощника министра обороны по вопросам управления войсками, связи и разведки. Непосредственное руководство решением задач информационной войны осуществляет заместитель Помощника министра обороны по вопросам информационной войны.

Для обеспечения применения информационных войск в соответствии с их предназначением предполагается создать специальные органы:

1) Центр планирования и координации по вопросам информационной войны (разработка системы планирования деятельности по всем вопросам, связанным с информационным противоборством);

2) Центр стратегического уровня по отслеживанию признаков начала информационной войны (сбор и анализ разведывательной информации, определение признаков начала информационных атак);

3) Центр по проведению операций в области защиты от информационного оружия (предупреждение об информационных атаках тактического уровня, ликвидация последствий информационного нападения);

4) отдел по разработке конструкций и архитектуры автоматизированных систем (разработка единых архитектур и технических стандартов в области средств и систем защиты от информационного оружия);

5) группу независимых экспертиз - “красную команду” (анализ уязвимости автоматизированных систем, в том числе, посредством осуществления экспериментальных атак на автоматизированные системы и их отдельные элементы).

Организационная структура информационных войск постоянно изменяется и совершенствуется. Военно-политическое руководство США часто действует методом “проб и ошибок”: создается структура, и затем проверяется ее эффективность. В случае, если структура не отвечает предъявляемым к ней требованиям, она расформировывается или изменяется.

Представленные организационная структура информационных войск и состав задач, решаемых отдельными подразделениями информационных войск, показывают, по мнению военно-политического руководства США, их

постоянно возрастающее значение, в том числе, и при ведении боевых действий.

3.1.2. Разработка средств информационного воздействия и способов их применения

С появлением первых деструктивных программных средств руководство США стремилось использовать такие средства для достижения политических и военных целей.

В 1990 году Министерство обороны США открыто объявило конкурс на разработку боевого деструктивного программного средства, выполняющего следующие функции:

нарушение нормального режима функционирования линий связи и абонентских комплексов автоматизированных систем военного назначения;

ввод в автоматизированные системы ложной информации (дезинформация противника);

модификация программного обеспечения (в том числе программного обеспечения бортовых ЭВМ спутников связи).

Предполагалось, что внедрение деструктивного программного средства в автоматизированные системы должно осуществляться по каналам радиосвязи противника.

В настоящее время разработка таких средств информационного воздействия в США продолжается ускоренными темпами.

Комплекс мероприятий по использованию компьютерных вирусов в боевых целях получил название CVCM (Computer Virus Countermeasures).

Новым при создании компьютерных вирусов является разработка так называемых информационных организмов. Под *информационным организмом* (в последнее время используется термин «пакет вложения») понимается относительно короткий набор команд (до 30 команд), которым передается управление компьютером, в результате чего осуществляется захват информационно-вычислительных ресурсов автоматизированной системы (оперативной памяти, пространства на магнитных носителях информации, процессорного времени).

Внедрение троянских программ в автоматизированные системы противника планируется осуществлять следующими способами:

- использованием механизмов удаленных атак;
- внедрением программных закладок в операционные системы и программное обеспечение, поставляемые на экспорт;
- агентурным путем;
- по каналам радиосвязи противника.

Принципиальным моментом является внедрение в поставляемые на экспорт ЭВМ и их периферийное оборудование *аппаратных закладок*, которые маскируются под обычные устройства микроэлектроники. Аппаратные закладки применяются для сбора, обработки и передачи конфиденциальной информации.

Для отработки способов применения информационного оружия военно-политическое руководство США периодически проводит военные игры, в ходе которых осуществляется моделирование атак на собственную информационную инфраструктуру. Известны случаи выполнения в ходе учений информационных атак на реально функционирующие системы. Основные результаты атак: дезорганизация функционирования автоматизированных систем и снижение доступности информации. Соответственно, в ходе учений осуществляется поиск слабых мест в системе защиты информации автоматизированных систем различного назначения.

3.1.3. Подготовка высококвалифицированных кадров для ведения информационной войны

Для реализации планов информационной войны, в том числе применения информационного оружия, требуются высококвалифицированные кадры. Их подготовка в США осуществляется в Университете национальной обороны (г. Вашингтон), где создана соответствующая специальность. По данной специальности обучаются представители всех видов и родов вооруженных сил США. В июне 1995 года проведен первый выпуск из 16 офицеров, подготовленных по всем аспектам информационной войны – от защиты против компьютерных атак до

использования виртуальной реальности в организации планирования боевых действий.

Во время учений в мае 1995 года в Форт-Ливенворт, шт. Канзас, где расположен командно-штабной колледж армии США, пехотная дивизия численностью 20 тысяч человек, оснащенная современными системами обработки данных и высокоточным оружием, противостояла превосходящему ее втрое армейскому корпусу условного противника. Используя компьютеры, а также различные датчики и сенсорные устройства, которые лучше «видят» неприятеля на поле боя, дивизия, по словам представителя учебного командования сухопутных войск США бригадного генерала К.Келлога, «просто задавила» противника.

В июле этого же года в военно-морском колледже США в г. Ньюпорт состоялись крупномасштабные учения, в ходе которых отрабатывались способы выведения из строя компьютерных устройств противника.

Кроме этого, введены в учебных заведениях Министерства обороны США (а также в отдельных гражданских высших учебных заведениях) курсы по обучению вопросам ведения информационной войны и информационных боевых действий (выполнения функциональных обязанностей) в условиях применения противником информационного оружия. Организована подготовка специалистов по специальностям “защита от информационного оружия” и “администратор систем и сетей”.

В известном меморандуме Клинтона и Гора, выпущенном в 1993 г., с которого, собственно, и начала свою жизнь Национальная информационная инфраструктура (NII), говорится о том, что стратегической целью США является "достижение мирового лидерства в фундаментальной науке, математике и технике". Последовательно претворяя в жизнь идеи NII, в конце февраля 1998 г. генеральный прокурор США Джанет Рено объявила о создании Центра по защите национальной инфраструктуры (National Infrastructure Protection Center). Наращивая отрыв в технологическом превосходстве и создавая компьютерный щит, Америка неуклонно идет к поставленной цели.

Представленный комплекс мероприятий по созданию и применению информационного оружия показывает особую роль, которую руководство

США отводит этому виду вооружений как средству достижения политических и военных целей в современной войне.

3.2. Подход администрации США к обеспечению информационной безопасности информационной инфраструктуры

Деятельность администрации Клинтона в области защиты критической инфраструктуры берет свое начало с формирования Президентской комиссии по защите критической инфраструктуры (President's Commission for Critical Infrastructure Protection) в 1996 году. Отчетный доклад этой комиссии выявил уязвимости национальной безопасности США в информационной сфере. Итоги работы комиссии были положены в основу правительственной политики в области обеспечения информационной безопасности критической инфраструктуры, сформулированной в Директиве президента № 63, подписанной в июне 1998 года (PDD-63).

Во исполнение указаний президента, обозначенных в этой директиве, был разработан Национальный план защиты информационных систем США, подписанный президентом 7 января 2000 года.

Согласно этому плану, администрация Клинтона получила 2.03 миллиарда долларов из федерального бюджета в 2001 финансовом году для выполнения работ по защите критической инфраструктуры. Среди основных программ, изложенных в плане, наиболее значимыми являются следующие программы.

Программа по формированию Федеральной службы компьютерной подготовки и обучения (требуемый объем финансирования - 25 миллионов долларов). Эта программа направлена на улучшение эффективности привлечения и удержания высоко квалифицированной рабочей силы в правительственных учреждениях, включая увеличение численности квалифицированных специалистов в области информационной безопасности. Инициатива состоит из множества мероприятий. Одно из них - это программа, в которой федеральное правительство через Национальный научный фонд оплачивает двухлетнее вузовское или послевузовское образование в сфере информационной безопасности в обмен на подписание

контракта на государственную службу в подразделениях информационной безопасности. Обучение должно проходить в течение двух лет в школах с учебными программами, аккредитованными в области информационной безопасности. Студенты, участвующие в программе должны проходить летнюю практику в правительственных агентствах, а также посещать тематические научно-практические конференции.

Вторая программа связана с формированием Центра повышения квалификации в области информационных технологий (CIET). CIET должен обеспечить переподготовку работающих администраторов федеральных информационных систем и специалистов по информационной безопасности. Предполагается, что руководство CIET будет осуществляться Департаментом управления персоналом. Обучение будет предлагаться участками, отобранным на конкурсной основе как внутри самих федеральных ведомств, так и в сторонних организациях.

Третья программа предназначена для обучения учащихся средней школы и преподавателей, а также широкую публику по вопросам информационной безопасности.

Четвертая программа должна продвинуть пониманием проблем информационной безопасности среди федеральных служащих.

Постоянно действующая группа экспертного контроля (требуемый объем финансирования - 5 миллионов долларов). По мнению представителей администрации Клинтона, наличие такой группы дало бы возможность постоянного экспертного контроля за ходом работ по внутренним планам информационной безопасности агентств, о ходе исследований по анализу уязвимости и т.д. Группа должна иметь поддержку со стороны Национального Института стандартов и технологии.

Федеральная сеть обнаружения вторжения (требуемый объем финансирования - 10 миллионов долларов). FIDNET является сетью обнаружения вторжений для гражданских правительственных агентств. Следует отметить, что Министерство обороны и АНБ имеют их собственные сети обнаружения вторжения. Все вместе они будут связаны между собой, а также с Национальным Центром защиты инфраструктуры ФБР.

Формирование инфраструктуры управления открытыми ключами средств криптографической защиты информации (7 миллионов долларов). Инфраструктура открытых ключей (PKI) позволяет устанавливать двухстороннее конфиденциальное соединение с проверкой подлинности по общедоступным каналам связи. Эта структура весьма актуальна для систем электронной торговли, а также для правительственных агентства, чтобы упростить процесс обмена информацией с подрядчиками и клиентами. Эта инициатива включает реализацию 7 экспериментальных программ в различных федеральных агентствах.

Институт защиты информационной инфраструктуры (50 миллионов долларов). Предполагалось, что эти средства станут основой фонда исследований и разработок, используемого Национальным институтом стандартов и технологии (NIST) для поддержки исследований, которые иначе не могло быть проведены федеральными агентствами или частными предприятиями. В настоящее время почти все текущее информационное исследование по информационной безопасности идут в агентствах, обеспечивающих национальную безопасность.

В феврале 2003 года Комиссией по защите критической инфраструктуры при президенте США была обнародована стратегия национальной безопасности киберпространства. Этот документ является развитием работы Комиссии в области обеспечения безопасности критической инфраструктуры.

Стратегия национальной безопасности киберпространства является одним из базовых документов, отражающим позицию нынешней администрации США на проблемы обеспечения национальной безопасности страны в XXI веке, отраженной в новой стратегии национальной безопасности США и стратегии внутренней безопасности, которые были также представлены широкой общественности в сентябре этого года.

Работы по обеспечению безопасности информационной инфраструктуры государства в США были начаты после издания президентской директивы PDD-63, определившей понятие «критической инфраструктуры». В ходе проведенных работ в январе 2000 года президентом Клинтоном был подписан План защиты национальной информационной инфраструктуры,

положивший начало организации специализированных структур по обеспечению национальной безопасности в информационной сфере. В ходе реализации этого Плана в США был создан ряд специализированных подразделений, проведена работа по совершенствованию законодательства в области информационной безопасности.

Прежде всего, изменения коснулись общего контекста документа с тем, чтобы он полнее соответствовал основным принципам, изложенным в новой Стратегии национальной безопасности США.

Согласно Национальной стратегии безопасности киберпространства ***США оставляют за собой право на превентивные действия в киберпространстве в отношении враждебных государств, в случае если их политика угрожает или в обозримом будущем будет угрожать национальным интересам США.*** Кроме того, США оставляют за собой право на адекватный ответ в случае нападения на информационные системы из киберпространства, а не ограничиваются юридическими вопросами и слушаниями в суде по факту нарушения защиты информационных ресурсов.

Значительная часть документа посвящена вопросам разграничения полномочий по обеспечению безопасности в киберпространстве между Департаментом внутренней безопасности, ЦРУ и ФБР. Согласно этому документу, на ЦРУ и ФБР возлагаются обязанности по нейтрализации деятельности враждебных государств в киберпространстве, направленной на получение разведывательной информации. На Департамент внутренней безопасности возлагается обязанность обеспечения бесперебойной работы компьютеризированных систем в различных сферах критической инфраструктуры США, а именно: в системе водоснабжения, энергосетях, на транспорте и др.

В ближайшее время одной из основных задач станет создание единой информационной сети, объединяющей базы и банки данных всех 22 федеральных агентства, вошедших в Департамент внутренней безопасности. Основные усилия будут сосредоточены на разработке биометрических систем аутентификации, программного обеспечения добывания и анализа данных (data mining) и развитие геоинформационных систем.

На решение проблем, стоящих перед Департаментом внутренней безопасности будет также направлена и работа Правительственной ассоциации электроники и информационных технологий (GEITA), которая планирует в 2003 году потратить около 74 миллиардов долларов на разработку проектов обеспечения информационной безопасности и развития информационной инфраструктуры США. В частности планируется потратить 1,2 миллиарда долларов на создание автоматизированной системы слежения за иностранными гражданами, въезжающими или проживающими в США, предназначенной для Службы иммиграции и натурализации.

Пентагон также планирует потратить в 2003 году около 10 миллионов долларов на создание единой базы данных по террористическим организациям и отдельным террористам. Исполнителем проекта будет являться Управление информационного взаимодействия (Information Awareness Office) Агентства перспективных оборонных исследований (DARPA).

В целом следует отметить, что после внесения изменений новая редакция Национальной стратегии безопасности киберпространства США стала теснее взаимосвязана с двумя другими основополагающими документами, определяющими позицию администрации США к вопросам безопасности – это Стратегия национальной безопасности и Национальная стратегия внутренней безопасности, которые также были приняты в 2002 году. Основная идея всех трех документов – отход от концепции сдерживания в пользу концепции превентивных ударов, а также главенствующая роль США во всех сферах жизнедеятельности современного общества, включая и информационную сферу.

3.3. О реализации Национального плана защиты информационных систем США

В январе 2001 года президентом США был подготовлен и представлен в Конгресс ежегодный отчет о проделанной работе по реализации основных положений Директивы президента PDD-63 (принятой в мае 1998 года) об организации работ по защите критически важной национальной инфраструктуры (Report of the President of the United States on the Status of

Federal Critical Infrastructure Protection Activities, Jan 2001, http://www.pccip.gov).

3.3.1. Основные направления работ в Министерстве обороны США

Согласно отчетному докладу президента США за прошедший год Министерство обороны США добилось значительного прогресса в защите критической инфраструктуры (critical infrastructure protection, CIP), сосредотачивая свои усилия по трем главным направлениям:

- обеспечение информационной безопасности информационных систем;

- продолжение работ по программе «Y2K», включающей разработку и реализацию программ тестирования решений на совместимость с «проблемой 2000 года» с целью обеспечения защиты критической инфраструктуры; отмечается, что ряд выполненных в рамках этой программы работ, продемонстрировал возможность проведения работ с информационной инфраструктурой любой сложности, способность определить уязвимые места в структуре, которые могут повлечь отказ, а также быстро исправить их с наименьшими затратами;

- расширение научно-исследовательских разработок в области защиты критической инфраструктуры.

Ключевым элементом в программе обеспечения безопасности информационного пространства Министерством обороны является подход, названный его разработчиками «Defense-in-Depth» («Глубокая оборона»). Информационные системы, построенные с использованием этого принципа, состоят из многослойных систем безопасности и процедур, использующих активные и пассивные мероприятия по защите информационных ресурсов, предотвращающих неправомочный доступ к информации. Глубоко эшелонированная оборона защищает критические ресурсы и процессы, формируя политику сдерживания, расширяющую возможности программных средств обеспечения информационной безопасности сети. Считается, что такой подход заставит противника тратить собственные ресурсы при преодолении множественных слоев защиты прежде, чем он достигнет способности воздействовать на функционирование информационных систем. Такая слоистая концепция безопасности позволяет максимально

использовать возможности коммерческих технологий и минимизировать дополнительные инвестиции, которые необходимы для совершенствования коммерческих технологий.

Эта технология, в основу которой положена тесная интеграция способностей персонала и современных технологий, основывается на организации защиты локальных вычислительных пространств отдельных объектов критической инфраструктуры (называемых также «анклавы»), границ анклава и сети коммуникаций, которая связывает эти анклавы, а также обеспечивающую инфраструктуру. Авторы отмечают, что сегодня они не в состоянии полностью устранить уязвимость информационных систем, однако они рассчитывают, по крайней мере, существенно смягчить их последствия.

3.3.2. Основные мероприятия по реализации базовых концепций «глубокой обороны»

Для реализации концепции «Defense-in-Depth» Министерство обороны выполняет ряд мероприятий. Так, например, в настоящее время во всем министерстве развертывается инфраструктура для обеспечения работы средств криптографической защиты информации с открытым ключом (Public Key Infrastructure, PKI) на основе стойких криптоалгоритмов. Считается, что эта система позволит обеспечить непрерывное шифрование информации, передаваемой по каналам связи, а также услуги аутентификации для «чувствительной, но несекретной» информации, а также обеспечит улучшенное управление доступом к информационным системам и компьютерам. Предполагается также, что в будущем эта система обеспечит безопасность секретной информации, передаваемой по незащищенным каналам связи сетей общего пользования. Политика, принятая в Министерстве обороны, по развертыванию PKI была подписана представителем Министра обороны в мае 1999 и обновлена в августе 2000 года. Эта политика устанавливает срок в октябре 2002 года, когда все военнослужащие, гражданский персонал и ряд сотрудников из числа резервистов будут иметь «типовую карту доступа» (Common Access Card) на основе смарт-карты со встроенным микропроцессором, которая будет содержать цифровые сертификаты PKI министерства с информацией о пользователе.

Предполагается, что все служащие Мионобороны (приблизительно 3.1 миллионов человек) будут иметь цифровые сертификаты к октябрю 2002. На момент подготовки президентского доклада было подготовлено приблизительно 43000 сертификатов (армия - 14600, флот - 3100, военно-воздушные силы - 10300, военная полиция - 2700, другие -12700); подготовлены сертификаты для 26500 серверов электронной почты; 2900 сертификатов обслуживающего персонала, а также 107 сертификатов для использования в сети NIPRNET. В 2001 году планируется подготовить еще около 1.3 миллиона сертификатов.

Вместе с работой по созданию PKI проводятся мероприятия по внедрению более стойкой технологий шифрования с тем, чтобы обеспечить необходимый уровень криптостойкости на уровне с быстрыми изменениями в области информационных технологий и методов криптоанализа. Отмечается, что Министерство обороны активно развивает соответствующие программы, с целью модернизировать методы и технологии безопасной передачи голоса и данных непосредственно на рабочее место сотрудников министерства, а также совершенствование безопасных технологий для сетей радиосвязи.

Перерабатывается программа Минобороны «Информационная инициатива». Темпы реализации этой программы, предусматривающей формирование Глобальной информационной сети (Global Information Grid, GIG) в настоящее время резко возросли. Именно Глобальной информационной сети отводится главная роль в достижении и удержании информационного превосходства. Политика информационной безопасности Глобальной информационной сети за номером 6-8510 была подписана в мае 2000. Эта политика включает не только требования по обеспечению конфиденциальности информации, но также и ее доступности, целостности и потребности в усиленной идентификации и предоставлении отказоустойчивых услуг.

3.3.3. О совершенствовании судебной практики в области компьютерных преступлений

Одной из наиболее важных из числа выполненных работ является существенное продвижение по пути совершенствования приемов и методов работы с доказательствами компьютерных преступлений, что имеет большое

значение при проведении расследований любых инцидентов, связанных с применением вычислительной техники. Так 24 сентября 1999 года была открыта Компьютерная судебная лаборатория Министерства обороны (Defense Computer Forensics Laboratory, DCFL). Это – одна из наиболее современных структур, предназначенная для обработки компьютерных доказательств в преступлениях и мошенничествах, а также при проведении контрразведывательных мероприятий для всех организаций, проводящих криминальные и контрразведывательные исследования. Управление специальных исследований Военно-воздушных сил США определено в качестве Исполнительного агентства для DCFL. В настоящее время DCFL имеет 42 позиции для исследователей и судебных приставов, позволяющие обрабатывать компьютерные доказательства наряду со звуковой и видео информацией в судебных делах в самом широком диапазоне: от детской порнографии до вторжений в компьютеры и шпионажа. Эта лаборатория министерства обеспечивает поддержку ФБР по вопросам расследования компьютерных преступлений. Специалисты DCFL уже накопили определенный потенциал и навык работы с инструментальными средствами анализа информации в ходе ряда успешных мероприятий по идентификации групп хакеров, а также при нейтрализации уязвимости в нескольких контрразведывательных операциях, связанных с деятельностью по защите национальных сети ЭВМ. Среди последних - такие нашумевшие мероприятия как "Солнечный восход", "Цифровой демон" и "Лабиринт лунного света" ("Solar Sunrise", "Digital Demon", "Moonlight Maze").

3.3.4. Формирование спецподразделений компьютерной обороны

Говорится также и об улучшении способности активно защищать информационные системы и компьютеры. Для этой цели была создана Объединенная оперативная группа по защите компьютерной сети Министерства обороны (Joint Task Force for Computer Network Defense, JTF-CND), а главнокомандующий космического командования принял полную ответственность за защиту сетей ЭВМ министерства с 1 октября 1999 года. Как отмечают авторы отчета, в ходе инцидента с вирусом "Мелисса" в марте 2000 года, JTF-CND, совместно с Группой реагирования на чрезвычайные ситуации с вычислительной техникой Министерства обороны (Computer Emergency Response Team, CERT), оказалась способной быстро оценить

угрозу, сформировать оборонительную стратегию и направить ход соответствующих оборонительных действий. Далее, в мае 2000 года, в ходе эпидемии компьютерного вируса "LOVELETTER" был продемонстрирован еще один пример четких действий JTF-CND. Персонал JTF быстро идентифицировал потенциальное повреждение и обеспечил своевременное уведомление подразделений, служб и агентств министерства, которые позволили им эффективно ответить на вторжение.

С 2000 года Министерством обороны начата работа с союзниками по вопросу обеспечения информационной безопасности: Канада имеет официального представителя, работающего в JTF-CND, развивается система разделения информации между Министерствами обороны в соответствии с основными положениями Меморандума о понимании и Концепции действий подписанными с канадской стороной.

Проведены работы по созданию системы сигнализации при обнаружении уязвимости информационной безопасности (Information Assurance Vulnerability Alert, IAVA) для распределения информации об уязвимости всем подразделениям и службам Минобороны. В 1999 году этой службой было подготовлено и выпущено 11 предупреждений (IAVT), 3 бюллетеня (IAVBs) и 20 технических консультаций. В 2000 году были выпущены 3 предупреждения, 3 бюллетеня и 9 технических консультаций. Агентство информационных систем Минобороны (Defense Information System Agency, DISA) сформировало банк данных, для немедленного распределения информации об уязвимости каждому администратору системы вместе с краткой информацией о возможных ответных действиях по локализации последствий.

3.3.5. Обучение персонала

Одним из серьезных достижений признается то, что сформированы и реализуются программы всестороннего обучения, тренировки и осведомления (Education, Training and Awareness, ETA) военнослужащих, гражданского персонала и служащих по контракту Министерства обороны. Для всех пользователей информационных систем установлен необходимый минимум базовых знаний в области информационной безопасности, без которого они не могут быть допущены к работе, при этом весь персонал

должен проходить ежегодную переподготовку. Дополнительно к этому для всех администраторов как засекреченных, так и несекретных систем требуется иметь сертификаты на допуск к работе. Соответствующие программы сертификации будут внедрены в текущем году. Для совершенствования обучения Управление программ по информационной безопасности (Information Assurance Program Office, IAPMO) Агентства информационных систем МО подготовило и распространяет множество компакт-дисков и видеофильмов с материалом по курсам обучения. Этот материал широко доступен всем федеральным структурам.

Чтобы повысить качество академического образования в области информационной безопасности, Агентство национальной безопасности сформировало в 1999 году Центры послевузовского образования по информационной безопасности, а в 2000 году значительно расширило программу, включив в нее 14 ведущих университетов США. Университеты отбирались на основании глубины и зрелости их учебных программ в области информационной безопасности в соответствии со стандартами, предложенными Комитетом по безопасности телекоммуникационных и информационных систем национальной безопасности (National Security Telecommunications and Information Systems Security Committee, NSTISSC).

3.3.6. Формирование единой оценки состояния информационной безопасности в МО

Интересной работой является развитие единого процесса формирования и самой метрики, посредством которой министр обороны может объективно оценить и ясно сформулировать статус боеготовности министерства в области информационной безопасности. Этот процесс будет применен во всем министерстве для взаимодействия как с боевыми, так и не боевыми подразделениями и службами. В качестве итогового результата работы станут: статус боеготовности в части информационной безопасности, формализованные требования на ресурсы для обеспечения информационной безопасности, исходные данные для формирования или пересмотра политики Минобороны в области информационной безопасности. Предполагается, что метрика будет иерархически структурирована на пять уровней иерархии. Эти уровни соответствуют пяти критическим индикаторам успеха: люди, мероприятия, обучение, оборудование, инфраструктура.

3.3.7. Формирование виртуального резерва

За прошедший год утверждена концепция действий виртуальной информационной организации объединенного резерва (Joint Reserve Component Virtual Information Organization, JRVIO), которая обеспечивает поддержку совместных информационных операций Агентства информационных систем Министерства обороны, АНБ, Объединенного Центра информационных операций (Joint Information Operations Center, JIOC), Технического Центра информационных операций (Information Operations Technical Center, IOTC) и Объединенной оперативной группы по защите компьютерных сетей Минобороны (JTF-CND). Структура и функции поддержки JRVIO приспособлена для выполнения роли активного компонента (например, JRVIO поддержка действий JIOC выполнят активные функции в пределах миссии JIOC). При этом у организации нет других функций, кроме функции проведения виртуальных действий. Руководство JRVIO гарантирует, что действия резерва оперативно изменяются в зависимости от миссии подразделений, в поддержку которых выступает резерв. Любая миссия по обеспечению информационной безопасности, проводимая одной из поддерживаемых организаций, будет открыта для управления задачами JRVIO. Так, если на объединенном уровне DISA проводит действия по обеспечению информационной безопасности с целью защиты Информационной инфраструктуру Министерства обороны (Defense Information Infrastructure, DII), то в этом случае все действия выполняются через Центр обеспечения функционирования и защиты глобальной сети (Global Network Operations and Security Center, GNOSC), центры обеспечения функционирования и защиты региональных сетей (Regional Network Operations and Security Centers, RNOSCs), группу реагирования на чрезвычайные ситуации с вычислительной техникой Министерства обороны (DOD CERT). Координация со службами и другими агентствами, координация с промышленностью и множеством других внутренних подразделений МО, а также организация внешних контактов лежит на JRVIO. Далее Управление информационной безопасности АНБ в координации с DISA и под политическим руководством ASD/C3I, проводит действия по обеспечению информационной безопасности в поддержку Министерства обороны и других правительственных отделов и агентств. Считается, что добавление поддержки JRVIO к этим мероприятиям расширит

их способность оперативно реагировать на быстрорастущие вызовы информационной безопасности.

3.3.8. Деятельности КНШ и видов командования видов ВС армии США по проведению работ в области информационной безопасности

Председателем Комитета Начальников Штабов (Chairman of the Joint Chiefs of Staff, CJCS) выпущено руководство для командующих и штабов Объединенных командований, служб и агентств по улучшению системы оповещения об уязвимости в информационной сфере (IAVAs).

В Объединенном оперативном плане 1999 года космическое командование (SPACECOM) обозначено в качестве руководящей структуры по обеспечению защиты компьютерных сетей Минобороны (computer network defense, CND) и противодействию нападениям на сети ЭВМ (computer network attack, CNA).

В директиве CJCS также отмечалось, что Объединенный штаб включает мероприятия по CND во все оперативные и долгосрочные планы боевой подготовки.

Отдельно рассмотрены вопросы, реализованные Директоратом коммуникационных и компьютерных систем и систем управления, контроля Объединенного штаба (Command, Control, Communications & Computer Systems Directorate, J-6). Отмечается, что это подразделение полностью укомплектовано и готово к выполнению инструкции CJCSI 6510.01C по определению минимума информационной безопасности (по 55 параметрам) требуемого для подразделений, служб и агентств Министерства обороны.

На сегодняшний момент в Директорате J-6 объединены несколько оперативных рабочих групп по проблеме информационной безопасности в рамках одного комитета, который докладывает Военной коллегии по электронике и коммуникациям (Military Communications-Electronics Board, MCEB). Работа комитета привела к существенному сокращению уязвимости мобильного программного кода (на основе интернет-технологий ActiveX и Java) в информационных системах Минобороны.

Совместно с другими подразделениями Директорат работает над формализацией метрики боеготовности в части информационной

безопасности и ее включении в ежемесячное Объединенное сообщение о готовности (Joint Monthly Readiness Report, JMRR), которое объединяет данные об информационной безопасности, переданные в сообщениях боевых расчетов дежурных смен.

В сухопутных войсках сформирована Программа усовершенствования безопасности сети (NSIP) в качестве армейской стратегии по осуществлению концепции Министерства обороны «Defense in Depth». В рамках этой программы создана инфраструктура групп реагирования на компьютерные инциденты (ACERT). ACERT принимает все сообщения о вторжении и поддерживает пользователей во всем мире в вопросах обеспечения необходимой защиты и возможных вариантов ответа на нападения на системы и сети.

Директорат J6 и Военная коллегия по электронике и коммуникациям (MCEB) финансировали разработку политики применения мобильного программного кода, которая была подписана 7 ноября 2000 года. Предполагается, что выполнение политики применения мобильного кода уменьшит уязвимость информационных ресурсов министерства от злонамеренных нападений из глобальной сети Интернет. С целью совершенствования этой политики, представители J6 активно сотрудничали с корпорацией Microsoft по выявлению возможной уязвимости мобильного кода и технологий на его основе. MCEB также финансировала формирование «Руководства по управлению коммуникационными портами и протоколами», одобренное исполнительным комитетом Министерства обороны по вопросам защиты критической инфраструктуры в ноябре 2000 года. Это руководство позволяет сотрудникам министерства управлять безопасностью в наиболее уязвимых точках межсетевых соединений.

Сотрудники J6 встречались с представителями корпорации Wang, чтобы обсудить направление, которое частная компания берет в отношении PKI. Будущие планы J-6 включают формирование программ аудита инфраструктуры, с целью определить объем работ по обеспечению информационной безопасности, возможный интерфейс как часть Глобальной информационной сети, а также зависимости между состоянием критических компонент инфраструктуры и боеготовностью подразделений.

Как член Консультативного совета по телекоммуникациям Национальной безопасности (NSTAC), J6 вовлечен в деятельность оперативных групп NSTAC по направлению "Распределение информации/Защита критической инфраструктуры" (IS/CIP). Одна из его выдвинутых на первый план инициатив состоит в координации действий Президентского Управления обеспечения безопасности критической инфраструктуры (President's Critical Infrastructure Assurance Office) с целью достижения положительных результатов в реализации президентской директивы PDD-63 1998 года.

Отмечается, что армия является признанным лидером, объединяющим и координирующим все работы по биометрическим системам обеспечения информационной безопасности для Министерства обороны. В 2000 финансовом году был создан Отдел биометрического управления (Biometrics Management Office, BMO). Основная цель BMO состоит в том, чтобы разработать и внедрить стратегию применения биометрических технологий, которые гарантируют безусловный контроль и управление доступом к критической информации и системам вооружения во всех сферах ведения боевых действий.

Армейский Центр информационного доминирования (Information Dominance Center, IDC) командования разведки и безопасности достиг начального уровня боеспособности 1 октября 2000 года и в настоящее время находится во второй фазе трехэтапного процесса развития. IDC обеспечивает армию технологиями и инструментами для поддержки совместного планирования, анализа и выполнения информационных операций.

В 2000 году был разработан Оперативный план информационной безопасности Армии XXI века. Этот план поддерживает защиту критической инфраструктуры путем целостного подхода, сосредоточенного на обеспечении функциональной способности во всем спектре конфликта. Наряду с этим сформирован стратегический план информационной безопасности, ориентированный на поддержку ключевых положений стратегии национальной безопасности США.

Боевые группы временных бригад сухопутных войск (Army's Interim Brigade Combat Teams, IBCT) и Цифровой корпус включили мероприятия по

обеспечению информационной безопасности в совокупность их действий. Сухопутные войска обновили План защиты для систем по программе "Force XXI". Этот план определяет требования по планированию безопасности, испытания с целью выявления уязвимости и формирования ключевых решений по их нейтрализации.

Сухопутные войска включили обеспечение информационной безопасности (защита критической инфраструктуры) в установочный курс подготовки высшего командного состава.

В 2001 году планируется провести военно-политические игры по отработке элементов обеспечения информационной безопасности с целью усиления понимания руководства вооруженных сил этой проблемы.

Военно-воздушные силы реализовали процесс сертификации продуктов и услуг на пригодности к использованию в сетях (Certificate of Networthiness, CON). Прежде, чем систему считают пригодной и выпущен соответствующий сертификат ведущим комитетом по защите инфраструктуры в ВВС США, проводится испытание оценки риска сети, идентифицируются потенциальные проблемы безопасности и выявленные дефициты исправлены.

В 2000 году Военно-воздушные силы провели 41 мероприятие по оценке террористической уязвимости используя интегральную оценку уязвимости Объединенного штаба (JSIVA) и Команды оценки уязвимости ВВС США. На 2001 год намечено проведение 44 оценок. Как и в предыдущие годы в фокусе этих оценок - защита персонала. Однако в будущем информационная безопасность и планирование ответных мероприятий займут важное мест в такого рода проверках.

Штаб ВВС совместно с ASD (C3I) участвовал в разработке Объединенной оценки уязвимости (DIVA) - ВВС США обеспечили исходные данные по интеграции существующих процессов оценки, рекомендовали, как структуру DIVA, численность и состав рабочих групп, а также протоколы обмена такой информацией. ВВС США провело отработку предложенной концепции в полевых условиях на авиационной базе ВВС Малмстром, штат Монтана.

Корпус морской пехоты разработал Базовый набор защиты инфраструктуры сети (Base Network Infrastructure Protection Suite) в настоящее время он проходит полевые испытания.

Военно-морской флот разворачивает безопасные информационные системы, которые облегчают работу для всех уровней классификаций информации.

Командование объединенных сил (USJFCOM) развернуло программы по защите информационных систем, по обучению приемам обеспечения информационной безопасности, и CND для компьютерных сетей штабов, наряду с проведением контроля по обеспечению информационной безопасности в 19 подчиненных командованиях. Командование объединенных сил включило дополнительную игру по обеспечению информационной безопасности в обучающее упражнение объединенного оперативного соединения в координации с группами планирования информационных операций Объединенного боевого центра (Joint Warfighting Center's Information Operations Planning Cell). Также обновлены процедуры информирования об инцидентах в сети ЭВМ, что позволить быстрее уведомлять вышестоящие подразделения об идентифицированных событиях.

Установлена периодичность контрольных проверок боеготовности в отношении информационной безопасности (IARRs) для всех 5 объединенных командований.

С 1 июля 2000 года введено использование Системы слежения Агентства информационных систем Министерства обороны за возможными уязвимостями (VCTS).

Введены в строй дополнительные, избыточные каналы связи для штабов в сети SIPRNET, которые позволят выполнять автоматизированное восстановление систем после сбоев.

В 2001 году Командование объединенных сил при поддержке DISA планирует установить дополнительные серверы безопасности, межсетевые экраны, системы обнаружения вторжения и сканеры уязвимости на своих компьютерных сетях.

3.4. О работах Агентства национальной безопасности США

Согласно Национальному плану защиты информационных систем США на АНБ возложены работы по обеспечению информационной безопасности в федеральных агентствах.

С целью выполнения возложенных обязанностей, в 2000 году АНБ провело ряд работ по оценке уязвимости и оценке риска собственной информационной инфраструктуры, а также инвестировало значительные средства в ее модернизацию, которая позволяет, по мнению экспертов АНБ, обеспечить защиту информационных ресурсов должным образом. За прошедшие 18 месяцев выполнены следующие мероприятия:

- введен институт уполномоченных по вопросам обеспечения безопасности информации (CIAO);

- разработан ведомственный «План защиты критической инфраструктуры», который включает ряд инновационных решений;

- определены три уровня критичности информационных систем Агентства;

- на основе результатов работ, выполненных согласно ведомственным планам мероприятий по программам подготовки к переходу на 2000 год и плану обеспечения непрерывности функционирования информационных систем, введена классификация систем, отнесенных к различным уровням критичности;

- проведены исследования нескольких методов и методик оценки риска и отобран один из них, наиболее соответствующий необходимым требованиям для использования в пределах АНБ;

- выполнена оценка рисков для наиболее критичных ресурсов;

- проведен ряд консультаций для полевых агентов с целью облегчения проведения оценок в полевых условиях;

- сформирована Группа реагирования на инциденты, связанные с информационными системами АНБ (Information Systems Incident Response Team).

Подразделения АНБ регулярно консультируют Министерство обороны и федеральное правительство по вопросам реализации положений программ INFOSEC и OPSEC в части оценки уязвимости их информационных ресурсов. В 2000 году АНБ обеспечило более 30 объединенных оценок и отчетов деятельности "Красных команд" для организаций Минобороны и около 20 - для других федеральных агентств. Кроме того, развернуто более 30 обучающих программ по программе OPSEC для федеральных агентств.

В качестве подкомитета в комитете по безопасности, секретности и критической инфраструктуре Совета уполномоченных представителей по информатизации была создана межведомственная рабочая группа, получившая название Федерального подкомитета по практическим вопросам безопасности (Federal Security Practices Subcommittee). АНБ обеспечивает поддержку данной подкомиссии и имеет своего представителя в руководстве комитета по безопасности, секретности и критической инфраструктуре.

В 2000 году АНБ продолжило поддержку ряда федеральных агентств, включая Минобороны, в вопросах разработки руководящих документов по организации закупок аппаратно-программных средств. В отношении поставок систем и средств защиты информации АНБ совместно с Комитетом безопасности телекоммуникационных и информационных систем национальной безопасности (NSTISSC) провело работы по введению в действие NSTISSP 11, документа определяющего национальную политику в вопросе обеспечения безопасности информационных технологий. NSTISSP 11 устанавливает порядок поставок сертифицированных коммерческих систем и средств защиты информации, которые должны использоваться в телекоммуникационных и информационных системах национальной безопасности, как определено в Директиве национальной безопасности № 42, от июля 1990 года. Кроме того, АНБ совместно с NSTISSC приняло участие в разработке меморандума NSTISS, вводящего в действие федеральный стандарт обработки информации (FIPS) 140-1, определяющего параметры криптографических модулей, которые могут использоваться для построения защиты несекретных информационных систем национальной безопасности. Этот Меморандум является руководством по закупкам и использованию изделий, соответствующих FIPS NIST'S 140-1, в телекоммуникационных и информационных системах национальной безопасности.

В 2000 году продолжились работы по Национальной корпорации в области информационной безопасности (NIAP) - сотрудничество между NIST и АНБ с целью выработать единые подходы для производителей и потребителей к обеспечению необходимой безопасности информационных технологий. Как заявляют специалисты АНБ, долгосрочная цель NIAP состоит в том, чтобы повысить уровень доверия потребителей к их собственным системам и сетям путем применения методик испытания и соответствующих программ сертификации. Чтобы поддержать эту цель, NIAP сосредоточила свою работу в трех ключевых областях:

- сертификация и оценка средств и систем безопасности;
- определение требований безопасности и спецификаций;
- исследования в области тестирования и оценке информационной безопасности.

Определенные NIAP действия включают:

1. Сертификация и оценка средств и систем безопасности.

- развитие "Общих критериев" для оценки информационной безопасности технологии (стандарт ISO/IEC 15408);
- развитие американского коммерческого сектора испытаний и сертификации информационных технологий. В настоящее время пять лаборатории NIAP частного сектора успешно функционируют, еще несколько ожидают своей очереди на аккредитацию;
- к концу 2000 года было проведено около десятка сертификационных испытаний коммерческих изделий на соответствие "Общим критериям". Еще 10 коммерческих изделий в настоящее время проходят эти испытания;
- успешно проведены переговоры с Канадой, Великобританией, Германией, Францией, Грецией, Норвегией, Финляндией, Италией, Испанией, Нидерландами, Израилем, Австралией и Новой Зеландией, обеспечивающие признание американских сертификатов оценки безопасности в этих странах. Как подчеркивают эксперты АНБ, это устраняет проблемы, связанные с необходимости повторной сертификации продуктов в соответствии с национальными стандартами, и обеспечивает превосходные

глобальные возможности маркетинга для американских товаропроизводителей;

- содействие правительственной политике внедрения информационных технологий (NSTISSP 11);

- в мае 2000 года проведена первая ежегодная Международная конференция по Общим Критериям (в июле 2001 прошла уже вторая подобная конференция).

2. Определение требований безопасности и спецификаций.

- координация деятельности группы по безопасности пользователей смарт-карт (Smart Card Security Users Group, SCSUG), которая включает большинство пользователей карт платежных систем American Express, Visa, MasterCard, Mondex и Europay с целью формирования требований безопасности ("профиля защиты" - в терминах общих критериев) для систем этого класса. Считается, что результатом этих работ станет улучшение безопасности для смарт-карт, используемых в финансовых сделках;

- координация деятельности Форума телекоммуникационных систем, члены которого работают над проблемами определения требований безопасности для коммутаторов и другого сетевого оборудования и услуг. Сегодня уже разработан профиль защиты коммутатора как набор общих требований безопасности;

- разработаны обучающие курсы по "Общим критериям" для продвижения этого направления.

3. Исследования в области тестирования и оценке информационной безопасности.

- создан автоматизированный инструментарий, позволяющий определить необходимые требования безопасности, сформулированные как, определенные пользователем, профили защиты или определенные разработчиком цели безопасности. Данный инструментарий позволяет выявлять несоответствия в подготовленных профилях безопасности;

- разрабатывается инструментарий для автоматизированных испытаний, который будет передан в сертификационные лаборатории для обеспечения гарантий последовательность испытаний;

- создается программа аккредитации в области информационной безопасности на соответствие «Общим критериям», с целью последующей аккредитации организаций и частных лиц, оказывающих услуги оценки безопасности систем в федеральных агентствах.

Центр реагирования на инциденты в области национальной безопасности АНБ (NSIRC) продолжает обеспечивать экспертную поддержку по идентификации, изоляции и устранению последствий нападений и вторжений, угрожающих системам национальной безопасности. Среди наиболее значимых результатов:

- в июне 2000 года АНБ разработало руководящие принципы сигнализации о нештатных ситуациях. Эти принципы определяют условия, при которых информация о нападениях может быть распределена потребителям.

- в мае 2000 года в Ситуационном центре национальной безопасности был установлен телефон "красной" АТС Минобороны, который увеличивает оперативность доступа в случае возникновения критичных ситуаций в киберпространстве;

- АНБ участвовало в учениях по обеспечению непрерывности функционирования, проведенных 1 и 2 августа 2000 года, совместно с рядом других Агентств. Текущие планы оборонительных информационных операций будут пересмотрены на основании результатов данных учений;

- представители АНБ принимают участие в нескольких рабочих группах Минобороны, Министерства юстиции и разведсообщества США, предназначенных для обмена информацией. Дополнительно, АНБ совместно с указанными выше агентствами поддержало проведение конференции, давшей возможность уточнить роль агентств в случае кибернетического нападения.

Одним из наиболее существенных результатов является формирование Национального Центра повышения квалификации в области информационной безопасности. В настоящее время есть четырнадцать вузов, участвующих в работе Центра. Очередной набор слушателей был начат 30 сентября 2000 года

Стандарты обучения руководящего персонала в области информационной безопасности включают подготовку по следующим основным специальностям:

- специалисты по информационной безопасности систем (NSTISSI 4011);
- руководство персоналом (NSTISSI 4012);
- системный администратор (NSTISSI 4013);
- уполномоченный по вопросам информационной безопасности (NSTISSI 4014);
- сертификация систем (NSTISSI 4015);
- аналитик в области оценки рисков (NSTISSI 4016).

3.4.1. Деятельность АНБ в области исследований и разработок

Исследовательское управление информационной безопасности АНБ (IARO) проводит всестороннюю программу исследований по созданию технологий и методов, необходимых для развития будущих решений в области информационной безопасности и средств ведения оборонительных информационных операций.

Наиболее эффективными в деле защиты инфраструктуры, и выдвинутый на первый план ниже, являются действия, нацеленные на обнаружение и предотвращение неправомочного доступа к критической информации и услугам. Стратегия Управления состоит в быстрой передаче передовых технологий в промышленность для их скорейшего внедрения.

Работы по ***защите активных сетей*** обеспечивают источник идей для развития методов проведения оборонительных информационных операций. Так, определенные примеры исследования в обнаружении вторжения и инструментов анализа включают:

- Thermionator, принципиально новая техника обнаружения не основанная на поиске аналогий, которая моделирует компьютерные сети как термодинамические системы, используя соотношение высокой температуры и энтропии, чтобы обнаружить аномальное поведение;

- статистическая методика построения профиля пользователя для использования при определении нарушителей среди законных пользователей системы;

- автоматизированное рабочее место аналитика вторжения, которое объединяет многочисленные системы аналитической обработки и технологии визуализации;

- опытный образец экспертной системы для использования в гибкой архитектуре анализа вторжения;

- VANAS система визуализации вторжения, которая основывается на технологии самоорганизующихся карт, изучается ее способность коррелировать и отображать данные от большого числа датчиков в интуитивном и понятном для аналитиков формате;

- развитие архитектуры комплекта инструментов обмана с целью его использования как основа для эксплуатационной способности ответа на вторжения.

Криптография - наиболее важная технология для обеспечения информационной безопасности. АНБ, как национальный первичный ресурс в области криптографии, продолжает обеспечивать криптографические алгоритмы федерального правительства, поддержанные самым высоким уровнем криптографической экспертизой математики. В этом году, существенные ресурсы были посвящены поддержке NIST в ее спецификации современных криптографических стандартов для Нации. АНБ закончило и представило всестороннюю оценку работы различных алгоритмов, конкурирующих за выбор в качестве Усовершенствованного стандарта шифрования (AES). Данная работа, является одной из наиболее важных для NIST. Также АНБ само разработало и представило в NIST новый алгоритм шифрования по требованиям AES, который обеспечит основу для надежных цифровых подписей и криптографических услуг.

Безопасное управление сетью - область технологии, которая поддерживает действие инфраструктуры управления безопасности (SMI) через развитие безопасных протоколов для разделения информации, управления сети, и контроля событий в пределах информационных систем. АНБ развивал GSAKMP структуру безопасности, схема, которая включает

эффективное компромиссное восстановление, и переданный Интернет-сообществу через IETF. Эта работа обеспечивает нормальную теоретическую основу для дальнейшей работы в области управления сетью. Была создана система отладки многомодовых сетей с целью разработки отказоустойчивых протоколов и системы моделирования для изучения устойчивости оптической сети.

Безопасность коммутируемой сети - эксперты АНБ развили и установили в эксплуатационных контекстах инструмент контроля и управления конфигурацией для АТМ сетей. Этот инструмент имеет большой потенциал и уже доказал полезный для управления состоянием комплекса АТМ сети, которые лежат в основе инфраструктур предприятия.

Обеспечение безопасности распределенных вычислений - АНБ участвовал в развитии безопасного стандарта для брокеров запросов (ORBSEC) и успешно лоббировал за его принятие. Такой стандарт помогает гарантировать целостность услуг в пределах архитектуры, основанной на предоставлении услуг.

Идентификация и установление подлинности - АНБ продолжил обеспечивать поддержку Биометрическому Консорциуму в продвижении использования биометрики для контроля доступа. АНБ продолжило исследование относительно интеграции биометрики и других технологий (типа смарт-карт), а также разработало руководящие принципы для их использования совместно с инфраструктурой открытых ключей (PKI). АНБ также поддержал NIST в создании единого формата обмена биометрической информацией.

3.4.2. Деятельность администрации США по модернизации национальной структуры защиты информационной инфраструктуры

Как часть программы полной перестройки организации, функционирования и распределения обязанностей, администрация Буша рассматривает и подходы по совершенствованию работ в области координации и руководства защитой критической инфраструктуры. В этом направлении имеются два вероятных решения.

Первое состоит в том, что Совет национальной безопасности подвергается серьезной перестройке. Все группы в составе Совета будут упразднены и затем сформированы заново в новой структуре. До какой степени Совет сохранит руководство по координации работ в области защиты критической инфраструктуры пока неясно.

Во вторых, продолжаются дебаты относительно достоинств введения во всех правительственных ведомствах института Уполномоченных представителей по информатизации в чьи обязанности должны быть включены вопросы защиты всех федеральных, не относящихся к области национальной безопасности, компьютерных систем, а также координация работ по защите компьютерных систем частного сектора.

По имеющейся информации, в настоящее время существует множество предложений, по изменению существующей организационно-штатной структуры и функциональных обязанностей ряда руководителей и подчиненных им структур, определенных в PDD-63. Согласно некоторым предложениям, основную ответственность по контролю за состоянием и координацией работ в области защиты критической инфраструктуры следует переложить непосредственно на Белый дом как часть более широкой функции противодействия террористическим актам внутри страны.

Другой подход был выдвинут американской Комиссией по национальной безопасности в 21-ом столетии (Комиссия Харта-Рудмена) члены которой предложили сформировать новое Национальное Агентство безопасности страны (National Homeland Security Agency). Это агентство предполагается создавать на основе Федерального Агентство управления в чрезвычайных ситуациях (FEMA), добавив к нему службу береговой охраны, пограничную и таможенную службу, а также некоторые другие агентства и службы. Это агентство включало бы и управление, ответственное за защиту критической инфраструктуры.

Предполагается, что судьба Управления безопасности критической инфраструктуры (Critical Infrastructure Assurance Office, CIAO), которое было создано согласно PDD-63, закончится вместе с окончанием текущего финансового года. Однако это управление занимало одно из ключевых мест в политике по защите критической инфраструктуры администрации Клинтона.

В этой связи интересно знать, какую роль будет играть в администрации Буша Национальный Центр защиты инфраструктуры (National Infrastructure Protection Center, NIPC).

NIPC, находясь под управлением ФБР, в последнее время оказался подверженным серьезной критике за то, что его персонал был сосредоточен на исследованиях и судебных разбирательствах, не имея структур и оборудования для объединения и анализа сведения из различных источников, а также в силу нежелания распространять информацию, полученную от его собственных источников, хотя этот функционал прописан за центром в PDD-63.

В силу того, что имелись определенные проблемы с функционированием NIPC, говорит то, что летом 2000 года было предложено сформировать Группу координации компьютерной инфраструктуры при Совете национальной безопасности. Группа состоит из двух подразделений: рабочей группы по разбору компьютерных инцидентов и руководящая группа разбора инцидентов.

NIPC будет находится под руководством рабочей группы, которая включает руководителя Объединенной рабочей группы обеспечения безопасности компьютерных сетей Министерства обороны, руководителя информационных операций от Агентства Национальной безопасности, директора FedCIRC и представителя министра юстиции и генерального прокурора. Эта группа рассматривает любые существенные инциденты, связанные с вычислительной техникой с тем, чтобы определить исходящую от них угрозу американской экономической и/или военной безопасности, а также планировать ответ на эти действия. Функционал этой группы во многом повторяет функционал, возложенный на NIPC, согласно PDD-63. Вместе с тем, с приходом новой администрации группа, подобно всем другим в Совете национальной безопасности, была расформирована и до настоящего времени нет сведений о том, восстановлена ли она.

До какой степени администрация Буша воспримет некоторые другие инициативы администрации Клинтона по защите критической инфраструктуры, типа федеральной программы обучения, создание FIDNET

и FedCIRC, а также программы по исследованиям и разработкам, также остается пока не известным.

Таким образом, можно сделать вывод о том, что подходы и взгляды новой Администрации по вопросу обеспечения информационной безопасности критической инфраструктуры значительно отличаются от взглядов ее предшественника. В этой связи в ближайшее время вместе с изменениями в концепции национальной безопасности, военной доктрине и внешней политике США следует ожидать и серьезных изменений в структуре и функциях сил и средств, сформированных для выполнения требований PDD-63 1998 года в области защиты критической инфраструктуры.

Анализ доступной статистики по динамике компьютерных инцидентов позволяет говорит и о том, что созданная на сегодняшний момент в США структура мало эффективна. Прежде всего, это касается организации противодействия, так называемым, «распределенным атакам отказа в обслуживании» (distributed denial of service attacks). Так как созданная система распределения информации между правительственными и частными структурами не всегда позволяет оперативно формировать стратегию противодействия таким атакам.

При этом следует учитывать, что сегодня вопросами обеспечения национальной безопасности США в информационной сфере занимается около 40 правительственных структур, и такие силы до настоящего времени не позволили построить сколько-нибудь надежной системы безопасности национальных информационных систем.

Результаты работы американских коллег могут служить наглядным примером сложности тех проблем, которые встают при попытке решить вопрос обеспечения информационной безопасности государства и его информационного потенциала, а также характера угроз, исходящих из киберпространства.

3.5. О работах в США по созданию особо защищенных информационных систем

3.5.1. Инициатива «Информационные технологии XXI века»

Ключевым пунктом раздела «Исследования и разработки» бюджета США на 2000 год стала инициатива «Информационные технологии XXI века». Эта инициатива предлагает увеличение расходов на 366 миллионов долларов на внедрение в промышленность накопленных знаний в области фундаментальной информатики, а также подготовку нового поколения исследователей, проще и полнее воспринимающего информационную революцию XXI столетия. Основываясь на предыдущих программах правительства США и существующих инвестициях в программы «Высокоэффективные вычисления и коммуникации», включая проект создания Интернет нового поколения и ускоренную стратегическую компьютерную инициативу Министерства энергетики США (ASCI), данная инициатива расширяет границы некоторых существующих исследований и обеспечивает возможности открытия новых, дополнительных разделов исследований в трех ключевых областях:

- долговременные исследования в области информационных технологий, результаты которых приведут к фундаментальным достижениям в области вычислений и связи;
- создание перспективной вычислительной инфраструктуры как инструмента облегчения научных и технических открытий в национальных интересах;
- исследования экономических и социальных последствий информационной революции, а также усилия по подготовке IT-специалистов нового поколения.

Среди прочих задач, включенных в федеральную программу «Высокоэффективные вычисления и коммуникации» есть подпрограмма, основной целью которой является разработка методов и методик создания высоко защищенных и отказоустойчивых информационных систем. Интерес к системам такого класса в последнее время значительно возрос, что связано с переоценкой основных взглядов на характер угроз, встающих перед человечеством в новом столетии.

3.5.2. Особо защищенные системы

Исследования в области высоко защищенных систем сегодня сосредотачиваются на критических информационных технологиях, необходимых для достижения предсказуемо высоких уровней системной готовности, надежности, безопасности, защиты и живучести. Высоко защищенная система - та, в которой последствия ее поведения хорошо поняты и предсказуемы. Она должна противостоять внутренним и внешним угрозам, исходящим как от опасностей естественной природы, так и от злонамеренных атак со стороны искушенного, подготовленного и хорошо финансируемого противника. По мнению специалистов, системы, которые используют подобные технологии, будут устойчивы к отказу различных блоков в результате злонамеренной манипуляции и смогут ответить на повреждение или воспринятую угрозу адаптацией или реконфигурацией своей структуры.

Подобные системы, критичные к обеспечению защиты, безопасности и жизни людей необходимы сегодня в химической промышленности, в энергетике, в области финансовых услуг, здравоохранении, машиностроении, нефтяной и газовой промышленности, транспорте, а также в чрезвычайных службах и в области национальной безопасности.

Основным федеральным ведомством, курирующим работы по созданию высоко защищенных информационных систем в США по программе «Информационные технологии XXI века» является Агентство национальной безопасности (АНБ).

3.5.3. Программа исследований Агентства национальной безопасности США в области особо защищенных систем

Организацию работы по данному проекту Агентство национальной безопасности осуществляет через работу Исследовательского совета по вопросам защиты информационных систем (INFOSEC). Основной задачей при этом является координация исследований с Агентством перспективных оборонных исследований (DARPA) и другими лабораториями министерства обороны США, Министерством энергетики, Национальным институтом стандартов и технологий (NIST) США.

Цель программы АНБ - гарантировать, что решения в области информационной безопасности сохраняют общий темп с развитием информационных технологий, что крайне важно для обеспечения потребностей службы национальной безопасности и критических областей промышленности.

Программа обеспечения информационной безопасности включает продвижение технологии активной сетевой защиты, безопасного управления сетью, создание технологий сетевой защиты, а также исследования в криптографии и технологии безопасной связи.

Активная сетевая защита

Исследования и разработки в направлении создания активной сетевой защиты обеспечивают и координируют развитие новейшей техники для поддержки проведения оборонительных информационных операций министерством обороны США. Среди последних достижений в этой области отмечают завершение изучения и обоснования минимально-необходимой информационной инфраструктуры (MEII) министерства обороны в ответ на рекомендации Комиссии оборонных исследований. По этой программе Тихоокеанским Институтом компьютерной защиты в Калифорнийском Университете в г. Дэвисе проводятся исследования и разработки инструментальных средств поддержки анализа вторжения в компьютерные сети и расследования компьютерных преступлений. В ходе исследований разработаны новые инструментальные средства и методы для анализа различных типов нападений, их источников и целей, а также технологии, способные поддержать как ручной, так и автоматический ответ на акт агрессии.

В работах по этой программе АНБ впервые успешно применило инструмент визуализации данных PARENTAGE, первоначально созданный для приложений сигнальной разведки - SIGINT, к анализу нападений на компьютерные сети. Агентство также исследует возможность применения и других технологии из области сигнальной разведки для использования в задачах защиты компьютерных сетей.

Перспективные исследования в визуальном анализе сетевых нападений сосредоточиваются на прототипах программ, способных отображать большие наборы разнородных данных, связанных с функционированием сложных распределенных информационных систем.

Агентством проводятся исследования с целью определить сценарии адекватных автоматизированных ответов для различных сценариев вторжения. Активно проводятся работы по исследованию технологии мобильных агентов с целью ее применения к обнаружению нападения и организации ответа в компьютерных сетях.

Безопасное управление сетью

Исследования и разработки в области безопасного управления сетью направлены на формирование инфраструктуры управления защитой путем разработки безопасных протоколов для совместного использования информации, управления и контроля в пределах информационных систем. По мнению специалистов АНБ, развитие протокола межсетевого взаимодействия и управления ключами (ISAKMP) обеспечивает гибкую возможность обеспечивать сетевые подключения.

Перспективные исследования в этой области должны помочь создать расширенные спецификации для защищенного протокола Интернет нового поколения. В этой связи АНБ продолжает совершенствовать рекомендации протокола IPSEC.

Наряду с защищенным механизмом маршрутизации и услуг управления групповыми ключами, исследования и разработки сосредоточатся на формировании концепции ключевого управления и некриптографических методов защиты для групповой связи. В области совершенствования управления инфраструктурой открытых ключей шифрования ведется доработка стандарта X.509 по организации работы с цифровыми сертификатами.

Разработка методов сетевой защиты

Основной целью этого направления исследований является обеспечение защиты информации в сетевой среде, которая характеризуется глобальным распределением систем и услуг наряду с совместным использованием информации. Одной из главных проблем является формирование защитного контура на границе информационной системы. Указанная проблема включает необходимость решения задачи установления и последующей защиты границы сети с целью установить точки контроля, управления и защиты от нападения из киберпространства.

Защита границы сети в настоящее время осуществляется, прежде всего, высокоэффективными системами типа межсетевых экранов, реализованных с использованием метода асинхронной передачи данных. АНБ достаточно широко использует результаты исследования в этой области, чтобы защитить собственные внутренние сети, причем с активным привлечением широкодоступных коммерческих систем.

По мнению рядя экспертов, результатом перспективных исследований в этой области должны стать высокоэффективные устройства защиты границы сети, которые добавят способность фильтровать данные различных протоколах с большей эффективностью и намного большей скоростью передачи данных, чем в существующих системах. Чтобы разрабатывать соответствующие решения в области информационной безопасности, АНБ также реализует программу оценки эффективности защиты перспективных технологий коммутации для сетей асинхронной передачи данных.

Кроме этого, АНБ провело ряд исследовательских работ по созданию ряда компонент, включенных в высоко защищенную операционную систему FLUK, разработанную университетом штата Юта. В этой области перспективные исследования будут сосредоточены на моделировании дополнительных компонентов защиты типа сервера политики безопасности, сервера взаимодействия служб безопасности и криптографической подсистемы и др.

Исследования в области создания сетевой защиты также включают технологии идентификации и аутентификации, применительно к персоналу, файлам, политике безопасности и аппаратным средствам. Программа на 2000 финансовый год планировала исследования в области основных

биометрических идентифицирующих технологий распознавания отпечатков пальцев, лица и распознавания речи, путем создания высокопроизводительных алгоритмов.

Кроме этого, АНБ проводит исследование, нацеленное на обеспечение защиты от физического вмешательства в деятельность информационных систем путем поставки микросхем со встроенными средствами несанкционированного доступа. Решение поставленной задачи достигается путем разработки специального защитного покрытия для подложек полупроводниковых кристаллов микросхем, предназначенных для использования в критических информационных системах.

Криптография

В качестве основного национального эксперта по криптографии, АНБ обеспечивает создание криптографических алгоритмов для удовлетворения потребностей федерального правительства США. Используя последние достижения в области криптоматематики, АНБ продолжает создание новых алгоритмов, соответствующих уникальным требованиям министерства обороны и разведсообщества США.

В течении ряда лет АНБ проводит исследования в области шифрования с открытым ключом. Сегодня эти исследования сосредоточены на совершенствовании алгоритмов и протоколов управления ключами; на создании быстрых и эффективных арифметических методов, основанных на эллиптических кривых; надежных методов аутентификации и др.

Квантовые вычисления - новая и мощная угроза традиционной криптографии. По заявлению ряда экспертов, сегодня исследователи АНБ пытаются противостоять этой угрозе, используя методы обмена ключей, реализованных на основе квантовой физики для обеспечения требуемого режима защиты. Недавнее исследование продемонстрировало выполнимость обмена ключами на расстояние более 50 километров по волоконно-оптическому кабелю, что весьма мало для коммерческого использования, но вполне оптимистично для результата пилотного проекта. Кроме этого, АНБ разрабатывает новые классы криптографических алгоритмов, которые не

восприимчивы к нападениям с использованием особенностей методов квантовых вычислений.

Одно из направлений работ АНБ связано с тем, что агентство пытается разработать стандартизированные интерфейсы по интегрированию криптографии в широко используемое программное обеспечение для всех министерств и ведомств США. Результатом этих работ стало создание криптографических интерфейсов прикладного программирования (CAPI), позволяющих достаточно легко встраивать необходимые защитные функции в приложения разного класса. Такой подход позволяет пользователям выбирать уровень защиты, в котором они нуждаются, в пределах от коммерческих алгоритмов от компаний типа RSA Data Security, Inc, до разработанной министерством обороны США аппаратной технологии типа Fortezza. В настоящее время АНБ разрабатывает рекомендации по применению CAPI для широкого класса служб безопасности.

Безопасная технология связи

Особые требования к методам передачи информации и связанной с ней инфраструктуры предъявляются во время кризиса, либо с началом военных действий. Исследование АНБ охватывает следующие технологии повышения надежности и достоверности связи: кодирование речи, беспроводная связь, высокоскоростная криптография и оптические сети.

Исследования по кодированию сосредоточено на создании алгоритмов, требующих малых ресурсов, которые необходимы для оцифровки, шифрования и передачи голоса в низовом звене инфраструктуры связи.

Исследования беспроводных коммуникаций направлены на выработку мер противодействия уязвимости беспроводных сетей. Результаты работ используются для совершенствования стандартов, а также для обоснования выбора критических беспроволочных технологий при создании информационных систем, необходимую, чтобы гарантировать работу решений в любых условиях. Так, АНБ разработало технологию, позволяющую использовать безопасные услуги голосовой связи (STU-III) поверх европейской сотовой сети GSM.

Исследования в области высокоскоростной криптографии включает создание высокопроизводительной микроэлектроники и высоко эффективные криптографические алгоритмы. АНБ разработан проект 10 гигабитного шифратора для сети асинхронной передачи данных.

Исследования в области оптических сетей связи сосредоточены на разработке концепции построения полностью оптической системы, включая разработку проектов фотонных коммутаторов и шифраторов, призванных устранить в сетях следующего поколения низкоскоростные электронные компоненты.

Живучесть информации

Агентство перспективных оборонных исследований Минобороны США (DARPA) разрабатывает технологии с целью защитить критические системы министерства обороны от нападений на или через информационную инфраструктуру.

Разработка методов повышения живучести информационных систем имеет своей целью уменьшить уязвимость национальной и оборонной вычислительной инфраструктуры, которая может быть использована противником при организации ведении информационной войны. Так, считается, что с использованием систем обнаружения вторжения возможно обнаружить факт нападения на инфраструктуру, после чего нанесенный ущерб будет оценен, и будет реализован адекватный ответ.

DARPA продолжает разрабатывать технологии обеспечения работы информационных сетей, в которых циркулирует секретная информация. Это направление исследований включает механизмы защиты и устойчивые сетевые протоколы, которые позволят обеспечить непрерывное функционирование системы во враждебной среде.

Кроме этого, Национальное агентство по аэронавтике и космическим исследованиям (NASA) и Национальный научный фонд (NSF) также проводят исследования по разработке технологий, предназначенных для обеспечения высокой степени безопасности информационных систем.

В Принстонском университете при финансовой поддержке Национального научного фонда реализуется проект безопасного Интернет-программирования, который сосредотачивается на защите мобильных систем, использующих код Java, JavaScript и ActiveX. Известно, что эти технологии имеют массу уязвимостей, которые могут быть использованы злоумышленниками при организации атак на информационные системы.

3.5.4. Национальное соглашение в области информационной безопасности

Данное направление разрабатывается в рамках программы National Information Assurance Partnership (NIAP), которая осуществляется Агентством национальной безопасности США и Национальным институтом по стандартам и технологиям (NIST) с середины 90-х годов. В рамках этой программы летом 1999 года АНБ и соответствующие ведомства ряда других стран (прежде всего – страны НАТО) договорились об определении единого набора стандартов по тестированию (получившего название Common Criteria – «общие критерии») инструментальных средств защиты информации, операционных систем и баз данных. Основу этому направлению работ положил отчет, опубликованный в 1989 году группой американских специалистов по информационной безопасности, в котором доказывалась необходимость подготовки международного стандарта, призванного заменить стандарт Министерства обороны США «Критерии оценки надежных компьютерных систем» (известный как «Оранжевая книга»). Особо следует отметить, что данный стандарт разрабатывался во исполнение директивы президента США PDD-63, положившей начало работам по защите критической инфраструктуры.

Цели программы включают:

- функционирование системы общих критериев оценки;
- обеспечение проведения оценок уровня защиты в лабораториях частного сектора;
- обеспечение непротиворечивости стандартов в области защиты информации;

- увеличивающаяся готовность и безопасность сертифицированных изделий;
- создание международного климата, способствующего экспорту американской продукции.

3.5.5. Программные технологии и стандарты

Национальный институт стандартов и технологий США (NIST) продолжает работу в нескольких областях по созданию стандартов разработки программного обеспечения и инструментальных средств анализа, среди них можно выделить следующие области:

- ***Качество программ***; по этому направлению NIST разрабатывает модели, методы, и инструментальные средства для анализа программных процессов, чтобы улучшить качество программного обеспечения; исследования включают формальные методы, верификацию, оценку функционирования и эталонное тестирование.
- ***Анализ программ***; по этому направлению исследователи разрабатывают инструментальные средства для статического и динамического анализа программного кода, сосредотачиваясь на выявлении соответствия спецификациям и выявлению причин отклонения от спецификаций.
- ***Надежность программ;*** в этом направлении создаются технологии, способные обеспечить создание надежного программного обеспечения для применения в промышленности и административных структурах.
- ***Стандарты программирования;*** NIST разрабатывает и совершенствует стандарты программирования, удовлетворяющие требованиям администрации США, в частности NIST разработал и поддерживает интерактивную поисковую систему федеральных стандартов в области обработки информации (FIPS).

Проведенный краткий анализ основных направлений программы создания высоко защищенных информационных систем, реализуемой правительством США в рамках инициативы «Информационные технологии XXI века», показал, что данному направлению исследований в предстоящие

годы будет уделено значительное внимание. Это связано с тем, что выявленная в ходе ряда исследований уязвимость национальной информационной инфраструктуры США в настоящее время может стать, а иногда уже становится, объектом информационного терроризма, что может привести к серьезным последствиям. Так отмечается, что компьютерный вирус длинной всего в несколько десятков строк кода, попав в информационную систему управления воздушным движением, может всего за несколько минут парализовать работу любого аэропорта в случае, если не применяются специальные средства повышения надежности функционирования информационной системы, а это связано с безопасностью и сохранением жизни сотням и тысячам авиапассажиров.

К сожалению, в России до настоящего времени в силу отсутствия достаточного финансирования, а зачастую просто в силу недооценки возможных последствий информационного терроризма, разработка специализированных информационных систем с повышенным уровнем информационной безопасности была областью интереса только ограниченного круга специалистов силовых ведомств. Вместе с тем реальность текущего момента показывает, что широкое применение общедоступных коммерческих систем там, где это связано с возможностью нанесения невосполнимого ущерба, крайне нежелательна и просто опасна.

3.6. Организация крупномасштабных сетей

Еще одним важным пунктом программы «Информационные технологии XXI века» является создание крупномасштабных высокопроизводительных телекоммуникационных сетей.

Исследования и разработки в области создания крупномасштабных сетей призваны обеспечить технологическое лидерство США в высокопроизводительных межсетевых коммуникациях. Данные технологии позволят обеспечить такой уровень развития методов построения сетей, который необходим для дальнейшего роста общедоступных сетей типа Интернет и внутренних сетей федеральных министерств и ведомств. Первоначальные инвестиции правительства США в исследования и разработки сетевых технологий дали возможность осуществит формирование

технологической основы сегодняшней глобальной сети Интернет. Научно-исследовательские лаборатории, научное сообщество и промышленность помогли развернуть прототипы создаваемых сетей на национальном уровне, а также организовать производство популярных приложений - электронной почты и программ просмотра гипертекста - которые изменили сам подход в использовании ЭВМ человеком. Все это проложило путь к лидерству США в много миллиардной информационной индустрии.

Важным является то, что результаты совместных исследований и разработок в области создания крупномасштабных сетей, проводимых научным сообществом, промышленностью и правительством, являются своеобразным мостом, переброшенным к частному сектору, где их использование преобразовывает сам характер общественных связей. Ключевыми направлениями исследований являются фундаментальные достижения в области создания сетевых компонент и технологий разработки и управления крупномасштабными сетями будущего. Считается, что программы создания крупномасштабных сетей в рамках правительственной инициативы «Информационные технологии XXI века» позволят:

- увеличить эффективность исследований в области сетевых технологий, финансируемых из федерального бюджета;
- увеличить эффективность в создании федеральных сетей;
- создать сетевые приложения, которые позволят решить ряд задач обеспечения национальной безопасности;
- обеспечить обмен информацией и облегчить взаимодействие участников в ходе проведения исследований и разработок;
- разработать механизмы сотрудничества в области исследований и разработок среди федеральных агентств, правительственных лабораторий, научного сообщества и промышленности.

Так в 1998 году основное внимание разработчиков было сосредоточено на инициативе создания Интернет следующего поколения (Next Generation Интернет, NGI). В основе создания NGI лежат программы развития крупномасштабных сетей, обеспечивающих исследования и разработку передовых технологий и приложений, а также тестирование и демонстрацию

результатов, внедрение которых позволит значительно расширить возможности Интернет.

Усилия научного сообщества по данному проекту координируются рабочей группой проекта создания масштабных сетей (LSNWG). С целью получения адекватного представления о ходе работ по проекту LSNWG организовала сбор необходимой информации от четырех специализированных рабочих групп, отвечающих за состояние дел по конкретному направлению развития проекта. Такими группами являются.

Объединенная инженерная группа (Joint Engineering Team, JET). JET координирует работы по выработке общей сетевой архитектуры и организации взаимодействия между сетями федеральных агентства (FedNets) и сторонними высокопроизводительными экспериментальными сетями. JET обеспечивает тесную координацию среди поставщиков, научного сообщества и промышленности в вопросе взаимодействия и предоставления услуг с тем, чтобы улучшить характеристики, доступные конечному пользователю, а также избежать дублирования ресурсов и усилий в обеспечении предоставления высококачественных услуг. Кроме того, JET сотрудничает с академическим сообществом по разработке гигабитных коммутаторов (Gigapops), сетью Abilene (консорциум компаний Qwest, Cisco, Nortel и Университета штата Индиана), а также с участниками программы создания Интернет 2 (I2).

В настоящее время JET помогает осуществлять тестирование и отладку NGI. Наряду с этим JET поддерживает взаимодействие между федеральными агентствами и сетью Abilene с целью обеспечения возможности доступа к более дешевым телекоммуникационным услугам, обеспечивающих пользователей географически удаленных территорий США (типа Аляски и Гавайев).

Группа исследования организации сети (Networking Research Team, NRT). NRT координирует исследовательские программы по организации сетей в федеральных агентствах, распределению информации о результатах исследований среди участников работ, а также поддерживает действия по достижению основных целей NGI. Проводимые работы позволяют снизить время на получение необходимой информации по результатам исследований

и способствуют улучшению взаимодействия между разработчиками и конечными пользователями.

Группа применения высокопроизводительных сетей (High Performance Networking Applications Team, HPNAT). HPNAT координирует исследования и разработки с целью сохранить и расширить технологическое лидерство США в использовании высокопроизводительных сетей посредством проведения исследований, результатом которых является создание усовершенствованных технологий организации сетей, новых услуг и повышения производительности. Эти достижения позволят получить новые более приспособленные сетевые приложения для решения задач, стоящих перед федеральными агентствами, помогая создавать основу для длительного развития национальной информационной инфраструктуры. HPNAT обеспечивает механизмы сотрудничества среди федеральных агентств, правительственных лабораторий, научного сообщества и промышленности в разработке приложений для крупномасштабных сетей, а также организовывает распространение информации, включая проведение демонстраций технологий, конференций и семинаров.

Группа обеспечения защиты Интернет (Интернет Security Team, IST). IST облегчает испытание и экспериментирование с усовершенствованными технологиями защиты и служит центром по выработке требований к системе защиты. Эта группа снабжает LSNWG необходимой информацией для организации исследований по защите NGI. IST финансирует разработку и тестирование систем защиты Интернет, тесно взаимодействуя с агентствами и JET, помогая осуществлять подобные эксперименты, а также делает их результаты доступными для национальных и международных исследователей в области безопасности.

3.6.1. Программа исследований и разработок в области создания крупномасштабных телекоммуникационных сетей

Программа исследований и разработок в области создания крупномасштабных сетей направлена на удовлетворение требований участвующих в работах агентств, а также на разработку технологий и приложений, расширяющих возможности Интернет, в этот круг программ включены следующие.

Программа исследований усовершенствованной сетевой инфраструктуры (ANIR). Данная программа объединяет исследования научного и технического сообщества США с целью повышения эффективности проводимых исследований в области фундаментальных работ по изучению сетей и сетевой инфраструктуры. В рамках программ обеспечивается разработка и развертывание высокопроизводительных сетей для проведения исследований по многим научным направлениям, требующим высокоскоростных вычислений, с целью выявления наиболее перспективных технических и технологических решений для их последующего внедрения в сети нового поколения.

Согласно этой программе сеть vBNS связала высокопроизводительные вычислительные центры Национального научного фонда и около 100 исследовательских институтов, занятых в работах по исследованию возможностей сетей следующего поколения. Связи устанавливаются с такими исследовательскими учреждениями, программы работы которых требуют от сетей самой высокой производительности.

ANIR поддерживает исследования по разработке протоколов сетевого доступа и управления, инструментальных средств управления сетью, методов организации беспроводных сетей, мобильных вычислений, оптических сетей, программного обеспечения поддержки распределенных вычислений, программного обеспечение поддержки поиска и распределения сетевых ресурсов, а также устройств и подсистем ввода-вывода.

Разработка технологии организации сети. Программа интернет-технологий Национального научного фонда фокусируется на достижениях фундаментальной науки и техники, необходимых для повышения эффективности высокоскоростной передачи информации в сетях и распределенных системах. В рамках программы поддерживается разработка

методов комплексного мониторинга сети, обнаружения проблем и механизмов их разрешения, разработка автоматизированных и усовершенствованных инструментальных сетевых средств, сетевого обеспечивающего программного обеспечения и сетевых инструментальных средств, а также создание сетевых приложений, которые способствуют организации совместных исследований и обмену информацией.

Активные сети. Управление перспективных исследований Министерства обороны США (DARPA) разрабатывает новую структуру сети, в основе которой лежит программируемая инфраструктура. В рамках программы разрабатываются методы организации активных сетей, методы управления и высокоуровневые услуги для конечного пользователя. Данная программа тесно взаимодействует с разработкой технологий сетей, проводимых Министерством обороны США, НАСА и другими федеральными агентствами.

Глобальные подвижные информационные системы. Работы по созданию глобальных подвижных информационных систем, проводимые DARPA, обеспечат мобильным пользователям возможность доступа и использование полного объема услуг, доступного в информационной инфраструктуре Министерства обороны.

Масштабируемая организация сети. Программа разработки расширяемой сети, проводимая DARPA, поддерживает базовые сети необходимые для адаптации к масштабным изменениям трафика в современных сетях. Достижения в этой области позволят обеспечить доступ к географически распределенной и гетерогенной информационной инфраструктуре гарантируя при этом, что емкость основной сети и ее услуги будут приспособлены к особенностям ускоренного роста масштабов системы. Чтобы поддерживать эту программу Управление перспективных исследований Министерства обороны США в 1999 году инициировало программу создания гигабитной беспроводной сети связи, включающей космический сегмент на базе низкоорбитальных спутников.

Создание сверхвысокоскоростных сетей. Результатом работ по этой программе, проводимой Агентством национальной безопасности США, должна стать инфраструктура высокоскоростной сети со скоростью

предоставления канала в несколько гигабит в секунду и способностью поддержать устойчивые потоки данных, по крайней мере, до сотен мегабит в секунду уже сегодня и, в конечном счете, достичь скорости потока информации в несколько гигабит в секунду. Еще в 1999 году Агентство национальной безопасности увеличило эффективность сетей путем снижения общего числа уровней протокола организации сети, а также путем перемещения управления к оконечным узлам сети. В сотрудничестве с NRL и Разведывательным управлением Министерства обороны США (РУМО), АНБ использовало режим асинхронной передачи (ATM) с разделением по длине волны для передачи 720 цифровых сигналов по 1.5 Гбит каждый на дистанцию в 400 километров через восемь ATM-коммутаторов.

Кроме этого, в рамках программы АНБ начало эксплуатацию полностью оптической сети, базирующейся на двух оптических технологиях:

- прототипах серийных маршрутизаторов с волновым разделением от Lucent, создаваемых в рамках одного из проектов Консорциума MONET, финансируемого DARPA;
- оптический коммутатор от Optical Networks, Inc.

Эта сеть позволяет АНБ организовать прямую связь между конечными пользователями без вмешательства электрооптического преобразования, что существенно повышает защищенность системы связи от несанкционированного доступа и перехвата сторонних излучений.

Основываясь на результатах экспериментов 1999 года, АНБ в настоящее время изучает новые подходы к управлению перегрузкой в сети, разрабатывая методы распределенного управления сетью связи.

Сети для биомедицинских исследований. Национальный институт рака (NCI) применяет развивающиеся технологии организации сети и высокоскоростные интерфейсы к вычислительной инфраструктуре одного из суперкомпьютерных центров (Frederick Biomedical Supercomputing Center, FBSC) с целью улучшить доступ к ресурсам для членов биомедицинского исследовательского сообщества. Считается, что это позволит получить новые данные по технологиям передачи данных в локальных мультимедиа-сети.

Усовершенствованная АТМ-сеть Национального агентства обработки и распределения информации дистанционного зондирования Земли. В результате проведенных экспериментов и испытаний, финансируемых в соответствии с этой программой. NOAA разворачивает АТМ-сеть. Сеть будет иметь 2400 узлов, объединенных в 80-90 виртуальных локальных сетей (VLANs). Такая архитектура дает избыточность и гибкость, необходимую для распределения полосы пропускания каналов в зависимости от индивидуальных потребностей. Инфраструктура сети должна поддержать в реальном масштабе времени обработку наблюдений поверхности Земли, получаемой со спутников

Федеральные сети (FedNets). FedNets - сеть федеральных агентств - включает действующие информационные сети федеральных агентств и высокоскоростные экспериментальные сети. FedNets включает:

- vBNS - высокопроизводительную магистральную сеть связи Национального научного фонда;
- DREN - исследовательская и инженерная сеть Министерства обороны;
- NREN - исследовательская и образовательная сеть NASA;
- NISN - сеть интегрального обслуживания NASA;
- Esnet - сеть научного сообщества энергетиков.

Точка доступа к высокоскоростным сетям для научного сообщества (STAR TAP) и международная сеть (iGrid). Национальный научный фонд установил точку доступа (STAR TAP) в точке сетевого входа (NAP) компании Ameritech в Чикаго для связи vBNS с аналогичными международными сетями. STAR TAP управляется Электронной лабораторией визуализации (EVL) университета штата Иллинойс в Чикаго, Национальная Лаборатория Argonne и NAP Ameritech - точка обмена с Интернет следующего поколения (NGIX), который соединяется с FedNets и Abilene, обеспечивая международное сотрудничество с другими Федеральными агентствами, университетами и промышленными компаниями.

Более 15 сетей разных стран были объединены посредством STAR TAP к концу 1999 года. Среди них сети Азиатско-Тихоокеанского консорциума (APAN), Канады (CA Net), сеть Европейской лаборатории физики элементарных частиц (CERN), Франциb (Renater), Израиля, Нидерландов (SURFnet), скандинавских стран (NORDUnet), Сингапура (SingaREN), Тайваня (TANet), Американо-азиатского тихоокеанского консорциума (TransPAC) и американо-российский Консорциум (MirNET). Одна из главных особенностей STAR TAP - разрабатывает и допускает объединенный подход к управлению, измерению характеристик, планированию и потреблению географически распределенными параметрами, вычисление, хранение, и ресурсы показа - названное Международной Сетью (iGrid).

IGrid приложения, инструментальные в разработке высокой скорости международные сети и услуги включают:

- параллельные приложения выполняемые на глобально-распределенных вычислительных элементах
- дистанционный доступ к инструментам типа электронных микроскопов и ускорителей
- телеобучение и общедоступные рабочие пространства
- совместные медицинские системы диагностирования
- новые подходы к высокому качеству цифровое видео по коммерческим сетям
- API и комплекты инструментов для доступа, идентификации, распределения ресурса, и коммуникаций, чтобы поддержать разработку распределенных приложений
- инструментальные средства мультимедиа конференц-связи, которые требуют качества обслуживания и обработки различных индивидуальных потоков в пучке (например, звуковое качество, обычно предпочитаются по видео, и достоверные протоколы необходимы для текстовой конференц-связи).

Провайдеры высокоскоростных сетей (HPNSPs). Национальный научный фонд обозначил категорию коммерческих провайдеров высокоскоростных сетей (HPNSPs), которые предоставляют

высокоскоростные услуги связи по широкополосным сетям для университетов и федеральных агентств, а также снабжают высококачественными услугами неправительствнные учреждения.

Сеть Abilene - первый абонент HPNSP. Продавцы координируют свои действия с HPNSPS посредством взаимодействия с JET и другими группами LSN.

Сеть научного сообщества энергетиков (ESnet). Сеть ESNET Министерства энергетики ориентирована на услуги, которые необходимы для министерства. Она предоставляет усовершенствованный протокол Интернет (IP), и услуги сети ATM для 30 сайтов министерства энергетики, включая национальные лаборатории, университеты и международных партнеров.

Основная сеть и программы исследования защиты сети включают услуги высокоскоростного доступа к приложениям, маршрутизации и управления перегрузкой, дифференцированные услуги управляемой инфраструктуры защиты и архитектуре, интегрирование услуг поперек автономных систем и сетей, измерения характеристики сети и управления и инфраструктуры, чтобы поддержать, и науку задачи и организацию сети R&D.

3.7. Эксперты RAND Джон Арквилла и Дэвид Ронфелд о путях борьбы с сетевыми структурами новых противников

В одном из информационных бюллетеней корпорации RAND, посвященном итогам 2001 года («Full Alert. An Arsenal of ideas for the War Against Terrorism», RAND Review, Fall 2001, Vol. 25, No. 3), опубликован ряд материалов, безусловно, заслуживающий внимания.

Среди таких материалов - статья «Битва сетей» Джона Арквиллы консультанта RAND и Дэвида Ронфелда старшего социолога RAND.

Статья основана на предположении, что, если сеть аль-Каеды Осамы Бен-Ладена является главным противником США на текущий момент, то Америка должна превзойти эту сеть на всех пяти уровнях, на которых сети

информационной эпох должны превосходить противника: структурном, мировоззренческом, доктринальном, технологическом и социальном[76].

Авторы считают, что на структурном уровне, глобальная конфронтация сегодня бушует между иерархическими (государственные игроки) и сетевыми структурами (негосударственные игроки). Возраст иерархий уступает возрасту сетей. Еще не ясно, имеет ли сеть аль-Каеды единственный узел коммуникаций и управления, центром которого является Бен-Ладен, или же она имеет множество таких узлов. Первый вариант наиболее прост. Если она имеет единственный узел, то смерть Бен-Ладена или его захват американскими войсками указал бы на поражение его сети. Однако большинство сетей имеет архитектуру типа «паучьей сети», это может иметь место и в случае с аль-Каедой. Будучи гораздо более избыточной и гибкой, такая структура обладает большей устойчивостью, что затруднит ее окончательное уничтожение. В этой ситуации, считают авторы статьи, Соединенные Штаты и их союзники должны совместно изучать особенности сетевых архитектур. Частично такой подход уже работает на примере взаимного обмена разведданными.

Подобные изменения являются большой и сложной работой для громоздкой американской бюрократии, которой необходимо развернуть широкие, хорошо организованные сети военных и юридических структур, элементов разведки, чье сотрудничество критично для достижения успеха. Следует отметить, что американские антитеррористические агентства развивались в этом направлении уже в течение ряда лет, но взаимная конкуренция и недоверие часто замедляли продвижение к намеченной цели.

Второй аспект противоборства касается мировоззренческого уровня. Западные идеи относительно распространения свободных рынков, свободных народов и открытых обществ сталкиваются с мусульманским убеждением относительно эксплуатационной, агрессивной и высокомерной природы западного присутствия в исламском мире. Соединенные Штаты еще больше ужесточили свою позицию, считая террористические атаки «действиями войны» против «цивилизованного мира», а американское общественное мнение гальванизировалось возрождением метафоры Перл Харбора.

---

[76] *The Advent of Netwar*, John Arquilla, David Ronfeldt, RAND/MR-789-OSD, 1996, 127 pp., ISBN 0-8330-2414-0.

Сегодня, больше чем когда-либо, необходимо овладеть искусством «информационной стратегии» реализуемой бригадами «специальных информационных сил», которые могли бы обобщать и распространять необходимую информацию. И везде, где США используют группы войск, необходимо остерегаться порождения неприятия этого присутствия со стороны мирного населения, которое чревато невоенным поражением. Все это необходимо, чтобы быть неуязвимыми к встречному обвинению в создании «государственного террора».

Третий аспект заключается в доктрине. Сеть Аль-Каеда, очевидно, организует атаки по множеству направлений рассеянными подразделениями. Бен-Ладен и его когорты, похоже, следуют доктрине «пчелиного роя». При этом различными узлами сети инициируется ряд эпизодических, пульсирующих атак во ряде мест, распределенных в глобальном пространстве и времени. Против этой доктрины, Соединенные Штаты пока еще немного, что могут противопоставить. Наступательная часть американской военной доктрины все еще основана на стареющих понятиях стратегической бомбардировки, которая, вряд ли будет правильным подходом в борьбе с терроризмом. В этих условиях должна быть развита новая доктрина, основанная на принципе «роения» малых мобильных и хорошо вооруженных подразделений, которая бы подчеркивала особую роль специальных сил и ограниченного применения авиации. Авиация использовалась бы главным образом для огневого обеспечения подразделений на земле.

В-четвертых, на технологическом уровне Соединенные Штаты обладают массой очень передовых систем, в то время как Аль-Каеда таковых не имеет, или имеет очень немного таких систем. Однако только малая часть таких высокотехнологических систем может быть полезна против рассеянных сетевых структур террористов.

В-пятых, на социальном уровне, сеть Аль-Каеда демонстрирует тесные религиозные и родственные связи среди людей, которые разделяют племенное, родовое представление «нас» против «них». В этом отношении Соединенные Штаты стоят перед сложной дилеммой. Если метафора Перл Харбора поддерживается, и если американские действия приводят к успешным ранним контрударам, то может иметься необычная общественная

сплоченность, чтобы поддерживать войну против терроризма. В случае, когда встает вопрос: должны ли контрудары следовать как элемент «войны» или «исполнения закона», возможно появление различных социальных реакций в США и Европе.

В заключение авторы отмечают, что Аль-Каеда на сегодняшний день обладает преимуществами на структурном, доктринальном и социальном уровнях, что серьезно осложняет борьбу с ней. Соединенные Штаты и их союзники, возможно, имеют преимущества только на мировоззренческом и технологическом уровнях. Поставленный в сложную ситуацию, Запад сегодня должен строить его собственные сети и изучать роящиеся вражеские сети, пока они еще не могут быть разрушены. Ключом к разрешению противоречия является понимание того, что в современном сетевом или информационно-ориентированном конфликте между сетями информационной эпохи гораздо большее значение имеет структурное и доктринальное превосходство, чем превосходство технологическое.

Другой, не менее интересный материал принадлежит Брюсу Хоффману - вице-президенту по внешним связям RAND, директору Вашингтонского офиса этой корпорации. В одном из последних своих выступлений перед Конгрессом США он очертил круг тех задач, которые предстоит решить американской Администрации в ходе борьбы с терроризмом.

Прежде всего, Б.Хоффман отметил, что для эффективной борьбы с терроризмом США нуждается в объединенном федеральном усилии, повседневных оценках угрозы, и трансформации всей структуры национальной безопасности.

Он отмечает, что множество федеральных агентств и программ, занимающихся антитерористической деятельностью, остаются сильно фрагментированными и не скоординированными, с взаимно пересекающимися обязанностями, но без ясной цели. Сейчас, по мнению автора статьи, необходимо всестороннее усилие, чтобы связать воедино под более четким руководством то огромное число возможностей и средств, которые Соединенные Штаты могут использовать в борьбе против терроризма.

Далее он отмечает, что предварительное условие для формирования национальной стратегии являются регулярные оценки террористической угрозы как внешней, так и внутренней. Последняя всесторонняя оценка внешней террористической угрозы в США была предпринята во время войны в Персидском заливе в 1990-91 годах. Хотя после этого и разрабатывался ряд оценок, они не учитывали те глубокие изменения в природе, действиях и мышлении террористов, которые стали очевидны в последние годы. Как только будет установлено ясное понимание понятия «новый терроризм» его мотивы, намерения и имеющиеся возможности, тогда станет возможным определить способ, позволяющий, прогнозировать, предотвращать и сдержать террористические атаки.

В-третьих, Б.Хоффман особо отмечает, что необходимо трансформировать все американское разведсообщество, чтобы иметь возможность противостоять террористическим угрозам не только сегодня, но и завтра. Он считает, что архитектура национальной безопасности США - реликт, символ холодной войны, который создавалась больше чем половина столетие назад, чтобы противостоять специфичным угрозам от отдельных стран со специфичной идеологией. Архаичность этой архитектуры, которая ориентирована в основном на военные угрозы и, следовательно, на военную разведку, была доказана разрушительными атаками, которые были выполнены 11 сентября негосударственными, невоенными противниками. Основа американской архитектуры национальной безопасности существенно не изменялась начиная со времени Второй мировой войны. Так около 60 процентов усилий разведсообщества сосредотачивается на военной разведке, имеющей отношение к регулярным вооруженным силам конкретных суверенных государств. Восемь из тринадцати американских Агентств, отвечающих за сбор развединформации, докладывают ее непосредственно министру обороны, а не руководству Центрального разведывательного управления. Это не удивительно, ведь, по мнению Б.Хоффмана, американская HUMINT (агентурная разведка) сегодня практически не дееспособна в силу того, что военная ориентация разведсообщества США основывается на технологической разведке типа MASINT (сигнатурная разведка), ELINT (электронная разведка) и SIGINT (сигнальная разведка),

осуществляемой, как правило, с использованием спутников на околоземной орбите.

Увеличивающееся поражающее действие межнациональных, негосударственных и невоенных противников, которые объединены в открытые сети, а не в жесткие иерархии «командования и управления», подчеркивает необходимость перераспределить сбор разведывательных сведений от традиционных военных противников на спектр противников скрытых, которые теперь являют собой угрозу национальной безопасности США.

Бюджет американского разведсообщество оценивается примерно в 30 миллиардов долларов, что уже больше чем бюджеты национальной обороны большинства стран мира (за исключением шести высокоразвитых стран Запада). Хоффман считает, что необходимо перераспределить персонал и ресурсы так, чтобы США могли адекватно реагировать на текущие и, возможно, будущие террористические угрозы. Анахроничная архитектура разведки создала опасный разрыв в обороноспособности страны. ЦРУ ответственно за внешнюю разведку и прогноз развития внешнеполитической обстановки. В соответствии с законом, ЦРУ не может работать в пределах Соединенных Штатов. Антитеррористические действия внутри страны падают на ФБР. Однако ФБР – это, прежде всего, агентство, занимающееся расследованием уголовных преступлений, а не спецслужба. Хуже все же, что его зона интересов перекрывает очень широкий спектр, возможно, даже слишком широкий, спектр которых включает похищения, грабежи банков, контрразведку, серийные убийства и другие, более прозаические, преступления в дополнение к терроризму.

Новое Управление внутренней безопасности потенциально дает идеальную возможность устранить этот промежуток между ЦРУ и ФБР, создавая новую аналитическую возможность раскрытия внутренних террористических угроз. Однако, по мнению Б.Хоффман, такая аналитическая возможность должна быть укреплена новой организационной структурой, в которой должны быть скоординированы антитеррористические усилия всех агентств. Пока еще нет полной ясности в том, будут ли предоставлено достаточно полномочий и ресурсов Управлению внутренней безопасности для выполнения этой задачи.

Пришло время, по мнению автора, отказаться от бюрократических проволочек, и радикально трансформировать внешние и внутренние возможности по борьбе с терроризмом. В заключении автор статьи высказывает мысль о том, что подобно тому, как задача борьбы с наркоторговлей была в свое время расценена как серьезная задача в обеспечении национальной безопасности США и были созданы специализированные Агентства по борьбе с наркотиками (причем они специализируются исключительно на борьбе с наркомафией не отвлекаясь «по пустякам»), необходимо создание подобных Агентств, занимающихся исключительно борьбой с терроризмом.

3.8. Информационная война как способ разрешения конфликтов в информационную эпоху

В одном из выступлений, прозвучавшем сразу после терактов в США, министр обороны Дональд Рамсфелд отметил, что в связи с совершенными 11 сентября в Нью-Йорке и Вашингтоне нападениями "мы наблюдаем появление нового поля боя... конфликтов иного типа". Далее он отметил, что в ближайшем будущем Америке предстоит решить две важные задачи: одержать победу в борьбе с терроризмом путем ликвидации сети террористических организаций, а также осуществить подготовку к совершенно другой войне - войне, которая будет разительно отличаться не только от войн прошлого столетия, но и от той новой войны с терроризмом, которую США ведет в настоящее время.

Так что же это за вторая война, к которой призывает готовиться американский министр обороны, в преддверии которой война с терроризмом – только учения? Какие цели она будет преследовать? Кто противник?

К лету 2001 года американская экономика оказалась в тяжелейшем кризисе. Об этом свидетельствовало неуклонное падение практически всех возможных биржевых индексов, характеризующих состояние экономики. В силу невозможности быстро перестроиться вместе с изменившейся после развала СССР и Варшавского договора военно-политической обстановкой американские вооруженные силы вынуждены поддерживать многие виды военной техники, оставшейся еще со времен «холодной войны». Это и

стратегические бомбардировщики B-52, и винтовка M16, и вертолеты AH-64 и многие другие образцы военной техники. Огромные вооруженные силы, оснащенные высокотехнологичными системами вооружения, стали серьезно тяготить американских налогоплательщиков. Это привело к тому, что США со временем могли повторить судьбу СССР, не реализовав во время программу модернизации своих вооруженных сил.

15 августа 2001 года на одном из мероприятий в городе Альбукерке президент Буш объявил о том, что предложил министру обороны Дональду Рамсфелду подготовить стратегическое представление о том, как американская армия "должна выглядеть сегодня и как она должна выглядеть завтра, чтобы сохранить мир; как в настоящий момент нам оставаться сильными и быть начеку; и, что столь же важно, как нам использовать технологии, чтобы сформировать войска, которые труднее будет обнаружить, которые будет обладать большей поражающей силой при ведении боевых действий, будут мобильнее и примут на вооружение новые технологии, чтобы мы не тратили даром деньги налогоплательщиков, когда речь идет о создании оружейных систем будущего".

Контуры новой стратегии были обозначены Рамсфелдом в статье «За рамками войны с террором», опубликованной в газете «Вашингтон пост» в октябре 2001 года. Он отмечает, что в свете последних событий в США подготовка к внезапному нападению - подготовка быстрая и решительная - должна стать одним из слагаемых военного планирования в 21 веке. Для того, чтобы отражать внезапные удары, военные стратеги США должны перенести центр тяжести в системе оборонного планирования с модели, отправным моментом которой является угроза и которая до сих пор доминировала в теории обороны, на модель, опирающуюся на силы и средства, необходимые в будущем. Вместо того, чтобы концентрировать внимание на том, кто именно окажется очередным противником, или где может произойти война, вооруженные силы США должны сосредоточиться на методах действий возможного противника - и, соответственно, развивать новые возможности для его сдерживания и поражения. Вместо того, чтобы планировать крупномасштабные войны на точно определенных театрах предполагаемых военных действий, считает Д. Рамсфелд, необходимо предвидеть появление новых и разнообразных противников, которые будут

полагаться на фактор внезапности, обмана и на применение ассиметричного оружия (согласно определению Института национальных стратегических исследований Национального университета обороны США, под "асимметричными" угрозами понимаются "использование фактора неожиданности во всех его оперативных и стратегических измерениях, а также использование оружия такими способами, которые не планируются США") для достижения своих целей.

Как заявил Д. Рамсфелд, подготовка к такому развитию событий стала целью проводящегося раз в четыре года анализа состояния и перспектив развития обороны, результаты которого были 30 сентября представлены Конгрессу США. В этом анализе изложена новая стратегия обороны США в XXI веке, призванная реализовать четыре ключевые задачи: заверить союзников в незыблемости поставленных целей и способности выполнять обязательства в сфере безопасности; разубедить потенциальных противников в целесообразности проведения программ или мероприятий, которые могут создавать угрозу интересам США или интересам союзников; обеспечить сдерживание агрессии и силового давления за счет передового развертывания сил и средств, способных быстро остановить разрастание кризиса, а также предпринимать решительные действия по нейтрализации любого противника в том случае, если методы убеждения и сдерживания окажутся неэффективными.

Для достижения поставленных целей США должны сохранить существующее военное преимущество на ключевых направлениях и разработать новые способы лишения противников преимуществ, которые они пытаются получить, применяя ассиметричные варианты действий.

В точном соответствии с речью Д. Рамсфелда операция американских войск в Афганистане во многом является полигоном испытания принципиально новой оперативной концепции ведения противоборства, известной из зарубежных источников как «сетевая война» (network-centric warfare).

Об активизации работ Министерством обороны США в этом направлении говорит тот факт, что за последние годы резко возрос интерес к реализации проекта создания глобальной информационной сети

Минобороны, известном как проект Defense Information Grid, который координируется Агентством информационных систем Минобороны (DISA). Глобальная информационная сеть Министерства обороны – основа ведения «сетевой войны».

Еще 27 августа 2001 года новый помощник министра обороны США по вопросам командования, управления, коммуникациям и разведки Дж. Стенбит в одном из интервью вновь акцентировал внимание на насущной необходимости развития концепции «сетевой войны». При этом продвижение данной концепции он назвал ключевым приоритетом деятельности на своем посту.

С сентября по октябрь 2001 года тематика «сетевой войны» так или иначе обсуждалась практически на всех конференциях и семинарах, проходивших с привлечением специалистов Министерства обороны США.

Наряду с этим, только за несколько последних лет анализу различных аспектов этой оперативной концепции был посвящен ряд исследований ведущих аналитических центров министерства обороны США.

По мнению ряда американских военных экспертов, новый взгляд на угрозы XXI века заключается в том, что в будущем основная угроза будет исходить не от регулярных армий разных стран, а от всевозможных террористических, криминальных и др. организаций, в том числе негосударственных, участники которых объединены в некие сетевые структуры. Подобные организации не имеют четкой иерархической структуры подчиненности, зачастую не имеют единого руководства, координируют свою деятельность с использованием средств глобальных коммуникаций. Отличительной особенностью таких структур является наличие единой стратегической цели и отсутствие четкого планирования на тактическом уровне. Для обозначения подобных структур появился специальный термин «сегментированная, полицентрическая, идеологизированная сеть» (Segmented, Polycentric, Ideologically integrated Network, SPIN).

В условиях воздействия подобных угроз изменяются роль и место вооруженных сил. В большей степени акцент делается на проведение

невоенных операций (Operation Other Then War), что требует тесного взаимодействия с негосударственными организациями и структурами.

Для организации деятельности вооруженных сил в условиях воздействия новых угроз и разработана концепция сетевой войны. По мнению ее авторов, сетевое противоборство или сетевая война (Network-Centric Warfare) является лучшим термином, предложенным к настоящему времени для описания пути организации и ведения противоборства в информационную эпоху. Как отмечает один из высокопоставленных офицеров ВМС США, это «принципиально отличное от традиционной войны, ориентированной на те или иные системы вооружения (танки, самолеты и др.) понятие, затрагивающее саму суть оперативного искусства».

Авторы определяют NCW, как оперативную концепцию, базирующуюся на информационном превосходстве и позволяющую достичь увеличения боевой мощи войск путем ориентации на сеть датчиков, штабов и исполнительных подразделений. Это дает возможность достичь широкой осведомленности, увеличить скорость доведения приказов, более высокого темпа проведения операции, большего поражающего действия, большей живучести и степени самосинхронизации. В сущности, NCW переводит информационное превосходство в боевую мощь, эффективно связывая интеллектуальные объекты в единое информационное пространство театра военных действий.

Основная задача разработчиков данной концепции – предложить военному руководству теоретическую и оперативную базу для организации противодействия в новых условиях.

В основу концепции положен опыт боевых действий, полученный армией США за время участия в конфликтах. Прежде всего – это война с партизанами во Вьетнаме, в Сомали, в Боснии, а также обобщение опыта боевых действий советской и российской армии в Афганистане и Чечне.

Ключевыми особенностями является трансформация понятия поле боя (battlefield) в понятие боевого пространства (battlespace) в которое помимо традиционных целей для поражения обычными видами вооружений включены также и цели, лежащие в виртуальной сфере: эмоции, восприятие и психика противника.

Воздействие на новые классы целей достигается за счет тесной интеграции сетевых структур Министерства обороны и сетевых структур гражданского общества (как совокупности общественных объединений, отвечающих за выработку «общественного мнения»).

Есть несколько ключевых понятий определяющих основные отличия «сетевой войны» от войны традиционной. Первое такое понятие заключается в использовании географически распределенной силы. Как указывают эксперты, ранее в силу разного рода ограничений было необходимо, чтобы подразделения и элементы тылового обеспечения располагались в одном районе в непосредственной близости к противнику или к обороняемому объекту. Новая концепция снимает эти ограничения.

Второе ключевое понятие состоит в том, что силы, участвующие в "сетевой войне" высокоинтеллектуальны. Пользуясь знаниями, полученными от всеохватывающего наблюдения за боевым пространством и расширенного понимания намерений командования, эти силы будут способны к самосинхронизации деятельности, будут более эффективными при автономных действиях.

Третье ключевое понятие - наличие эффективных коммуникаций между объектами в боевом пространстве. Это дает возможность географически распределенным объектам проводит совместные действия, а также динамически распределять ответственность и весь объем работы, чтобы приспособиться к ситуации.

Как отмечалось выше, основой новой концепции является информационная сеть (The Grid). При этом данная сеть состоит из трех подсетей: подсеть датчиков (сенсоров), подсеть узлов, принимающих решения, и подсеть исполнительных узлов.

Все три подсети включают узлы, работающие как с реальными, так и с виртуальными объектами. Так в сенсорной подсети сами датчики могут быть пассивными и активными, а располагаться могут как в реальной, так и в виртуальной сфере боевого пространства. Это же касается и подсети исполнительных узлов. В нее включены как традиционные средства поражения (танки, самолеты, корабли и др.) так и средства воздействия на

цели в виртуальном пространстве: средства массовой информации, компьютерные вирусы и др.

Американским военным не дают покоя результаты собственных прогнозов, согласно которым в сложившихся условиях после 2015 года военный потенциал Китая будет сравним с военным потенциалом США, а в дальнейшем начнется опережение Китаем США в экономическом и военном развитии.

Исследования и анализ подходов к ведению боевых действий Народной армией КНР, а также роли и места революционных процессов, протекающих в военной сфере, вызванных интенсификацией процессов информатизации; анализ концепции «народной войны» (прежде всего в ее приложении к информационной сфере) вынудил американских военных пойти на те кардинальные изменения, которые мы сегодня наблюдаем. Именно тот факт, что сама природа китайского общества, феномен мировой китайской диаспоры, имеют структуру все той же сети, и вызвал к жизни активизацию процессов внедрения концепции «сетевой войны».

Задолго до событий в США глава Центрального командования вооруженных сил США, генерал Томми Р. Фрэнкс совершил вояж по ряду стран Центральной Азии, включая Казахстан, Узбекистан, Таджикистан, Киргизию, и Туркменистан. Возможная цель визита состояла в зондировании обстановки на случай развертывания американских войск в этом регионе. Та поспешность, с которой правительства большинства стран региона приняли решение о допуске американских войск на свою территорию с началом операции в Афганистане говорит о том, что, возможно, принципиальная договоренность по этому поводу была достигнута ранее.

В ходе состоявшейся 18 мая 2001 года в Ташкенте пресс-конференции, на вопрос журналистов о том, что, по мнению ряда экспертов, оценка террористической угрозы в Центральной Азии весьма преувеличена, Томми Р. Фрэнкс заявил, что не считает преувеличенной угрозу террористических актов в Центральной Азии и надо готовиться к ее нейтрализации уже сейчас.

Расширяя свое военное присутствие в Центральной Азии, американские военные уже создали в Узбекистане два училища для подготовки

сержантского состава узбекской армии. В 2001 году подразделения американских сил особого назначения провели здесь ряд совместных учений с подразделениями узбекских вооруженных сил. Бюджет военного сотрудничества только с Узбекистаном на 2001 год составил более трех миллионов долларов США.

Рисунок 20 Головная часть противоракеты - основа американской ПРО

С началом операции в Афганистане и развертыванием американских сил в республиках Центральной Азии резко возросло информационное воздействие на население этих стран. Так с 3 декабря 2001 года радио «Свободная Европа» и «Радио Свобода» увеличили объем своего вещания на азербайджанском, фарси и туркменском языках в контексте общего расширения присутствия этих станций в эфире Центральной Азии. В течение января-февраля 2002 года планируется еще большее расширение вещания на азербайджанском, фарси, казахском, киргизском, таджикском, туркменском и узбекском языках в общей сложности на двадцать часов, а также расширение вещания на арабском языке через радио «Свободный Ирак».

Еще 11 декабря прошлого года, когда военная фаза операции в Афганистане была в самом разгаре, в Нью-Йорке еще не разобрали руины, а в головах многих еще были свежи провозглашенные Администрацией США лозунги о борьбе с терроризмом, информационное агентство «Росбизнесконсалтинг» со ссылкой на пакистанскую газету Frontier Post сообщило, что Соединенные Штаты Америки уже планируют развернуть на юге Афганистана элементы НПРО для перехвата китайских баллистических ракет.

Со ссылкой на «хорошо осведомленные источники в дипломатических кругах» пакистанская газета отмечает, что приход американских сил в Центральную Азию преследовал несколько целей (а, возможно, всего лишь одну – закрепиться в регионе). США стремятся закрепиться в Афганистане, чтобы взять под свой контроль поток природных ресурсов из азиатских стран, проходящий через афганскую территорию. Не менее важной целью для Вашингтона является сдерживание роста экономического и военного могущества Китая.

Рисунок 21 Старт ракеты-перехватчика

Далее, уже в январе 2002 года агентство «Росбизнесконсалтинг» со ссылкой на испанскую газету El Pais пишет, что Соединенные Штаты намерены сохранить свое военное присутствие в Средней Азии и после окончания военной кампании в Афганистане. Ссылаясь на источники в Пентагоне, испанская газета отмечает, что Вашингтон уже начал строить в Киргизии военно-воздушную базу, которая станет транспортным центром и будет способна вместить около 3 тысяч солдат, а также многочисленные самолеты и оборудование.

Американские инженеры завершают также подготовку к строительству военных баз в Узбекистане и Афганистане. Как отмечают журналисты, представитель Центрального командования ВС США контр-адмирал Крейг Куигли полагает, что создание военных баз вокруг Афганистана имеет «большое значение» для Соединенных Штатов, поскольку позволит осуществлять целый ряд задач в краткосрочной и долгосрочной перспективе.

Кроме того, в настоящее время Франция ведет переговоры с таджикскими властями о строительстве в Айни военного аэродрома, который будет предоставлен к услугам НАТО. El Pais пишет, что усиление военного присутствия США и НАТО в Средней Азии, очевидно, не может не беспокоить Кремль. Сегодня Москва стоит перед реальной угрозой того, что весьма скоро Североатлантический альянс окажется не только у западных границ России, но также и «на ее заднем дворе» - в среднеазиатских республиках, куда США и НАТО пустили лишь на время проведения антитеррористической кампании, отмечает издание.

В развитие обстановки в регионе 10 января 2002 года представитель Министерства иностранных дел Китая Сан Юкси назвал «не имеющим оснований» опубликованный ЦРУ США прогноз о перспективах развития китайских ядерных вооружений к 2015 году. По заявлению МИД КНР, Китай будет усиливать свою национальную оборону «в соответствии со своими нуждами», и любые прогнозы в связи с этим представляют собой лишь ничем не подкрепленные умозаключения.

В опубликованном 9 января 2002 года докладе Центрального разведывательного управления под названием «Развитие иностранных ядерных ракет и ядерная угроза на период до 2015 года», в частности, говорится, что через 14 лет Китай будет иметь от 75 до 100 ядерных ракет дальнего радиуса действия, что вчетверо превышает сегодняшний ядерный потенциал Китая. Также, по мнению аналитиков ЦРУ, большинство китайских межконтинентальных ракет будет располагаться на мобильных платформах.

Как и ряд других изданий, британская пресса высказывает мнение о том, что американское военное строительство на территории бывших советских республик в Средней Азии вызывает растущее недовольство в Пекине. Так, британская газета Guardian сообщает, что из пяти бывших советских республик в Центральной Азии только Туркмения до сих пор не допустила на свою территорию американские войска. Вместе с тем, «поспешное строительство американских баз может вызвать раздражение у Пекина, так как новая американская база в Киргизии будет находиться почти на восточной границе этого государства с Китаем. Учитывая американские базы в Японии и в Южной Корее, а также поддержку, оказываемую Соединенными Штатами Тайваню, КНР может почувствовать себя в окружении».

По мнению ряда российских экспертов, возможное развертывание американских военных баз в Узбекистане, в других азиатских бывших советских республиках, в северных провинциях Афганистана может снять необходимость создания НПРО США. Высокоточные ракеты средней дальности (до 3 тыс. км) с территории этих баз перекрывают всю российскую территорию до Северного Ледовитого океана. В зону поражения попадают все пусковые установки российских стратегических ракет.

Таким образом, в начале третьего тысячелетия человечество стоит на пороге новой мировой войны. Хотя многие отмечают, что эта война уже идет. Нежелание США признать саму возможность наличия альтернативной им силы ведет к резкому обострению ситуации во всех регионах страны. Сегодня, по словам некоторых американских политиков, цитата из речи Буша «кто не с нами – тот против нас», стала стандартом новых международных отношений.

В условиях, когда американская экономика находится в глубоком кризисе, Администрация США стремится предпринять ряд шагов, дабы помешать возможному стратегическому партнерству России и Китая. С этой целью в сердце Евразийского континента вонзается нож американских военных баз.

3.9. О работах в области информационной войны в Великобритании, Франции, Германии, КНР

Более полувека назад, на заре информационной эпохи, когда была обнаружена восприимчивость человеческой психики к внушению, информация в форме пропаганды стала важнейшим средством управления широкими массами людей. С течением времени она постепенно заменила собой грубую силу и насилие, которые долгое время считались единственным и непременным средством управления народами. В западной прессе появился даже термин «мягкая сила», отражающий потенциал идеологии и пропаганды.

Процессы глобализации, протекающие в современном мире, накладывают свой отпечаток на путях разрешения конфликтов в XXI веке.

Применение современного информационного оружия отражает историческую тенденцию перехода от войн с истреблением противника к войнам, ориентированным на деморализацию противника без его уничтожения. Характерно, что еще Ричард Никсон в одном из выступлений перед Конгрессом США заявил, что ***он считает 1 доллар, вложенный в информацию и пропаганду, более ценным, чем 10 долларов, вложенных в создание систем оружия, ибо последнее вряд ли будет когда-либо употреблено в дело, в то время как информация работает ежечасно и повсеместно***.

Сегодня стало вполне очевидным, что, несмотря на неопределенность встающих угроз и проблем XXI века, США намерены и в будущем сохранить роль лидера в усложняющемся и все более глобализирующемся мире. Для этого они ориентируются на опережающее формирование адекватной их интересам стратегической среды, а в случае неуспеха - на готовность к силовой нейтрализации неблагоприятных для США процессов.

В этой связи примечателен следующий факт. Еще в августе 1997 года ЦРУ провело брифинг по вопросам развития Каспийского региона, как одного из наиболее богатого нефтяными и газовыми ресурсами. Для наблюдения за развитием политических событий в регионе и оценки его потенциала ЦРУ создало специальное подразделение. После доклада представителя ЦРУ, присутствовавшая на брифинге госсекретарь США Мадлен Олбрайт заявила, что «одной из самых важных задач … будет работа над ***формированием будущего*** этого региона». Это и есть ключ к пониманию проблемы информационного противоборства: ***создание всеми средствами необходимой, отвечающей национальным интересам США, политической атмосферы в тех регионах, которые входят в сферу интересов США***.

Проведение этой политики доказывает справедливость тезиса о том, что именно лидерство в сфере приоритетных знаний, информатике, технологиях и повседневному влиянию на жизнь миллионов людей во всем мире через потребляемые ими продукты, товары, услуги, культуру и будет определять в будущем статус «великой державы»

События 11 сентября 2001 года в США резко осложнили проведение работ по установлению международного контроля за процессами создания и применения информационного оружия.

Только за первый месяц после терактов в США в разных странах Запада под эгидой борьбы с международным терроризмом был принят ряд законодательных актов расширяющих возможности и права специальных служб по использованию различных средств, которые по ряду характеристик могут быть отнесены к средствам ведения информационной войны (прежде всего, системы типа Carnivore, о чем говорилось выше). Сам факт использования панического состояния населения и парламентов этих стран в интересах расширения влияния специальных служб может быть расценен как акт информационно-психологического давления.

Чего стоят введение в международный обиход таких понятий как «ось зла», «страна-изгой» или «международный терроризм». Ни одно из них не подкреплено юридическими нормами.

Никто не знает принципа, по которому формировался знаменитый «список Буша», включающий организации, якобы поддерживающие международный терроризм.

Однако это не мешает творить правосудие. Только по подозрению или доносу закрываются фирмы, арестовываются счета, уничтожаются интернет-сайты. Так в список компаний, поддерживающих террористов, попал национальный провайдер услуг доступа в Интернет Сомали. Этого хватило для того, чтобы отключить целую страну от международных коммуникаций, поскольку коммутаторы базовых сетей связи оказались принадлежащими British Telecom.

Следует отметить, что терроризм – продукт информационной эпохи. Вне средств массовых коммуникаций и массовой информации, распространяющих требования террористов, сами теракты теряют всякий смысл. Можно рассматривать теракты как инициаторы информационных операций в ходе широкомасштабной информационной войны. Они позволяют нужным образом подготовить восприятие широких масс, а в дальнейшем поддерживать состояние страха, способствующее манипуляции сознанием общества, что и является целью террористов. Примером могут служить последние американские события.

Так сам теракт в США и его классная профессиональная подача операторами CNN использовался для изменения состояния сознания американской нации. Однако менталитет и пацифистский характер психики американцев не позволяет проводить достаточно длительных операций, неизбежно нарастает протест против любого неоправданного насилия. В этом случае используется катализатор, поддерживающий измененное состояние сознания – информационный вброс по поводу бактериологической атаки террористов. Однако очевидно, что преодолеть эпидемиологический порог неконтролируемого распространения выбранной инфекции в современных условиях невозможно, но достигается необходимая пролонгация требуемого психологического состояния.

Более того, и это становится уже очевидным, масштабность, четкая координация действий и подготовка современных террористов вышли за рамки возможностей отдельных террористов-одиночек и даже ряда

террористических организаций недавнего прошлого. Сегодня цели террористов глобальны и затрагивают интересы не отдельных государств, а мира в целом. Современный терроризм – один из продуктов глобализации. Проведение терактов такого масштаба требует не только отличной подготовки исполнителей, но и широкомасштабного обеспечения проведения таких операций, прежде всего – информационного. Для охвата возможно большей аудитории необходимо привлечение глобальных телекоммуникационных компаний, мгновенно разносящих весть о теракте, и доносящих ее в каждый дом, каждую семью. Безусловно, такие действия невозможны без заинтересованности транснациональных корпораций. Сегодня терроризм – средство изменения состояния сознания широких масс для последующего манипулирования в интересах транснациональных корпораций. Налицо становление нового способа разрешения конфликтов информационной эпохи: для достижения поставленной цели сегодня нет необходимости разжигать региональный конфликт, достаточно провести теракт и грамотно его осветить в СМИ, а далее, используя измененное в результате стресса и страха сознание общества провести информационную операцию по манипулированию сознанием. Более того, используя принцип «реальной виртуальности» (когда освещение события важнее его самого) возможно и не проводить сам теракт, либо провести его в незначительных масштабах, а все остальное доработать в процессе его освещения в СМИ. Примером использования этого приема могут служить действия США в Афганистане, когда нет объективной информации о происходящих событиях, зритель не знает, куда именно попали бомбы, но доверяет сообщениям СМИ и верит в объективность подачи информации. Все больше современный конфликт приобретает черты некоего театра, театра абсурда. Как это ни странно, но в начале XXI века театр, уйдя со сцены, вошел в жизнь общества как главное средство управления восприятием. Об этом очень хорошо сказано в книге Сергея Кара-Мурзы «Манипулирование сознанием».

Сегодня, несмотря на законодательно провозглашенную и активно декларируемую в западном мире «свободу слова», вопросам использования информационных средств и технологий для достижения политических целей уделяется самое пристальное внимание.

Так, «свобода слова» в США опирается на так называемую Первую Поправку к Конституции и гарантируется в соответствующих законах всех штатов страны. Однако, декларируя идею «свободы информации», органы государственной власти США подразумевают под ней свободное распространение такой информации, которая способствует реализации и защите их национальных интересов, достижению поставленных целей, существенно регламентируют ее содержание.

Еще в 1934 г. Конгрессом США был создан орган надзора над радио- и телевещанием - Федеральная комиссия по связи (FCC, ФКС). И хотя это произошло еще до того, как телевидение стало средством массовой информации, законодательство с тех пор существенно не менялось. Закон наделил ФСК не только контрольными, но и нормотворческими функциями, правом выдачи лицензий и др. В частности, именно ФКС установила, что иностранные корпорации не могут быть держателями более 25% акций, дающих их владельцу права голоса при проведении любой радио- или телевещательной сделки в США.

Примечательно, что соотношение реальной и декларируемой свободы информации в западных странах позволило одному из американских специалистов отнести свободу СМИ к одному из пяти основных мифов, утверждающих господство правящей элиты[77].

Рассматривая органы формирования и реализации информационной политики западных государств, следует выделить два уровня: уровень формирования и уровень реализации.

К примеру, в США вопросы формирования информационной политики государства находятся в ведении Совета национальной безопасности (СНБ) страны. Как отмечается в работах ряда экспертов, после окончания «холодной войны» СНБ США стал уделять больше внимания невоенным, в том числе и информационным, способам достижения военно-политических целей[78]. Непосредственно при президенте США с 1996 года функционирует консультативный орган по вопросам информационной войны. В его работе принимают участие советники и помощники президента по вопросам

---

[77] Шиллер Г. Манипуляторы сознанием (пер. с англ.) - М.: 1980. С. 25-40.
[78] Писарев В.Д., Хозин Г.С. Механизм выработки внешнеполитических решений //США: экономика, политика, идеология. - 1996. - №1. С. 28-29

национальной безопасности, государственный секретарь, главы ключевых министерств (финансов, энергетики и торговли), директор ФБР, председатель Комитета начальников штабов, другие лица.

В Германии базовой структурой формирования информационной политики государства является Федеральное ведомство печати и информации, имеющее статус высшего федерального ведомства. Его статс-секретарь принимает участие в заседаниях кабинета министров.

Рассматривая уровень реализации информационной политики США и западных государств необходимо отметить, что отличительной чертой здесь является активное личное участие в ней первых лиц государства[79]. Непосредственное осуществление задач информационно-психологического воздействия, как правило, возлагается на аппарат психологической войны, включающий специальные формирования психологических операций. Он имеет модульный (причем, непостоянный) характер и ориентирован на решение конкретных задач в случае возникновения кризисных ситуаций в тех или иных регионах мира.

Для координации усилий по использованию информационных средств и технологий в период конфликта и организации взаимодействия командования оперативного и стратегического звена с представителями СМИ могут создаваться специальные органы: Межведомственный координационный комитет по общественной дипломатии («Буря в пустыне»), Группа информационного обеспечения (Гаити), Центр операций в СМИ в штаб-квартире НАТО (Косово), Информационный центр в штаб-квартире коалиционных сил в столице Катара Дохе, а также Управление стратегического влияния (Ирак) и др. Ими разрабатываются соответствующие планы, готовятся пропагандистские материалы, проводятся целенаправленные мероприятия по дезинформации общественного мнения и дискредитации неугодных лидеров, распространяются слухи и т.п.

В последнее время, в соответствии с введенной в действие в октябре 1998 года «Доктриной информационных операций ВС США»,

---

[79] Николаев Д. США готовы нанести удар по Ираку.// Независимое военное обозрение. 2002. № 10.

психологические операции рассматриваются американскими специалистами как действия по доведению определенной информации до иностранных аудиторий. При этом психологические операции могут осуществляться в рамках программ связи с общественностью (Public Affairs), предусматривающей доведение «точной и своевременной информации» до американских аудиторий и личного состава ВС США, а также до иностранной общественности, содержания целей и задач военных компаний и операций, информирование заинтересованных аудиторий о касающихся их важнейших изменениях, обеспечение возможности командованию посредством СМИ довести до потенциально противника сведений о намерениях и возможностях вооруженных сил США и их союзников. Кроме того, в интересах психологических операций осуществляются программы по работе с гражданским населением, трактующиеся как действия командиров по установлению и поддержанию отношений между подчиненными им войсками и гражданскими властями, организациями и местным населением в дружественных, нейтральных и враждебных районах развертывания формирований ВС США.

В ряде публикаций отмечается, что в настоящее время в ведущих зарубежных государствах созданы или создаются специальные структуры по работе с общественностью. Так, в соответствии с директивой министра обороны США № 5122.5 его помощник по связям с общественностью несет основную ответственность за разработку и реализацию информационной политики министерства обороны; осуществляет координацию вопросов информационной политики с председателем комитета начальников штабов, руководством министерств видов вооруженных сил и главнокомандующими объединенными командованиями ВС; определяет круг должностных лиц, имеющих официальное право принимать решение о передаче в СМИ тех или иных данных о деятельности ВС и др.

Рассматривая средства реализации информационной политики США и западных государств, необходимо в первую очередь отметить новостные информационные агентства. Строго говоря, сами они, как правило, не занимаются передачей информации непосредственно ее конечным потребителям - читателям, слушателям, зрителям, а собирают информацию, обрабатывают ее и передают органам массовой информации.

На сегодняшний день информационные агентства являются главными инструментами оперативного сбора и передачи информации внутри стран и между ними.

Так, под непосредственным руководством Совета национальной безопасности США функционирует Информационное агентство Соединенных Штатов (USIA, ЮСИА), директор которого одновременно является главным советником президента страны по вопросам информации. Располагая штатом около 10 тыс. человек и выпуская информационные программы на 62 языках мира, ЮСИА имеет более 200 своих отделений в 120 странах мира!

Более 2 тысяч сотрудников французского агентства Франс Пресс (АПФ) работают в 13 отделениях во Франции и в 163 отделениях в различных регионах мира.

Занимающее ведущее место на немецком информационном рынке германское агентство печати ДПА имеет свои бюро и корпункты в 80 странах, причем половину расходов на их содержание берет на себя федеральное правительство.

Учитывая вышесказанное можно сделать вывод о том, что в настоящее время мировые державы благодаря наличию соответствующей правовой базы, органов и средств формирования и реализации информационной политики, располагают широкими и разнообразными возможностями для достижения своих политических и военных целей, защиты государственных интересов посредством влияния на общественное сознание как внутри страны, так и за рубежом. «Мы не побеждаем, пока Си-эн-эн не говорит, что мы побеждаем»[80]. Эта фраза, принадлежащая американскому генералу Джону Шаликашвили - председателю комитета начальников штабов США в период кризиса на Гаити в 1994 г. - наглядно отражает отношение высшего военного руководства США и западных государств в целом к использованию информационных ресурсов в решении задач современных войн и вооруженных конфликтов.

---

[80] Михайлов Б. Армия и пресса: не противники, а союзники. //Красная звезда. 25 июля 1996 г.

Лет пять назад Центральное разведывательное управление США упоминало только Россию и Китай в качестве основных источников угрозы из киберпространства для Америки. Сегодня американские военные эксперты отмечают, что уже более 20 стран планируют и осуществляют различные виды информационных операций, направленных против Соединенных Штатов.

Оценка угрозы, проведенная Военно-морским флотом США, выделяет Россию, Китай, Индию и Кубу в качестве стран, которые открыто подтвердили политику подготовки к информационной войне, и которые быстро развивают свои способности в этом направлении. Северная Корея, Ливия, Иран, Ирак и Сирия по сообщениям имеют потенциал и серьезное желание к продвижению в этом направлении, а Франция, Япония и Германия уже весьма активны в этой области.

Как же видят в разных государствах основные подходы к ведению информационной войны?

3.9.1. НАТО в целом

Согласно руководящим документам НАТО, принятым в 1999 году, информационные операции определяются как «действия, предпринимаемые с целью оказания влияния на принятие решений в поддержку собственных политических и военных целей, путем воздействия на информацию, информационные процессы и системы командования и управления противника, при одновременной защите собственной информации и информационных систем». Подобно американскому подходу, в определении НАТО также введены понятия оборонительных и наступательных информационных операций.

Вместе с тем, на проведенной объединенным штабом НАТО в начале 2000 года конференции по проблемам информационной войны все участники пользовались определениями, разработанными в их странах.

3.9.2. Великобритания

Британское представление об информационной войне во многом подобно таковому в Соединенных Штатах. Оно определяет информационную войну как действия по оказанию влияния на

информационные системы противника, при одновременной защите собственных информационных систем. «Свобода слова» в Великобритании регулируется, по крайней мере, десятком законов и множеством подзаконных актов. В настоящее время там действует более десяти государственных и независимых учреждений и организаций, занимающихся регулированием в сфере массовой информации. В Великобритании основные направления государственной информационной политики разрабатывает Британский совет совместно с Центральным бюро информации. Совет находится в непосредственном подчинении МИД Великобритании.

Организация связи с общественностью в структуре министерства обороны Великобритании возложена на аппарат пресс-секретаря – начальника службы информации Минобороны. Руководитель этой службы (гражданское лицо) имеет ранг государственного чиновника. Кроме того, в Великобритании в 2000 году введен в действие комплекс законодательных актов, который в значительной степени может применяться к расследованию преступлений в киберпространстве – Regulation of Investigatory Powers Act (RIP). Он предполагает, что нападения на информационные системы могут рассматриваться как обычное уголовное преступление со всеми вытекающими последствиями. Данный акт позволяет британскому правительству перехватывать и читать электронную почту, а также требовать расшифровки личных файлов по требованию государственных чиновников.

3.9.3. Германия

Главным образом немецкое представление информационной войны совпадает с таковым в США и Великобритании. Оно включает ведение наступательной и оборонительной информационной войны для достижения целей национальной политики. Вместе с тем ФРГ имеет тенденцию оставаться более системной в подходах к обеспечению информационной безопасности, чем Соединенные Штаты, что вообще свойственно немецкой педантичности.

При определении угроз и возможных ответов, иностранные государства рассматриваются отдельно от негосударственных организаций (типа политических партий, международных организаций и средств массовой информации). Также отдельно выделяются преступные сообщества

(организованные преступные группы, хакеры и т.д.), и отдельные индивидуумы (религиозные фанатики и др.).

В двух случаях, однако, немецкое представление об информационной войне отличается от американского. ФРГ рассматривает управление средствами массовой информации как элемент информационной войны. Кроме того, Германия отдельно вводит определение для экономической информационной войны, подобно французам (см. ниже). Такой подход является следствием двух причин: Германия оценила потенциал возможного экономического ущерба, который может быть нанесен немецкому бизнесу и экономике; Германия, возможно, испытала существенные экономические потери от Франции в операциях индустриального шпионаж в киберпространстве; также Германия может искать пути смягчения последствий потенциальных вторжений.

В ФРГ система органов связи с общественностью бундесвера предназначена для освещения в СМИ вопросов военной политики, взглядов руководства ФРГ и НАТО на перспективы строительства и развития вооруженных сил, ведения информационно-пропагандистской работы с общественными и молодежными организациями, а также для изучения общественного мнения по вопросам военного строительства.

3.9.4. Франция

Французские военные эксперты рассматривают концепцию информационной войны, состоящую из двух главных элементов: военной и экономической (или гражданской). Военная концепция предполагает несколько ограниченную роль информационных операций. Военная концепция определяет место информационным действиям в основном в контексте конфликтов малой интенсивности или в миротворческих операциях. В этом контексте, союзники не рассматриваются как противники.

Напротив, экономическая или гражданская концепция включает более широкий диапазон потенциального применения информационных операций. Французское представление принимает намного более широкое и более глубокое представление для конфликта в экономической сфере. В этом случае французы не видят себя связанными рамками НАТО, ООН или согласием США на проведение операций. Такой подход к экономическому

конфликту учитывает возможность быть и союзником, и противником одновременно.

В вооруженных силах Франции вопросами взаимодействия с общественностью занимается служба информации и общественных связей (SIRPA). Современная структура службы определена в 1990 г., одновременно были уточнены и значительно расширены ее задачи и функции. SIRPA находится в непосредственном подчинении министра обороны, возглавляется бригадным генералом.

Франция активно формирует структуры по контролю за своими гражданами в киберпространстве. В ряде средств массовой информации отмечалось, что французы создали собственную версию системы «Эшелон» (по сообщениям американской прессы система направлена на перехват фактически всех частных глобальных коммуникаций). «Frenchelon», так некоторые назвали эту систему, по сообщениям используется для контроля и анализа коммуникаций, особенно в районе Парижа.

В последнее время правительство Франции, изучив опыт работы арабских телеканалов по освещению агрессии против Ирака, приступило к формированию собственного новостного спутникового канала, предназначенного для организации вещания на ряд азиатских стран, в которых позиции Франции традиционно сильны.

3.9.5. Китайская народная республика

Китай уже давно включил термин «информационная война» в лексикон своих военных специалистов[81]. Сегодня он неуклонно движется к формированию единой доктрины информационной войны. Фактически, если революция в военном деле определяется как существенное изменение в технологии, дающее преимущество в военном обучении, организации, стратегии и тактике военных действий, то, возможно Китай из всех стран сегодня испытывает истинную революцию в киберпространстве.

Китайская концепция информационной войны включает уникальные сугубо китайские представления о войне вообще. Эти представления основаны на концепции «народной войны», стратегемах великого Сун Цзы, а

[81] Qiao Liang; Wang Xiangsui, Unrestricted Warfare. - PLA Literature and Arts Publishing House, Beijing, 1999

также местных представлениях о том, как воевать на стратегическом, оперативном и тактическом уровне. Многое из этого подхода делает акцент на обмане, войне знаний и поиске асимметричных преимуществ над противником. Информационная война определена как «переход от механизированной войны индустриального возраста к... войне решений и стиля управления, войне за знания и войне интеллекта».

Китай развивает концепцию «сетевых сил» (воинские подразделения численностью до батальона), которые будут состоять из высококлассных компьютерных экспертов, подготовленных в ряде множестве государственных университетов, академий и учебных центров. Предполагается, что основной акцент будет сделан на привлечение активной молодежи.

На сегодняшний момент было проведено уже несколько крупномасштабных учений этих сил по отработке концепции информационной войны.

По утверждению ряда американских экспертов[82, 83, 84], усилия Китая сегодня направлены, главным образом, на укрепление его экономического состояния, поддержания национального единства, значительного улучшения технологических и военных способностей, а также на увеличение регионального и глобального влияния.

Основным условием решения стоящих задач является минимальное или полностью отсутствующее явное и открытое противоборство, которое может привлечь внимание стран Запада к Китаю и региону в целом. По мнению американских специалистов, поставленная цель достигается реализацией уникальной формы информационной войны, эффективно использующей тактику обмана, маскировки и введения в заблуждение противника. Как утверждают американские эксперты, эта теория поддерживается различными источниками, которые имеют непосредственное отношение с Великой китайской стратегии и стратегическому наследию Китая и во многом ведет к пересмотру границ западного определения понятия информационной войны.

---

[82] Sobiesk Edward, Redefining the Role of Information Warfare in Chinese Strategy. - SANS Institute, 2003
[83] Yoshihara Toshi, Chinese information warfare: a phantom menace or emerging threat? - Strategic Studies Institute, U.S. Army War College, 2001
[84] Xiaoping Deng, The Military Power of the People’s Republic of China. - Office of the Secretary of Defense of the United States of America, 2002

Особо следует отметить, что подобная трактовка развития китайского подхода к информационной войне существенно отличается от результатов, которые высказывались американскими экспертами всего несколько лет назад. Так еще в 2001 году результат идентификации китайской доктрины информационной войны рассматривался ими как «разочаровывающе неуловимый». Однако существенное переосмысление произошло после опубликования книги китайских военных специалистов «Неограниченное противоборство» («Unrestricted Warfare»).

Ранее американские эксперты отмечали, что в открытой литературе китайские специалисты используют определения, практически полностью повторяющие американское видение информационной войны, а часто просто занимаются плагиатом. Однако, большая часть экспертов обращает внимание на то, что копирование действительно может иметь место, а большая часть дебатов в Китая по рассматриваемой проблеме могла быть организована с целью сокрытия реальных намерений и способностей Китая, что заставляет воспринимать ее как масштабную кампанию по дезинформации. Некоторые эксперты предупреждают, что Соединенные Штаты должны быть осторожны, чтобы всецело не полагать, будто Китай рассматривает информационную войну через призму открытых американских публикаций.

Как отмечается в ряде прогнозных исследований, выполненных за последние годы в аналитических центрах США, Китай становится главным экономическим и военным конкурентом Соединенных Штатов в наступившем столетии. Однако, несмотря на наличие такого серьезного противника, американское понимание стратегического наследия Китая, его Великой стратегии и роли информационной войны в поддержке этой стратегии, по мнению американских экспертов, серьезно недооценены. Существующий сегодня в США уровень развития приемов и методов анализа и прогнозирования не позволяет полностью постичь то сильное и глубокое воздействие, которое восточное стратегическое наследие имеет в действиях Китая.

Вместе с тем недостаток любой официальной информации, закрытость китайского общества, ряд существенных разрывов в китайских открытых публикациях в области информационной войны между теорией и практикой, продолжающиеся дебаты и отсутствие единого мнения по ряду вопросов, а

также уникальное влияние китайской стратегической традиции ставит перед американскими специалистами со стороны Китая все более и более непредсказуемые вызовы в информационном пространстве.

По мнению аналитиков сегодня американская военная доктрина, основанная на всеобъемлющем высокотехнологичном превосходстве, должна включать и совершенную оценку ситуации в различных областях, в первую очередь – в военной и информационной. Однако, как показали результаты ряда последних конфликтов, в которых приняли участие американские войска, США пренебрегают детальным изучением и осознанием стратегической культуры потенциальных противников. Классический пример: вьетнамская война. Она показала, что наличие технически превосходящей силы недостаточно для победы над противником. Необходимо помнить, что цель любой войны состоит, прежде всего, в сломе воли противника к сопротивлению. Сегодня это ключевой аспект информационной войны. Эксперты отмечают, что, учитывая складывающуюся военно-стратегическую обстановку, а также продолжающееся размывание границ между войной и миром, область информационной войны требует еще более внимательного изучения всех аспектов, связанных с выработкой и принятием решений противником, а главное – его стратегической концепции.

Исследуя стратегию действий Китая, а также роль и место в ней средств и методов информационной войны американские аналитики столкнулись с рядом фундаментальных отличий, корни которых лежат в культурном различии Западной и Восточной цивилизаций. По мнению специалистов наиболее рельефно отражают различия в менталитете народов древнейшие логические игры, получившие широкое распространение и признание на Востоке и на Западе: для Запада это шахматы, а для Востока - игра Го. Шахматы предполагают наличие полного комплекта фигур до начала поединка, в то время как партия Го начинается с чистого игрового поля. В процессе игры в шахматы силы противников убывают, пропорционально утрате отдельных фигур, вместо этого в Го силы одного из противников увеличиваются за счет установления контроля над фигурами другого противника. Чем больше длится партия в Го, тем чувствительнее становятся позиции противников к ошибкам, тем значительнее становятся

преимущества того, кто первый сможет воспользоваться ошибкой противника. Итог шахматной партии – разгром армии противника и гибель короля, при этом, как правило, серьезно страдает и собственная армия, итог же партии Го – установление контроля над большей частью территории игрового поля, причем сила победителя тем больше, чем была больше сила противника. Важным итогом этой аналогии является осознание сути восточной стратегии противоборства: в стратегии нужно стремиться к большему влиянию при минимальных затратах при этом не уничтожать противника и собственную нацию в бесконечной борьбе, а использовать ресурс и возможности противника для собственного роста.

Важным является также и то, что главной целью остается не победа над противником любой ценой, даже ценой его полного истребления, но, избегая непосредственных столкновений и стратегических перемещений сил, достижение господства, выживания и процветания собственного народа. Этот подход оставляет жизнеспособной нацию, позволяя ей доминировать над процветающим миром, а не над миром разрухи, негодования и бедности.

В качестве еще одного подтверждения культурных различий, американские эксперты отмечают следующее: Китай официально не опубликовал свою «великую стратегию», однако анализ различных источников позволил американским специалистам идентифицировать две стратегические цели Китая: развитие «всесторонней национальной мощь» и максимизация «стратегической конфигурации силы», названной китайскими специалистами «ши», с целью поддержания независимости и создания импульса для усиления национальной мощи.

Полная стратегия Китая остается закрытой от широкой публики, однако наибольший интерес, по мнению экспертов, представляет именно англоязычная интерпретация китайского «ши», так как в отношении этого термина отсутствует какой-либо западный эквивалент. Лингвисты трактуют его как «выравнивание сил», «склонность вещей» или «потенциал, рожденный диспозицией», который в руках высококлассных стратегов может гарантировать победу над превосходящей силой.

Осознание базовых принципов китайской стратегии позволяет американским аналитикам утверждать, что сегодня в Китае может

превалировать совсем иное представление о США как о глобальном противнике. Наиболее вероятно, что, базируясь на культурных различиях и «стратегии Го», Китай видит Соединенные Штаты как препятствие к достижению контроля и влияния в регионе и в мире в целом, однако победа Китая над этим противником не возможна без использования ресурса самого противника. Учитывая безусловные выгоды во взаимодействии с Соединенными Штатами - прежде всего в вопросах торговли и технологий – Пекин, очевидно, полагает, что Соединенные Штаты представляют существенный долгосрочный вызов. Руководство Китая утверждает, что Соединенные Штаты стремятся поддерживать доминирующее геостратегическое положение, сдерживая рост китайской мощи, и, в конечном счете, их стремление будет направлено на расчленение и «вестернизацию» Китая, одновременно не допуская возрождения России. Кроме этого Китай отрицательно относится к взаимоотношениям США с Японией и Тайванем.

В целом же аналитики предполагают, что в ближайшей перспективе Китай будет стремиться уменьшить влияние США в Азиатско-Тихоокеанском регионе, не предпринимая при этом резких конфронтационных действий с тем, чтобы не допустить открытого противостояния с превосходящими силами.

Между тем современная американская военная доктрина стремится к достижению информационного превосходства над противником путем массированного использования высоко-технологичных систем вооружения и военной техники, поддержанных разветвленной инфраструктурой командования, управления, систем связи и разведки, а также широким использованием высокоточного оружия для уничтожения ключевых целей. Основной задачей является при этом разрушение способностей противника по управлению войсками. Информационные действия ведутся американскими войсками в поддержку традиционного кинетического оружия. Основываясь на подобной доктрине, цель американских военачальников сегодня заключается в том, чтобы быть на несколько шагов впереди противника, находясь внутри его цикла принятия решений, обладая актуальной информацией и не допуская противника к пониманию характера действий своих войск, быстро наносить удары по противнику с

хирургической точностью. Однако, возвращаясь к аналогии шахмат и Го, американская военная доктрина сегодня, это только иной способ изложения еще одного варианта как победить в шахматах.

Основной вывод экспертов сводится к тому, что существующая сегодня в Китае концепция информационной войны не есть борьба в традиционном, западном смысле этого слова. Информационные действия Китая сегодня идут вне военной области, которая более традиционна для Запада. Они главным образом базируются на достижении благоприятного для Китая развития событий и их положительного исхода вместо наращивания мощи технических средств или использования текущей уязвимости американской инфраструктуры. Цели информационных действий Китая вероятнее всего удалены во времени на десятилетия в противоположность существующей американской тенденции к немедленным, но краткосрочным успехам.

Эксперты полагают, что версия о том, что Китай в настоящее время ведет информационную войну «незападной» формы получает достаточно много подтверждений. Так, в последнее время Китай стремится накапливать как можно больше значащей информации (особенно в области экономики и обороны), защищать собственную информацию, лиц принимающих решения и национальное единство. Китайцы стремятся эксплуатировать информационные системы их противника, создают общественные структуры, пытаясь влиять на процесс принятия решений их противником. При этом Китай пробует скрыть свои собственные намерения от Запада, потому что китайские стратеги осознают преимущества такого положения: возможность эксплуатации намного больше, когда цель предпринимаемых действий не осознается противником.

По мнению американских экспертов, если Китай намеревается победить, не вступая в открытое противоборство, то он в ближайшие годы будет тщательно придерживаться выбранной линии подкупа, запугивания, заимствования и кражи каждого возможного преимущества, но не противопоставляя при этом себя Западу и не идя на открытую конфронтацию.

Анализ открытой китайской литературы позволил американским экспертам выделить ряд базовых положений китайской концепции

информационной войны. К ним относят: атаки на компьютерные сети, информационные операции, экономические операции, высокоточные удары и направленные акции. Среди наиболее часто описываемых целей возможной войны было идентифицировано пять: преимущество национальной безопасности, экономическое преимущество, финансовая выгода, политическое влияние и изменение политики. В перспективе можно ожидать тесного переплетения всех четырех инструментов национальной мощи: вооруженных сил (преимущество национальной безопасности), экономики (финансовая выгода), дипломатии/политики (изменение политики) и информации (политическое влияние). Таким образом, любые средства, которые увеличивают национальную мощь, рассматриваются китайскими стратегами в качестве средства противоборства.

Понимание американскими экспертами китайского подхода к концепции информационной войны в академических кругах и сообществах экспертов остается сегодня недостаточным для построения адекватной стратегии противодействия Китаю в информационной сфере в ближайшие годы.

На основе детального анализа доступных источников делается вывод о том, что уязвимость инфраструктуры Америки сегодня, безусловно, очень высока, и угроза «электронного Перл-Харбора», особенно со стороны негосударственной организации, ответные действия против которой были бы весьма затруднены, не должна игнорироваться. Однако, в случае с Китаем, за исключением его возможного нападения на Тайвань, следует особенно внимательно относиться к долгосрочным целям его концепции информационной войны, которые гораздо больше сосредотачиваются на экономике и региональном влиянии. Эксперты подчеркивают, что экономическое развитие остается для Китая самым высоким национальным приоритетом.

Глава 4. Информационная борьба в конфликтах последнего десятилетия

4.1. Информационная борьба в ходе агрессии против Союзной Республики Югославии

Наиболее полную картину о характере информационной борьбы в период агрессии войск коалиции во главе с США против Югославии можно получить из книги аналитиков российского Генштаба /39/. В этой работе отмечается, что при подготовке агрессии против Союзной Республики Югославии НАТО придавало большое значение проведению информационных операций. Военно-политическое руководство блока исходило из того, что умелое и эффективное осуществление информационно-психологического воздействия в значительной степени определит уровень международной поддержки проводимых НАТО силовых акций и существенно скажется на морально-психологической устойчивости вооруженных сил и руководства СРЮ.

При планировании агрессии основные усилия информационных структур блока направлялись на решение следующих задач:

- формирование негативного представления о военно-политическом руководстве СРЮ как об источнике кризиса и основной причине гуманитарной катастрофы в Косово и Метохии, разрушение морально-

этических ценностей сербского народа и нагнетание неблагоприятного психологического климата в отношениях различных политических сил СРЮ;

- создание и поддержание у военно-политического руководства СРЮ сдерживающего страха перед силовыми акциями НАТО, в том числе и за счет подчеркивания реализуемости декларируемых угроз, афиширования высокой эффективности имеющихся вооружений и потенциальных возможностей объединенных вооруженных сил блока;

- формирование репутации внешнеполитического руководства США и НАТО как весьма жесткого в своих решениях и последовательного в действиях;

- прицельную информационную обработку ключевых фигур в руководстве СРЮ на основе учета их психологических особенностей, политической и иной ориентации, пропаганду и внедрение форм общественного поведения, снижающих моральный потенциал нации.

Одновременно с решением перечисленных задач планировался целый ряд мероприятий по воздействию на информационную инфраструктуру СРЮ, так как, по мнению американских военных экспертов, важным элементом в развитии современных политических кризисов является частичная или полная потеря институтами власти контроля над ситуацией вследствие разрушения информационной инфраструктуры.

События в Югославии с точки зрения информационного противоборства развивались стремительно и зачастую трагично. Югославские СМИ старались всячески подчеркнуть единство союза. Однако мировое общественное мнение формировалось в основном под воздействием западных СМИ, склонных к поддержке сепаратистских тенденций и настроений в югославских республиках. В силу этого предыстория гражданских, а затем и межгосударственных военно-политических конфликтов на территории бывшей Югославии не получала должного освещения, тем более, что негативный образ СРЮ был создан и поддерживался в мировом общественном мнении еще со времени военного конфликта в Боснии и Герцеговине.

Еще с начала 90-х годов вокруг событий в Югославии была начата информационная война. Рассматривая Югославию в качестве полигона для обкатки новых средств и способов ведения вооруженной борьбы, США и НАТО придавали большое значение информационному противоборству в военных операциях. Следует подчеркнуть, что решение по этому вопросу принимал лично президент США Б. Клинтон. Это говорит о том, что в США информационной войне отводится значительная роль, и она поставлена в один ряд со специальными операциями спецслужб.

На основании решения главы государства были определены объекты воздействия: на политическом уровне — это широкие слои населения стран НАТО и мировая общественность, на стратегическом — правительство, народ и вооруженные силы Югославии. Все мероприятия планировалось провести в два этапа.

На первом этапе (до начала агрессии) было предусмотрено информационное воздействие в основном на политическом уровне. Его основными объектами являлись: широкая общественность стран НАТО, других государств Европы, включая Россию, население Ближнего и Среднего Востока, Азии. Главные цели, поставленные на этом этапе, состояли в обеспечении международной поддержки курса США и их союзников по НАТО в отношении СРЮ, убеждении мирового сообщества, что в Югославии нарушаются права албанцев, и оправдании необходимости применения военной силы.

На втором этапе (с началом агрессии) акцент был сделан на ведение информационного противоборства на стратегическом уровне. В качестве основных объектов воздействия на территории Союзной Республики Югославии на этом этапе были определены ее правительство, личный состав вооруженных сил и население. Основная цель всех мероприятий по информационному воздействию на этом этапе — безоговорочная капитуляция СРЮ на условиях США и НАТО.

План информационной войны был согласован со всеми странами — участницами НАТО, от которых были выделены воинские контингенты. В ее осуществлении участвовали высшее политическое руководство стран НАТО, министерства иностранных дел, спецслужбы, национальные СМИ, армейские структуры ведения психологических операций. Участие этих сил в информационной агрессии против Югославии было подтверждено многочисленными теле- и радио заявлениями президента США, премьер-министра Великобритании, генерального секретаря НАТО, руководителей министерств иностранных дел и обороны стран — членов Североатлантического альянса.

При реализации перечисленных способов ведения информационной войны важнейшими формами информационного воздействия были информационно-пропагандистские акции, радиоэлектронная борьба, дезинформация. Использовались также специально разработанные методики и новые технологии разрушения баз данных, нарушения работы югославских компьютерных сетей.

Успешное выполнение задач информационной войны, по мнению военных экспертов, предполагало достижение трех важнейших целей:

- способности к дешифровке и пониманию работы информационных систем противника;
- наличие разнообразных и эффективных средств их поражения;
- готовности к оценке качества уничтожения информационных целей.

В США основные задачи в информационной войне выполняли государственный департамент, Информационное агентство США (ЮСИА) со своими подразделениями (международные спутниковые телесети, радиостанции "Го-

лос Америки", "Свобода", "Свободная Европа"), Центральное разведывательное управление и специалисты-психологи из Пентагона.

Структурные подразделения ЮСИА бесплатно рассылали в адрес тысяч радиостанций многих стран мира свои передачи в записи, издавали различные информационные бюллетени. Большое значение в деятельности ЮСИА придавалось реализации американских материалов в зарубежной прессе. Необходимо особо отметить, что распространение продукции самого ЮСИА внутри США было строго запрещено.

Одной из частей информационной агрессии явилось и развертывание направленного и интенсивного вещания на территорию Югославии радиостанции "Голос Америки", уничтожение теле- и радиоцентров с целью обеспечения контроля над общественным мнением населения. Так, после разрушения телецентров в Приштине и Белграде местные жители вынужденно оказались в информационном поле СМИ только стран НАТО. Для непосредственной "оккупации информационного пространства Югославии" НАТО применяло апробированные ранее США в Ираке, Гренаде и Панаме способы, в том числе летающую теле- и радиостанцию "Commando Solo", смонтированную на борту транспортного самолета С-130, которая транслировала свои передачи на частотах, используемых сербским телевидением.

В рамках информационно-пропагандистских акций было спланировано ведение радиовещания на Югославию с территорий сопредельных стран, а также разбрасывание пропагандистских листовок. Предполагалось активное использование штатных формирований психологических операций и соответствующих СМИ, находящихся в распоряжении командования сухопутных войск США. Для нарушения работы югославских компьютерных сетей Нью-Йорским университетом по заказу Пентагона были разработаны программные пакеты вирусов для внедрения в компьютерные базы данных.

Роль главного агитатора и пропагандиста, призванного отстаивать позицию США и НАТО в ходе агрессии, была отведена министру обороны У. Коэну. По сообщениям наблюдателей, только за первый день бомбардировок он выступил сразу в восьми телепрограммах, в пяти утренних выпусках новостей основных телеканалов и трех наиболее популярных вечерних ин-

формационно-аналитических передачах. У. Коэну помогали также помощник президента США по национальной безопасности С. Бергер и госсекретарь М. Олбрайт. К гражданам США с антисербским воззванием обратился и президент Б. Клинтон.

В этот же период прошла серия передач заказного характера на телевизионном канале Си-эн-эн, в ходе которых военные эксперты и аналитики буквально заполнили основную часть времени новостных и аналитических выпусков пропагандой в пользу действий НАТО. Ведущим корреспондентом Си-эн-эн, умело спекулировавшим на чувствах американцев, являлась К. Аманпор. Следует отметить, что использование корреспондента-женщины для освещения сюжетов о зверствах сербов в Косово и Метохии, страданиях косоварских женщин и детей имело сильное психологическое воздействие на американскую аудиторию.

Только в течение первых двух недель операции в Косово и Метохии Си-эн-эн подготовила более 30 статей, которые были размещены в Интернете. В среднем каждая статья содержала около десяти упоминаний о Т. Блэре со ссылками на официальных представителей НАТО. Примерно столько же раз в каждой статье использовались слова "беженцы", "этнические чистки", "массовые убийства". В то же время упоминание о жертвах среди мирного населения Югославии встречалось в среднем 0,3 раза.

Одним из безотказных приемов воздействия на аудиторию стало использование так называемых объективных цифр и документальных данных. Так, один из аналитиков Си-эн-эн заявил о будто бы имевшим место факте использования 700 албанских детей для создания банка крови, предназначенного для сербских солдат. Такая дезинформация, естественно, произвела сильное впечатление на общественное мнение Запада.

4.1.1. Характер и особенности информационного противоборства в ходе агрессии НАТО против СРЮ

Информационное воздействие в операции НАТО "Союзническая сила" велось с использованием отлаженного механизма, который был успешно апробирован в ходе подготовки и ведения военных операций ВС США в 90-х годах ("Буря в пустыне" в Ираке, "Поддержка демократии" на Гаити, миротворческая операция ИФОР-СФОР в Боснии и Герцеговине и др.) Главные

усилия в борьбе за информацию между ОВС НАТО и ВС Югославии были сосредоточены в информационно-психологической и информационно-технической сферах.

Информационные операции в ходе военных действий США и НАТО были направлены, прежде всего, против системы управления ВС СРЮ. В этих целях помимо применения управляемых ракет использовались электромагнитные бомбы, разрушительное действие которых сравнимо с поражающим фактором электромагнитного импульса, возникающего при ядерном взрыве. Этот импульс способен вывести из строя всю радиоэлектронную технику в радиусе десятков километров.

Наибольшее внимание при проведении операций уделялось следующим основным способам ведения информационной войны:

- применение тяжелого вооружения для полного разрушения штабов, командных пунктов и центров боевого управления войск (сил) югославской армии;
- использование соответствующих электронных средств и электромагнитного оружия для подавления и нейтрализации работы центров сбора информации ВС Югославии, для выведения из строя его средств связи и радиолокационных станций;
- введение в заблуждение югославских органов, ответственных за сбор, обработку и анализ разведывательной информации о противнике посредством имитации подготовки и проведения наступательных действий;
- обеспечение оперативной скрытности посредством строгого соблюдения режима секретности и воспрепятствования доступа противника к своей информации;
- проведение психологических операций, особенно с использованием телевидения, радио, печати для подрыва морального духа войск и населения СРЮ.

Основной составляющей информационного противоборства ВС НАТО во время агрессии против СРЮ являлось массированное идеологическое и психологическое воздействие крупнейших СМИ стран Запада и сил психологической войны ВС США на население и личный состав вооруженных сил

Югославии, государств Североатлантического блока, а также мировую общественность. Для обеспечения позитивного мирового общественного мнения о действиях ОВС НАТО в операции "Союзническая сила" страны блока вели мощную и активную пропагандистскую кампанию, направленную на формирование образа врага, против которого не только можно, но и необходимо применить оружие. При этом активно использовались традиционные методы воздействия на общественное сознание:

- репортажи о событиях;
- описание актов геноцида албанского населения Косово и Метохии;
- демонстрация силы и показ возможностей современных видов вооружения ВС США и других стран альянса, результатов ракетно-бомбовых ударов по Югославии;
- комментарии социологических опросов, связанных с событиями на Балканах.

В то же время повсеместно занижались боевые потери блока, замалчивалась информация о просчетах руководства НАТО, гибели мирного населения, выступлениях мировой общественности против продолжения и эскалации военных действий.

Целью информационно-психологического воздействия США и руководства НАТО на население и вооруженные силы стран-участниц вооруженного конфликта явилось формирование такого общественного мнения, которое в значительной степени оправдывало бы агрессию ОВС альянса против суверенного государства.

Временные неудачи США и его союзников по западному альянсу в информационно-психологическом противоборстве с Югославией на первом этапе конфликта были обусловлены многочисленными ошибками, которые были допущены руководством НАТО в сфере связей с общественностью. Так, настоящий провал произошел при интерпретации руководителями НАТО факта авиационного удара по колонне беженцев в Косово и Метохии 14 апреля 1999 года. Пресс-службе альянса потребовалось пять дней, чтобы в конце концов предоставить собственную более или менее ясную версию случившегося.

Несогласованность действий руководителей блока и его пресс-службы наблюдалась также и при оправдании авиационных ударов ОВВС по зданию посольства Китая в Белграде 8 мая, транспортным средствам (12 апреля, 1, 3, 5, 30 мая) и жилым кварталам в городах Алексинац (5 апреля), Приштина (9 апреля), Сурдулица (27 апреля, 31 мая), Софии (28 апреля), Ниш (7 мая), Крушевац (30 мая), Нови-Пазар (31 мая) и другим объектам.

Участившиеся провалы и упущения в работе пресс-службы НАТО привели к тому, что в ходе второго этапа операции в штаб-квартире блока в Брюсселе произошла серьезная реорганизация информационно-пропагандистского аппарата НАТО. Аппарат пресс-службы был усилен опытными специалистами в области "паблик рилейшнз", в том числе организаторами предвыборных кампаний в США и Великобритании.

Для восстановления утраченного в информационном противоборстве превосходства НАТО предприняло целый ряд решительных мер.

Во-первых, ряд ведущих мировых радиостанций ("Голос Америки", "Немецкая волна", Би-Би-Си и др.) значительно увеличили интенсивность радиовещания в УКВ-диапазоне на страны Балканского региона на албанском, сербохорватском и македонском языках. При этом радиостанции использовали американские передатчики, которые в срочном порядке были установлены на границах с Сербией. Передачи информационно-психологической направленности из-за пределов воздушного пространства СРЮ осуществлялись силами авиационной группы 193-го авиакрыла сил специальных операций национальной гвардии ВВС США с бортов самолетов EC-130E/RR.

Во-вторых, с целью подрыва информационно-пропагандистского потенциала Югославии ОВВС НАТО нанесли ракетно-бомбовые удары по теле- и радиостанциям, студиям и ретрансляторам, редакциям СМИ, большинство которых было уничтожено, что фактически означало ликвидацию системы телерадиовещания СРЮ.

В-третьих, на исходе второго месяца вооруженного конфликта под давлением НАТО совет директоров европейской телевизионной компании 'ЕУТЕЛСАТ" принял решение о запрете для компании "Радио и телевидение Сербии" вести вещание через спутник. В результате Сербское государ-

ственное телевидение лишилось последней возможности транслировать передачи на страны Европы, а также на значительную часть территории своей республики.

В-четвертых, силами психологических операций ВС США над территорией Югославии было разбросано более 22 млн. листовок с призывами к сербам выступить против президента С. Милошевича и способствовать «скорейшему завершению операции объединенных сил НАТО.

В-пятых, впервые мощная информационная поддержка крупной военной операции НАТО была развернута в сети Интернет. В ней было размещено более 300 тыс. сайтов, посвященных или в разной степени затрагивающих косовскую проблему и военную операцию альянса а Югославии. Подавляющее большинство указанных сайтов было создано непосредственно или при содействии американских специалистов по компьютерным технологиям, что, безусловно, повысило эффективность пропагандистской кампании НАТО.

Еще одной составляющей информационного противоборства в операции "Союзническая сила" явилось информационно-техническое противостояние ОВС НАТО и ВС СРЮ.

Борьба за информационное доминирование развернулась прежде всего в сфере электронных средств разведки, обработки и распространения информации ОВС НАТО при активном использовании современных средств и систем разведки, связи, радионавигации и целеуказания. В связи с этим соответствующие подразделения ОВС НАТО провели широкомасштабные акции по поражению важнейших пунктов управления ВС СРЮ, других элементов государственной и военной информационной инфраструктуры Югославии, а также подавлению находящихся на вооружении югославской армии систем и средств радиосвязи и радиолокационной разведки.

Другой важнейшей составляющей информационно-технического противоборства явилась борьба за информацию в вычислительных системах. Югославские хакеры неоднократно пытались проникнуть через сеть Интернет в локальные вычислительные сети, используемые в штабах ОВС НАТО. Массовые запросы серверов этих сетей в отдельные периоды времени

затруднили функционирование электронной почты. И хотя действия хакеров имели эпизодический характер, применение информационного оружия следует считать перспективным направлением информационного противоборства.

В итоге, несмотря на отдельные сбои, руководство НАТО сумело переломить ситуацию в информационно-психологическом противоборстве с Югославией и завоевать информационное превосходство. Информационно-пропагандистский аппарат альянса в целом выполнил поставленные перед ним задачи, своевременно внес коррективы в свою деятельность, разработал и применил новые формы и методы информационно-психологического воздействия на противника.

4.1.2. Противодействие вооруженных сил СРЮ силам НАТО в информационной войне

Тенденциозный, агрессивный характер информационного воздействия, осуществляемого НАТО в рамках начавшейся операции, впервые вызвал активное противодействие со стороны Белграда. Анализ событий показывает, что руководство США и НАТО на первом этапе операции оказались не в полной мере готовы к таким ответным действиям СРЮ. Подтверждением тому являются не только негативные для НАТО результаты социологических опросов, но и конкретные действия альянса, предпринятые уже по ходу второго этапа операции для того, чтобы вернуть утраченную инициативу в информационном противоборстве.

Несмотря на сильнейшее информационно-психологическое воздействие со стороны США и НАТО и неблагоприятный информационный фон, руководство СРЮ в целом достаточно умело действовало в сфере управления информацией, успешно противостояло информационно-психологическому давлению. В ходе конфликта не было зафиксировано случаев частичной или полной потери контроля над ситуацией со стороны югославских институтов власти из-за нарушения информационной инфраструктуры.

Как показывает анализ событий, то, что привело к ожидаемым результатам в Панаме и частично в Ираке, в Югославии оказалось малоэффективно. Так, в ответ на бомбардировки и массированное информационно-психологическое воздействие народ Югославии продемонстрировал

единство и согласие, в том числе и среди недавних политических противников, а многократный перевес войск стран — участниц агрессии против Югославии в личном составе и технической оснащенности не дал ожидаемых результатов при ведении широкомасштабных боевых действий.

Используя все возможности СМИ, военно-политическому руководству Югославии удалось временно перехватить инициативу в информационном противоборстве. Югославские СМИ, задействованные в пропагандистской кампании, удачно использовали факты жертв среди гражданского сербского и албанского населения Косово и Метохии, нарушений ОВС НАТО основных положений Женевских конвенций и дополнительных протоколов к ним, а также поддержку политических, религиозных и общественных деятелей России, Украины, Белоруссии и других государств.

Проведенные контрмеры вызвали всплеск патриотических чувств среди населения Югославии и подъем морально-психологического состояния военнослужащих ВС СРЮ. За счет ограничения передвижения иностранных журналистов, введения запретов на распространение определенной информации руководство СРЮ добилось сокращения количества сообщений СМИ негативного характера о проводимой им политике.

Таким образом, своевременно принятые меры политическим и военным руководством СРЮ на первом этапе операции "Союзническая сила" помешали США и блоку НАТО убедить мировую общественность в адекватности методов и способов проведения военной операции в Югославии, справедливости ее целей и задач. В результате в мировом общественном мнении произошел определенный раскол в отношении политики США и НАТО на Балканах.

С другой стороны, ход боевых действий показал, что умелое управление информацией со стороны руководства СРЮ в определенной степени позволило противостоять информационно-психологическому воздействию со стороны НАТО на население и вооруженные силы страны.

Полной дезорганизации системы управления ВС Югославии удалось избежать лишь благодаря комплексному применению защитных мер, включающих оперативную маскировку, радиоэлектронную защиту и противодействие разведке противника. Творчески используя опыт иракских

ВС в борьбе с МНС во время войны в Персидском заливе, ВС СРЮ удалось отразить большинство ударов интеллектуальным оружием, сохранить большую часть своего вооружения и военной техники, в том числе средств радиосвязи, радиотехнической и радиолокационной разведки.

Большое значение для сохранения боеспособности армии имели:

- своевременный перевод системы управления группировками войск (сил) ВС Югославии на полевые пункты управления;
- периодическая передислокация частей и подразделений;
- маскировка вооружения и военной техники;
- устройство ложных позиций, в том числе с использованием надувных макетов тяжелого вооружения;
- введение режимных ограничений на работу радиоэлектронных средств.

Опираясь на это, можно заключить, что даже самые современные информационные технологии вряд ли когда-либо могут заменить осознание каждым военнослужащим целей и характера войны в защиту территориальной целостности и независимости своей страны.

США и НАТО, обладающие более совершенными методами и средствами информационного противоборства, добились в ходе военного конфликта подавляющего превосходства в информационной сфере. Вместе с тем активные действия военно-политического руководства Югославии по нейтрализации информационно-психологических воздействий со стороны НАТО позволили ослабить информационный натиск на личный состав ВС СРЮ и население страны, а на одном из этапов даже перехватить инициативу в этом противоборстве.

Стратегия оборонительных военных действий ВС Югославии, ограниченность средств ведения радиоэлектронной борьбы, отсутствие методологии применения информационного оружия не позволили им провести комплекс мероприятий по активному информационно-техническому воздействию на системы управления, разведки, навигации и целеуказания противника. Это обусловило поражение ВС СРЮ в информационном противоборстве с ОВС НАТО.

Можно констатировать, что информационное противоборство в операции "Союзническая сила" занимало значительное место в действиях противостоящих сторон. Полученный опыт, а также перспективы технического развития дают основание выделить этот вид противоборства в рамках вооруженной борьбы в отдельную область противостояния между государствами или союзами государств. Особенность такого противостояния заключается в скрытности мероприятий, находящихся в контексте общей политики государств, преследующих свои национальные интересы.

Администрация США и руководства других стран-участниц НАТО развернули мощнейшую пропагандистскую кампанию и провели ряд операций в ходе информационной войны против Югославии, которая, однако, не сломила волю югославского народа, особенно ее вооруженных сил, их решимости в борьбе с агрессорами. В то же время благодаря активному использованию новейших информационных технологий общественное мнение в США и в большинстве стран Западной Европы оказалось на стороне инициаторов и виновников военного конфликта на Балканах.

В ходе военной операции против СРЮ руководство США и НАТО добивалось не только всестороннего обеспечения выполнения конкретной акции. Значительное внимание уделялось отработке перспективных способов ведения информационной войны.

Можно заключить, что войска НАТО, оснащенные информационными технологиями, имеют боевой потенциал, троекратно превышающий эффективность боевого применения обычных частей. Анализ боевых действий армии США показал, что информационные технологии обеспечивают сокращение среднего времени подлета и подготовки к атаке ударных вертолетов с 26 до 18 минут и увеличение процента поражения целей ПТУРами с 55 до 93 проц. Обработка и передача донесений в вышестоящие штабы в звене "рота—батальон" сокращается с 9 до 5 минут, вероятность дублирования телеграмм снижается с 30 до 4 проц., передачи подтверждающей информации по телефонным линиям — с 98 до 22 проц.

По взглядам руководства НАТО, вооруженные силы, владеющие информационными технологиями, представляют собой новую категорию войск с особой тактикой ведения боевых действий, организационно-штатной

структурой, уровнем подготовки личного состава и вооружением, полностью отвечающим требованиям современной войны. Войска и силы, привлекаемые для ведения информационной войны, активно применяют технологии цифровой связи, целостные системы боевого управления и разведки, высокоточное оружие и связь со всеми операционными системами. Важнейшим условием эффективных действий этих сил является их оснащение самыми современными видами вооружений: радарами второго поколения, системами опознавания типа "свой—чужой", глобальными космическими навигационными системами и боевой техникой со встроенной цифровой аппаратурой.

Учитывая большие возможности и высокую эффективность структур НАТО по информационному воздействию в военных конфликтах, следует ожидать, что руководство блока будет активно применять его в ходе подготовки и ведения возможных военных действий. Вследствие этого можно констатировать возрастание роли и значения информационного противоборства в военных конфликтах XXI века.

4.2. Управляемый хаос - базовая концепция управления кризисом в Македонии

Анализ таких концептуальных документов как «Стратегия национальной безопасности» и «Национальная военная стратегия США», а также базирующейся на них новой «Стратегической концепции НАТО» дал возможность российским военным экспертам сделать следующие выводы:

- в настоящее время отмечается существенное повышение военно-политической активности блока НАТО и расширение географии возможного применения военной силы далеко за пределы его зоны ответственности, определенной договором о создании альянса; настораживающим фактором здесь являются попытки объявить эти зоны сферой своих «интересов безопасности»;

- возрастает готовность США и НАТО использовать военную силу в различных ситуациях (примером тому являются минувшие события в Ираке, Сомали и Югославии); возможность применения военной силы на постсоветском пространстве также не исключается;

- активизируется разработка новейших технологий, способных обеспечить США военно-техническое превосходство над другими крупнейшими странами мира; большое внимание уделяется разработке новых приемов использования военной техники и вооружений, новых способов ведения военных действий применительно к изменившимся внешнеполитическим условиям, при этом особо следует отметить разработку и совершенствование средств и методов ведения информационных и психологических войн;

- в последнее время США и НАТО откровенно игнорируют международные институты обеспечения мира и безопасности (ОБСЕ, ООН, Совет Безопасности), которые рассматриваются в нынешних условиях как лишняя обуза, сдерживающая их геостратегическую активность.

Эти выводы были изложены в работе специалистов Центра военно-стратегических исследований Генерального штаба ВС РФ, результаты которой недавно опубликованы /39/.

Ни для кого не секрет, что, готовя военную акцию против Югославии, НАТО и США решали в основном собственные проблемы. Их действия мотивировались отнюдь не заботой о косовских албанцах. Так еще в мае 1996 года на заседании Билдербергского клуба, прошедшего в Турции, был поднят вопрос о ситуации в югославском крае Косово (по материалам канадской газеты «Toronto Star», июнь 1999 г.). Обсуждение вопроса о судьбе Косово возникло по чисто экономической причине: Запад получал стратегически важный металл хром в основном из Заира, однако в 1994 году после свержения режима Мабуту хромовые поставки оказались под угрозой. На территории же Косово (вместе с Албанией) находится до 90% разведанных европейских запасов этого сырья, стоимость доставки которого к европейским потребителям в 10 раз ниже, чем из Заира. Можно утверждать, что именно эти причины и мотивы, а не соображения высшей гуманности явились основой решения НАТО проигнорировать Устав ООН и общепризнанные принципы международного права.

Объективный анализ итогов военной агрессии против Югославии показывает, что на Балканах вслед за Ираком была предпринята попытка реализовать замысел, основанный на положениях новой стратегии НАТО: ***силой***

навязать миру право альянса на односторонние вооруженные действия по собственному усмотрению.

Кроме того, на Балканах США имеют и собственные специфические интересы, позволяющие держать Европу “в узде”:

экономически ослабить ЕС, дискредитировать единую европейскую валюту, что особенно важно в период кризиса американской экономики;

затормозить создание европейской оборонной структуры и консолидировать Европу на базе НАТО, где главную роль играют американцы;

усилить свое военное присутствие на Балканах (в «мягком подбрюшье Европы»);

продемонстрировать военную силу в целях устрашения несогласных с политикой США государств.

В соответствии с этими интересами с начала 90-х годов главной целью активно проводившейся политики США на Балканах было не достижение мирного урегулирования на основе принципов ООН, а стремление создать новый стратегический баланс сил после утраты Россией ключевых позиций в регионе.

Как отмечает «Независимое военное обозрение»[85] со ссылкой на британскую газету «Санди таймс», находясь в Косово в качестве международных наблюдателей за прекращением огня, сотрудники ЦРУ в течение длительного времени вели разведку югославской армии и полиции в интересах Освободительной армии Косово (ОАК), помогали обучать ее боевиков.

По данным той же «Санди таймс», когда представители ОБСЕ покидали Косово незадолго до начала первого массированного ракетно-авиационного удара натовской группировки по югославским городам, многие телефоны спутниковой связи и системы глобального позиционирования были переданы агентами ЦРУ боевикам ОАК. Это обеспечило им не только возможность поддерживать контакты с командованием НАТО в Брюсселе и наводить авиацию альянса на цели, но и вести прямые переговоры с Пентагоном,

[85] Веет холодной войной. За спиной косовских мятежников стоит американское ЦРУ, Николай Плотников, "Независимое военное обозрение", номер 10 (183) от 24 марта 2000 года.

государственным департаментом США и штаб-квартирой ЦРУ в Лэнгли. По некоторым данным, лидер косовских сепаратистов Хашим Тачи и начальник Генерального штаба ОАК Агим Чеку даже вели прямые переговоры по мобильной связи с главнокомандующим объединенными вооруженными силами НАТО в Европе американским генералом Уэсли Кларком, делились с ним впечатлениями от ударов авиации альянса и консультировались по тактике дальнейших действий.

Такое поведение представителей ЦРУ отнюдь не случайно. Согласно имеющимся данным четко прослеживается определенная последовательность событий, логическая цепь которых соответствует разработанной на Западе ***технологии управления кризисом***.

Проведенная операция сил НАТО в Македонии не претерпела сколько-нибудь явных изменений в плане режиссуры и постановки уже подготовленного сценария.

Еще с середины 90-х годов, не смотря на показной оптимизм США и НАТО в вопросе скорейшего приема в альянс новых членов из числа балканских государств в рамках программы «Strategic home» (в том числе и Македонии), стала четко прослеживаться линия, согласно которой эти балканские страны не будут в ближайшее время приняты в альянс по ряду причин и, прежде всего, в силу невозможности полного и беспрекословного подчинения славянского населения этих стран целям НАТО. Можно предположить, что в этой ситуации специалистами США и НАТО была предложена новая программа утверждения Альянса на Балканах – путем разжигания и поддержания нескольких конфликтов малой интенсивности с целью формирования на месте суверенных государств ряда протекторатов НАТО. Сегодня эта политика реализуется в отношении Югославии и Македонии.

Этот вывод подтверждается результатами анализа последних действий НАТО в Македонии.

Еще в период югославского кризиса западные спецслужбы самым тщательным образом изучили степень оснащенности боевиков ОАК[86]. Кроме

[86] Плечом к плечу с мафией. Амбиции Объединенной Албании взращиваются на криминальной почве. Владимир Владимиров, «Независимое военное обозрение» (НВО), электр. версия прил. к «НГ» (ЭВНВО). Номер 019 (142) от 21 мая 1999 г.

тяжелого и легкого вооружения, доставшегося по бросовой цене в результате разграбления складов албанской армии в 1997 г., значительная его часть была закуплена на деньги итальянской мафии и переброшена в Косово через Албанию, Боснию, Хорватию и даже Македонию. В свое время правительство Албании обратилось в ООН с просьбой оказать помощь в возврате 650 тыс. единиц тяжелого и легкого оружия, находящегося в руках у населения страны. В течение нескольких месяцев эксперты ООН установили, что из арсеналов албанской армии было похищено 226 тыс. автоматов АК-47, 351 тыс. карабинов СКС, 38 тыс. пистолетов, 25 тыс. ручных и станковых пулеметов, 2,5 тыс. ручных гранатометов и 750 гаубиц. Одновременно албанское правительство объявило пропавшим 215 тыс. противопехотных мин, 1 млн. противотанковых мин, 20 тыс. тонн тротила и полтора миллиона патронов калибра 7,62 мм. Значительная часть похищенного оружия была продана албанской диаспоре в Косово и Македонии. И на этом фоне «миротворцы» НАТО в рамках операции «Необходимая жатва» планируют собрать в Македонии всего около 3 тыс. единиц оружия!

Эта ситуация сегодня оказалась в центре внимания СМИ Великобритании. По мнению англичан, если речь идет всего лишь о сборе 3 тыс. единиц оружия, то почти равная этой численность натовских военнослужащих явно завышена.

Безусловно, оценка в 80 тысяч единиц вооружения, данная правительством Македонии, намного точнее отражает сложившуюся ситуацию, но западные СМИ уже за несколько дней до начала операции четко очертили границы возможной уступки со стороны албанцев: 3000 единиц и не стволом больше, причем добровольно!

Во время косовского кризиса пресс-секретарь ОАК Гани Сюлал сказал: «НАТО должна "пробить коридор" для ОАК, уничтожив сербские танки и артиллерию, надежно прикрывающие административную границу Косово». Теперь на пути албанских террористов встала армия Македонии, и вновь на помощь боевикам приходит «Большой брат» в лице НАТО.

В этой связи уместно привести слова Майка Хоссудовски, профессора экономики Университета Оттавы, Канада. В своей статье, перевод которой

был опубликован в газете «Советская Россия»[87], он отмечает, что западная пресса утверждает, будто США и ЕС играют посредническую роль во "внутреннем конфликте". Общественному мнению Запада внушают, что кризис в Македонии проистекает прежде всего от ущемления социальных, политических и культурных прав албанского меньшинства и, что "международное сообщество" стремится прекратить насилие между "правительственными войсками и албанскими повстанцами", помогая обеим сторонам достичь урегулирования. И только это!

Правда же состоит в том, что, по словам М. Хоссудовски, Освободительная армия Косово (ОАК) и Национально-освободительная армия (НОА) в Македонии являются вспомогательными воинскими формированиями США. Главари ОАК и НОА, которые до последнего времени находились на содержании миссии ООН в Косово, обучены офицерами частей специального назначения Великобритании и США.

Большинство западных СМИ описывают террористов как "албанских повстанцев", защищающих права этнического меньшинства в Македонии. Однако имеется достаточно доказательств того, что ОАК-НОА являются хорошо организованными наемническими силами, в состав которых входят, в том числе, и наемники из стран-членов НАТО.

Западные СМИ утверждают, что американский посол Джеймс Пардью призван "способствовать урегулированию". На деле же его военно-разведывательная миссия состояла в том, чтобы посредством угроз, запугивания и политических манипуляций добиться подписания "рамочного документа", который и был подписан 13 августа 1998г. Смысл этого документа в том, чтобы создать юридическое обоснование для оккупации Македонии войсками НАТО. Чтобы достичь этой цели лидеров македонских политических партий обманывали и втягивали в сомнительные сделки и (по сообщению из одного источника) прямо подкупали. За всем этим стоят крупные экономические интересы США. В то время, как "посредники" из США и ЕС обещали, что "мирное соглашение" закладывает основу для "разоружения повстанцев" и для обеспечения прекращения огня, в реальности дело движется в обратном направлении. У НАТО нет и не было

[87] Оккупация Македонии. Майкл Хоссудовски, перевод с англ. В.Тетекина. «Советская Россия», 28 августа 2001 г.

намерения полностью разоружить АНОА, лишить сепаратистов новейшего оружия с клеймом "сделано в США".

Далее М. Хосудовски отмечает, что интервенция НАТО под кодовым названием «Необходимая жатва», осуществляемая под контролем Великобритании, выполняет несколько основных задач. Прежде всего - это не «разоружить повстанцев», а ослабить и деморализовать вооруженные силы Македонии, о чем свидетельствует давление, оказываемое Вашингтоном на Украину с целью заставить ее прекратить военную помощь Македонии. Соглашение призвано усилить атмосферу этнической ненависти между албанским меньшинством и македонским большинством, что будет оправдывать дальнейшее военное и политическое вмешательство по «гуманитарным мотивам» и, наконец, «рамочное соглашение» закладывает основу для превращения Македонии в натовский протекторат (как это произошло с Боснией и Косово), что приведет к разрушению Македонии как страны. Подписывая соглашение, власти Скопье под давлением реально отказались от своих властных прерогатив на одной трети своей территории, открывая дорогу оккупации страны войсками НАТО в нарушение международного права. Такая интерпретация происходящих событий совпадает с мнением российских экспертов.

Анализ складывающейся обстановки на Балканах позволяет предположить возможность расширения конфликта и возникновения нового очага напряженности - на этот раз уже в Греции - как следствие поддержки (информационной и финансовой) официальной Анкарой, разворачивающегося в Албании движения так называемых «чамов». Так на организованных в июне этого года митингах и демонстрациях у посольства Греции выдвигались требования по возвращению их на историческую родину, компенсации ущерба за конфискованную собственность и, в последующем возможности создания своей культурной автономии. Турция, как и Греция, является членом НАТО, и поэтому обещает вынести данный вопрос на международный уровень.

Кроме того, еще в середине 90-х годов масоны Греции, провозглашая новые устремления «мировой закулисы» открыто заявили о своей полной поддержке территориальных претензий Афин к бывшей югославской республике Македонии («Правда», 13.02.1996).

Превращение Македонии в безвольный протекторат Северо-Атлантического Альянса является очередным шагом к дальнейшей милитаризации Балкан. Многие эксперты сходятся во мнении, что во многих отношениях все это напоминает оккупацию Судетской области Чехословакии фашистской Германией по Мюнхенскому соглашению между Гитлером и Чемберленом. Аннексия Судет «третьим Рейхом» стала предпосылкой к вторжению в Польшу в 1939 году. В этой ситуации правительствам многих государств, так стремящихся ввергнуть народы своих стран в ряды членов Альянса, следует задуматься над возможными последствиями их соучастия в грязных делах НАТО. Пример Македонии, еще вчера так рьяно стремившейся в НАТО, позволяет сделать некоторые выводы.

Учитывая определенную шаблонность действий американских военных, можно достаточно точно прогнозировать дальнейшее развитие обстановки не только на Балканах, но и в ряде прилегающих районов. Следует ожидать провокаций в период выборной кампании в Белоруссии, в отношении Калининградской области, в Средней Азии и в ряде других регионов на подступах к государственной границе России, а зачастую - и на ее территории. Наметившиеся позитивные сдвиги в экономическом и социальном возрождении России, а также укрепление Китайской народной республики заставляют США и НАТО спешить с реализацией своих устремлений о мировом господстве.

В настоящей книге мы уже не раз обращались к теме 11 сентября прошлого года и тем событиям, которые последовали после. Чем дальше отдаляемся мы от этой даты, и чем глубже делаем анализ происходящих событий, тем тревожнее и безрадостнее становятся прогнозы.

Одним из них является вывод о том, что после событий 11 сентября 2001 года глобальная экспансия США развернулась такими темпами, что говорить о некой антитеррористической операции, разработанной всего за месяц после терактов, просто бессмысленно: даже обывателю сложно отделаться от мысли, что все действия были давно и четко спланированы - система ждала только «времени Ч» для начала этой беспрецедентной стратегической операции.

Да, Россия, уставшая от внутренних проблем с терроризмом, уже 12 сентября полностью поддержала США в необходимости проведения ответных действий по искоренению «мирового зла» - терроризма, и одной из первых вступила в антитеррористическую коалицию. Но надежда на «индульгенцию» в решении чеченской проблемы растаяла менее чем через месяц после начала активной фазы операции в Афганистане: в западной прессе российское сотрудничество в рамках борьбы с террором расценивается не иначе как «попытка скрыть варварства, чинимые российскими военными в Чечне». Сегодня уже настало время снять розовые очки и посмотреть на реалии «обновленного» мира. А они далеко не радостные.

Во всех случаях эскалации напряженности в ряде регионов Центральной и Восточной Европы, а также Центральной Азии и на Кавказе, имевших место в последнее время, четко прослеживается определенная последовательность событий, логическая цепь которых соответствует применению технологии управления кризисом, разработанной на Западе в начале 80-х годов прошлого века. Так, детальный анализ развития обстановки на территории бывшей Югославии позволил выделить в событиях того периода вполне конкретные элементы этого подхода[88]:

- объединение разрозненных политических сил, выступающих против существующего легитимного правительства;
- создание объединенного руководства оппозицией;
- разработка выгодной для субъекта управления системы корпоративных взглядов на будущее развитие страны;
- формирование стратегических, оперативных и тактических целей оппозиции;
- разработка программы, обосновывающей деятельность оппозиции и обещающей населению страны улучшение жизненных условий после свержения существующего правительства;

[88] Технология управления кризисом изложена в полевых уставах американских ВС FM-100-20 1990 г. и FM-100-23 1994 г.

- выработка организационных и оперативных методов работы оппозиции;
- подрыв уверенности лидеров правительства в своих силах и в лояльности (преданности) силовых структур государственному руководству;
- завоевание поддержки ведущих социальных групп;
- расширение международной поддержки оппозиции при одновременной изоляции существующего правительства от дипломатической, экономической и особенно военной помощи других государств;
- открытая дестабилизация обстановки в стране, поощрение мародерства, терроризма и др. с целью посеять панику среди населения страны и его недоверия к правительству;
- организация смены власти путем военного мятежа, “демократических” выборов или другим путем;
- поддержание в государстве противоречий с целью недопущения стабилизации обстановки и утраты контроля над действиями марионеточного руководства.

Такая концепция обычно реализуется как стратегия «управляемого хаоса», построенная на межэтнических или религиозных конфликтах.

На прошлой неделе по сообщениям ряда СМИ стало известно, что на фоне глобальной антитеррористической кампании, проводимой США во многих регионах мира, завершилась подготовка ко второй фазе широкомасштабных военных учений объединенных сил НАТО. Данная фаза учений, начавшихся в ноябре 2002 г., получила название «Strong Resolve-2002». Она проходила с 1 по 15 марта 2002 года на территории Норвегии и Польши - в непосредственной близости от границ Белоруссии и России. Уже завершена переброска войск НАТО в район учений.

По данным прессы, в качестве цели учений руководство Североатлантического альянса называет проверку способности объединенных вооруженных сил (ОВС) НАТО и подразделений стран - участниц программы «Партнерство ради мира» вести одновременно на различных театрах военных действий две крупномасштабные операции: по урегулированию кризиса (по сценарию - на территории Польши) и по

обороне территории одной из стран-участниц в соответствии с коллективными обязательствами (центральные области Норвегии и прилегающая акватория Норвежского моря).

Особо подчеркивается, что главная задача норвежской фазы учения заключается в отработке действий ОВС НАТО по отражению агрессии и восстановлению контроля над территорией подвергшегося нападению государства-члена блока с применением сухопутных, военно-воздушных и военно-морских сил Альянса.

В учениях принимают участие военнослужащие 18 стран НАТО и государств - участников программы "Партнерство ради мира", в том числе: Литвы, Латвии, Эстонии, Австрии, Болгарии, Финляндии, Словакии, Словении, Швеции, Украины, Узбекистана и Ирландии. Кроме того, приглашены наблюдатели из 50 государств.

По некоторым оценкам общая численность личного состава, принимающего участие в учениях, достигает 40 тысяч человек. Задействованы 7-8 тысяч единиц боевых машин, более 200 самолетов и вертолетов, а также корабли ВМС Норвегии и других стран НАТО.

В связи с тем, что Норвегия не обладает собственными системами наблюдения, разведки и целеуказания, в учении задействованы немецкие разведывательные беспилотные летательные аппараты и система воздушного наблюдения и разведки НАТО «Цезарь». О масштабах проводимых учений говорит и то, что штаб ВГК ОВС НАТО в Европе обратился к США с просьбой развернуть в районе учения систему J-STARS.

Проводимые учения являются крупнейшими маневрами сил НАТО со времен югославского конфликта. Они являются второй фазой военных маневров, которые были начаты еще в ноябре 2001 года с проведения учений «Baltic Confidence–2001», проходивших с 12 по 23 ноября 2001 года. Эти командно-штабные учения проводились в рамках подготовки к учению ОВС НАТО «Strong Resolve-2002». Основная цель - отработка руководства действиями сухопутного компонента многонациональных оперативных сил в операции по кризисному урегулированию. Система управления создавалась на базе штабных структур германо-датско-польского объединенного армейского корпуса путем включения в их состав офицеров ОВС НАТО и

вооруженных сил ряда государств-участников программы «Партнерство ради мира».

Характерно, что предусмотренная сценарием учения исходная военно-политическая обстановка характеризовалась обострением отношений между двумя бывшими республиками одного (в прошлом единого) государства, «имеющими, неоднородный этнический состав населения». Руководство одной из этих республик готовилось применить силу для защиты национального меньшинства в другой республике с пересмотром существующих государственных границ. Согласно сценарию, ситуацию усугубляет активизация в приграничном районе преступных и террористических групп. В этих условиях Многонациональные силы вводятся на территорию страны, которой угрожает агрессия, и способствуют урегулированию межэтнических разногласий.

Сегодня мы можем наблюдать дальнейшее развитие событий по «кризисному управлению». Не надо быть большим специалистом в области оценки военно-политической обстановки, чтобы догадаться, какая из стран стоит за определением «одно в прошлом единое государство, имеющее неоднородный этнический состав населения» - это Россия.

Учения сил НАТО проходят в условиях серьезно обострившейся международной обстановки. Так, одновременно с информацией о проведении учений в прессе появились сообщения о том, что недавно Минск посетил представитель Госдепартамента США Ричард Баучер, который сообщил журналистам, что у США имеются неопровержимые доказательства причастности Беларуси к продаже оружия террористам.

Удивительно, что Беларусь сразу не была включена в провозглашенную Д. Бушем «ось зла». Ведь еще в октябре 2001 года помощник Госсекретаря США по делам Европы и Евразии Элизабет Джонс заявила, что «… результаты выборов в Беларуси «были украдены» Александром Лукашенко - последним диктатором Европы».

Кроме того, на текущий момент США уже достаточно прочно закрепились в Центральной Азии. В качестве подтверждения этому в декабре 2001 года в Комитете по международным отношениям Сената США был создан специальный подкомитет по Центральной Азии и Кавказу. На его

открытии Элизабет Джонс заявила: «Уже сам факт его [подкомитета] создания свидетельствует о большом значении, придаваемом сейчас Соединенными Штатами этой части света. С Центральной Азией мы взаимодействуем серьезно и на долгосрочной основе». Далее она отметила следующее, что «…к концу 19-го века враждующие местные деспоты не устояли перед колонизацией, проводимой Российской империей. В начале 20-го столетия советская империя зажала этот регион в тиски сталинизма…», нынешний же приход в регион американских войск следует рассматривать как долгожданное освобождение из под «тяжкого ига».

Хотя Пентагон и уверяет Россию, что оставаться на долгосрочной основе в Центральной Азии США не собираются, что они целиком признают приоритет России в этом регионе, но реальность гораздо прозаичнее: в настоящее время на территории ряда государств Центральной Азии разворачивается активное военное строительство.

Практически одновременно с триумфальным входом американских войск в Центральную Азию происходит резкое обострение напряженности в Молдавии. Вновь вспыхивают разногласия в Крыму. Буквально ураганом в прессе проносится информация о высадке американских войск в Грузии.

По этому поводу несколько дней назад исполняющий обязанности американского посла в Тбилиси Филипп Ремлер в интервью еженедельнику Akhali Versia заявляет, что Вашингтон готов помогать тем странам, где прячутся члены Аль-Каиды. По его словам, несколько десятков боевиков бежало из Афганистана и теперь скрывается на Кавказе. Часть из них прячется в Панкисском ущелье. Однако действительно ли боевики Аль-Каиды находятся в Панкисском ущелье на сегодня совершенно неясно. Но утверждения на это счет делают не только американцы. Министр безопасности Грузии Валерий Хабурдзания заявил на заседании кабинета министров 9 февраля, что еще в прошлом году были арестованы арабы, которые собирались создавать в Панкисском ущелье «нелегальные вооруженные формирования» для налетов на территорию России. Но увидеть якобы арестованных так никому и не удалось до сегодняшнего дня. Неизвестны имена и пяти афганцев, которых, как утверждает грузинская служба, она уже арестовала.

Очевидно, что грузины и американцы просто разыгрывают карту Аль-Каиды, чтобы оправдать излишнее военное присутствие США в зоне российских интересов.

Одновременно с этим, Запад пытается подыграть России с тем, чтобы очередное расширение НАТО не оказалось для нее слишком болезненным. Несколько дней назад появились сообщения о том, что высказанные британским премьером Т.Блэром предложениях о «качественно новых отношениях» НАТО и России, сделанные им около трех месяцев назад, только сегодня получили одобрение со стороны всех девятнадцати членов Альянса. «Новые отношения» с одной стороны, должны отдать должное готовности президента В.Путина к сотрудничеству после террористических актов, совершенных 11 сентября 2001 г., а, с другой, - помочь России легче перенести новый этап расширения НАТО. По всем прогнозам, новыми членами альянса станут три государства Балтии. Вопрос о расширении НАТО должен быть решен уже в ноябре текущего года на саммите Альянса в Праге. Однако сразу после этого британская «The Financial Times» опубликовала открытое письмо генерального секретаря НАТО лорда Робертсона в котором он ясно дал понять, что Россия никогда не сможет стать полноправным членом Альянса.

В этой ситуации уместно вспомнить, чем обернулась предыдущая волна расширения блока – с началом агрессии против Югославии России было отказано в предоставлении воздушного пространства для пролета самолетов с целью доставки гуманитарных грузов. В той ситуации мы на себе ощутили достоинства решения руководства Североатлантического блока, согласно которому необходимо было сначала принять в НАТО Польшу и Венгрию, а уже потом нанести удар по Югославии.

К величайшему сожалению следует признать, что сегодня в столь сложной и динамичной обстановке российское военно-политическое руководство серьезно проигрывает в развязанной информационно-пропагандистской кампании, обеспечивающей операцию США по переустройству мира.

Многие решения принимаются либо с серьезным опозданием, либо без должного анализа возможных последствий. К таким решениям можно

отнести недостаточно просчитанное решение о сокращении российских баз на Кубе и во Вьетнаме, которое оказалось на редкость «кстати» для американцев, лишив Россию весомой доли оперативной информации о развитии «антитеррористической» операции, а обещанного в замен десятка спутников наблюдения нет даже в арсенале.

К разряду таких решений можно отнести и поспешные заявления Министра обороны РФ о «невозможности, даже гипотетически, присутствия войск НАТО в Центральной Азии». А последние события в Грузии стали откровением даже для президента, в чем он сам признался на саммите глав СНГ.

Сейчас еще есть время, чтобы России не стать «одним в прошлом единым государством, имеющим неоднородный этнический состав населения», но оно катастрофически тает.

4.3. Опыт информационной войны США в Афганистане в ходе антитеррористической кампании

4.3.1. Геополитические устремления США в Средней Азии

Руководство США не предоставило общественности никаких доказательств вины Усамы бен Ладена, мусульманских террористов, но сразу же, по существу, "назначило" виновных и стало готовиться к широкомасштабной антитеррористической операции, войне, вовлекая в нее другие государства. Бывший руководитель Первого главного управления КГБ СССР Л. Шебаршин прямо говорит: «практически сразу в причастности к случившемуся был обвинен бен Ладен... Был ... весьма странный момент, во всех событиях, последовавших за трагедией 11 сентября. Я имею в виду рефлекторную реакцию американской стороны на всех уровнях: априорно во всем были обвинены мусульманские организации и ислам в целом. В том же духе были выдержаны заявления официальных американских лиц, которые не успели, да и физически не могли ни в чем разобраться. Они в один голос заявили: это не экстремисты, не террористы - это ислам. *Похоже, что сценарий реакции американского общества на трагедию был заранее тщательно подготовлен*».

Среди многих специалистов-политологов сформировалось устойчивое мнение о том, что *США 11 сентября 2001 г. провели колоссальную*

провокацию, направленную на развязывания рук для активной реализации идеи мирового господства на планете.

В подтверждение этого умозаключения приводятся следующие доводы:

1. Террористическая организация "Аль-Каида", несмотря на ее могущество, не могла провести нападение на выбранные цели. По утверждению Л. Шебаршина, «… упомянутая организация известна миру не первый год. Еще лучше она известна спецслужбам США, Англии, Израиля. Разумеется, эти спецслужбы затратили немало усилий, чтобы держать эту организацию под контролем, знать кадры, быть в курсе ее замыслов. Электронная почта, радиосвязь, телефонная связь - все под контролем. Трудно даже представить, что подготовка и осуществление такой масштабной операции, как теракт 11 сентября, прошли без использования электроники и эфира. Еще труднее представить, чтобы это не было перехвачено и зафиксировано… Профессионалы, которыми были укомплектованы упомянутые службы, не могли не использовать свою агентуру в окружении лидеров экстремистских группировок".

2. Факты свидетельствуют о задолго и тщательно продуманном замысле и четкой организации действий террористов. Для одновременного захвата 6 и даже более самолетов требовалось соответствующее количество пилотов. Пилоты захваченных самолетов показали высокий профессионализм: нужно было практически синхронно и без подозрений долететь до целей и не промахнуться. Значит, их тщательно и долго готовили для вождения именно этих самолетов. Тем не менее, о многомесячной подготовке пилотов и самих терактов, в которых были задействованы десятки, если не сотни человек, американские спецслужбы ничего не знали.

3. Террористы знали и использовали в переговорах кодовое слово, обозначавшее самолет президента США. Им были известны и коды (комбинацию из шести цифр), которые получают командиры "Боингов" лично от диспетчера непосредственно перед вылетом. Не введя эти цифры, пилот, во-первых, не сможет вырулить и взлететь. Во-вторых, после ввода шифра он в течение примерно 20 минут не имеет возможности отклониться от заданного курса. Единственное, что ему разрешается - увеличить высоту в пределах своего коридора. Поменять курс можно только тогда, когда

кончается время шифра. На самом деле самолеты после взлета в направлении Лос-Анджелеса спустя минуту-другую разворачивались на Нью-Йорк. Напрашивается очевидный вывод: чтобы совершить диверсию такого масштаба террористы должны были иметь своих людей в огромной сети взаимно перекрывающих, дублирующих, многократно резервированных спецслужб с огромными финансовыми и техническими возможностями.

4. Особо стоит отметить, что теракты были совершены именно в тот момент, когда уже назревал международный финансовый кризис. После упорных разговоров о неминуемом падении доллара за день до террористических актов некие крупные игроки на Лондонской бирже стали играть на понижение.

5. Террористические акты произошли накануне введения Европейским Союзом в наличный оборот своей валюты, в которой США видят реальную угрозу своему доллару. Теракт помог американцам спасти свою валюту за счет привлечения европейских ресурсов на ведение боевых действий.

6. Из 352 подозреваемых в помощи террористам, задержанных агентами ФБР, никто не имел прямого и доказательного отношения к девятнадцати террористам-смертникам, принимавшим участие в терактах. Об этом сообщил Генеральный прокурор и министр юстиции США Дж. Эшкрофт членам американского конгресса. ФБР также не располагает никакими свидетельствами деятельности "Аль-Каида", или любой другой группы Усамы бен Ладена в США.

7. Исчезновение бен Ладена и его главных сообщников позволяет Белому дому говорить о необходимости распространения антитеррористической операции не только на Афганистан, но и на другие государства, по тем или иным причинам неугодные Соединенным Штатам (Ирак, Иран, Йемен, Сирию, Индонезию, Филиппины и т.д.).

Однако приведенные умозаключения не являются юридическими доказательствами отнесения событий 11 сентября к провокации, проведенной американскими глобалистами. *Очевидным последствиям информационно-психологической обработки мировой общественности под флагом антитеррористической операции стало расширение влияния США в азиатском регионе*. Лозунг борьбы с терроризмом стал хорошим поводом

вмешиваться во внутренние дела других государств. Помощник госсекретаря США Элизабет Джонс не случайно заявила, что "когда конфликт в Афганистане завершится, мы не уйдем из Центральной Азии". И речь идет не только о появлении военных баз США и их союзников в Пакистане и Афганистане. Присутствие США будет увеличиваться во всех странах, втянутых и втягиваемых в борьбу с терроризмом, даже несмотря на некоторое сопротивление правительств этих стран.

Рисунок 22.Подразделение психологических операций армии США за работой

Военные базы, создаваемые Соединенными Штатами в Средней Азии, выполняют функции не только борьбы с терроризмом. *Их долгосрочной задачей является обеспечение военного, стратегического и экономического влияния Америки в богатом нефтью и газом регионе*. Эти базы будут служить фундаментом для строительства Америкой своей мировой империи.

Соединенные Штаты осуществляют грандиозный стратегический захват власти в Средней Азии. В прежние времена такой вид экспансионизма был бы назван колониализмом или империализмом. Сегодня эта экспансия называется просто "войной против терроризма". Война в Афганистане представляет региональные политические, экономические и военные возможности, которые долго изыскивались Соединенными Штатами и которые сейчас попали им в руки. В сентябре 2000 года, например, генерал Томми Фрэнкс уже колесил по Средней Азии, размахивая чековой книжкой военной помощи. Однако в целом, во время правления Клинтона острое желание Соединенных Штатов протоптать дорожку к среднеазиатским запасам нефти и газа наталкивалось на различные препятствия, особенно после ракетных ударов по Афганистану 1998 года, которые последовали после устроенных движением "Аль-Каида" взрывов зданий американских посольств в Кении и Танзании.

Соединенные Штаты, натиском, лестью и подкупами пробив себе дорогу в Среднюю Азию, не выказывают никакого желания покинуть в скором времени этот регион. Предотвращение угрозы возвращения

политической ситуации в Кабуле к прошлому состоянию или возрождения движения Талибан только частично является задачей американских баз, повсеместно создаваемых вокруг Афганистана. Их более *значимой, более долгосрочной задачей является защита американского влияния и американских интересов в странах, куда США ранее не проникали.*

Потенциальные выгоды для Соединенных Штатов в Средней Азии огромны: растущее военное господство в одной из немногих частей света, которая еще не находится под влиянием Вашингтона, рост стратегического влияния за счет уменьшения влияния России и Китая, существенное политическое влияние и, что является самым важным, доступ к огромным запасам среднеазиатской нефти и газа, не находящихся под контролем ОПЕК. США стремятся создать энергетический источник, альтернативный Персидскому заливу. Такой альтернативой в Азии является Каспийский регион. В Азербайджане запасы нефти и газа могут составлять около 10% мировых запасов, в Казахстане и Туркмении также около 10% в обеих странах. По оценке ОПЕК, общие запасы нефти и газа в регионе составляют 23 млрд. тонн. Коммуникации Каспия, прежде всего нефтепровод "Баку-Новороссийск", традиционно шли через территорию России. В середине 1990-х годов это перестало устраивать США. Почти все альтернативные российскому нефтепроводные проекты: "Баку-Супса", "Баку-Джейхан", "Одесса-Броды-Гданьск" родились в результате прямых или завуалированных усилий американской администрации.

В США рассматривался вариант переброски энергоносителей через Иран. Были предприняты шаги для сближения с иранскими либеральными кругами, но это ни к чему пока не привело. Нефть из Казахстана может пойти в Китай, которому для рывка в мировые лидеры не хватает только дешевых энергоносителей. Этого США допустить не хотят.

Путь из Туркменистана и Казахстана через Афганистан и Пакистан в Индийский океан самый дешевый для прикаспийской нефти и, главное, не проходящий через российскую территорию. Для обеспечения этого маршрута США могут взять под контроль Гератскую долину в направлении на Кабул и пакистанский Пешавар. По этому пути наиболее вероятна прокладка трубопроводов из Узбекистана и Туркмении к пакистанскому порту Карачи.

Контроль может быть обеспечен насаждением в Афганистане марионеточного режима.

Для России реализация замыслов США принесет огромные потери.

Присутствие США и НАТО на южных рубежей бывшего СССР закрепит геополитический отрыв среднеазиатских республик от России. Судьба контингента российских войск в Таджикистане, Армении и особенно в Грузии становится очевидной - вывод под первым же благовидным предлогом. Грузия уже требует этого. При наличии войск НАТО в Грузии и Азербайджане российские погранвойска в Армении теряют смысл.

Узбекистан пока заперт Ираном с юга и Россией с севера, но получив устойчивый выход на порт Карачи в Пакистане, он может полностью отказаться от партнерства с Россией и переключиться на Запад. Оказавшись в ключевой зоне ветки на Ашхабад, Баку, Тбилиси и Стамбул, Ташкент сможет строить особые отношения и с Турцией.

Осуществление проекта Евросоюза в рамках программы "Tacis" "Шелковый путь 21 века" ("TRACECA" - Transport Corridor Europe Caucasus Asia) с целью организации нового пути, соединяющего Европу с Китаем и Юго-Восточной Азией, проходящего по территории государств СНГ, минуя транспортные артерии России, Турции, Ирана приведет к экономического отрыву бывших советских среднеазиатских республик от России и выводу части грузопотока с российской транспортной сети.

Ослабление геополитических и экономических позиций России преследует достижение давней стратегической цели США – устранение с политической арены мира и превращение ее в сырьевой придаток Запада. Направленность этой политики сформулирована в ясных высказываниях его идеологов: секретарь Трехсторонней комиссии З. Бжезинский: "Россия - побежденная держава. Она проиграла титаническую борьбу. И говорить "это была не Россия, а Советский Союз" - значит, бежать от реальности. Это была Россия, названная Советским Союзом. Она бросила вызов США. Она была побеждена. Сейчас не надо подпитывать иллюзии о великодержавности России. Нужно отбить охоту к такому образу мыслей... Россия будет раздробленной и под опекой". Член Трехсторонней комиссии, руководитель "Бнай Брит" Г. Киссинджер: "Распад Советского Союза - это, безусловно,

важнейшее событие современности, и администрация Буша (имеется в виду старшего) проявила в своем подходе к этой проблеме поразительное искусство... Я предпочту в России хаос и гражданскую войну тенденции воссоединения ее в единое, крепкое, централизованное государство". Премьер-министр Великобритании Дж. Мейджор: "...задача России после проигрыша холодной войны - обеспечить ресурсами благополучные страны. Но для этого им нужно всего 50 - 60 млн. человек".

Несмотря на сближение России и США на почве антитеррористической борьбы, никто в Америке не заявил о дезавуации высказываний своих идеологов. Памятуя об этом, Россия должна твердо и последовательно проводить свою стратегию по отношению к международным процессам быстро меняющегося современного мира, по отстаиванию российских интересов в различных регионах планеты.

4.3.2. Информационное обеспечение при подготовке операции

История второй половины XX века показывает, что от конфликта к конфликту, от войны к войне и в мирные периоды информационное противоборство (борьба) государств приобретает все больший масштаб и играет все большую роль в достижении поставленных целей. В XX веке роль информационных факторов усилилась благодаря бурному развитию средств массовой информации. Появление глобальных телекоммуникационных сетей, спутниковых ретрансляторов, всемирной компьютерной «паутины» Интернета сделала информацию доступной до миллионов и миллионов потребителей. Она превратилась в своеобразный продукт массового спроса со своими параметрами ценности и качества, воздействующими на мысли, чувства, мировоззрение, поведение и процесс принятия решений потребителями этого продукта.

Информация стала мощным оружием межгосударственного противостояния, эффективным средством воздействия на личный состав войск и население при подготовке и проведении военных операций. Идет постоянная отработка и совершенствование организационных, методических и технических приемов и средств ведения информационной борьбы, их апробация в ходе подготовки и ведения боевых действий в локальных конфликтах.

Опыт ведения локальных войн и конфликтов подтверждает одну из главных особенностей - *информационная борьба стала неотъемлемой частью боевой операции*. Она организуется и проводится по единому плану в виде заранее планируемых информационных мероприятий. При этом *четко выделяются два этапа борьбы:* до начала боевых действий, проводимого на глобальном и региональном уровнях, в обеспечение задуманной военной операции, и после начала боевых действий, проводимого в обеспечение боевых операций.

На первом этапе (как правило, задолго до начала боевых действий) главные усилия направляются на информационно-психологическую обработку индивидуального и общественного сознания ключевых фигур правительств и населения тех стран, интересы которых затрагивает задуманная к проведению военная акция. Агрессор пытается на этом этапе привлечь на свою сторону как можно больше союзников, втягивая их непосредственно или косвенно в раскручиваемый водоворот конфликта.

Основные задачи, решаемые агрессором на этом этапе, преследуют достижение следующих целей:

- оправдать в глазах мировой общественности агрессивность задуманной акции, прикрываясь громкими лозунгами защиты «общечеловеческих ценностей» от экологической катастрофы, терроризма, права нации на самоопределение, свободы слова и т.д.;
- сформировать коалицию государств (ударный кулак), вооруженные силы которых примут непосредственное участие в нападении на избранную жертву;
- втянуть в конфликт страны региона, расположенные вокруг страны противника; постараться разжечь межрегиональную войну и решить задачу чужими руками, в крайнем случае, заручиться их молчаливым согласием на проведение акции;
- по возможности изолировать противника от международной моральной, финансовой, военной и материальной поддержки; разрушить его союзные договора и обязательства с другими государствами.

К начала конфронтации с Афганистаном США уже имели отработанную и апробированную в боевых условиях единую концепцию информационной войны, которая нашла четкое отражение в армейских уставных документах. В частности, полевой устав армии США FM-100-1 («Ведение боевых действий») устанавливает, что действия частей психологической войны, а также «независимых» средств массовой информации и общественных организаций (фондов, союзов, партий, сект и пр.), осуществляются военным командованием США.

Основными объектами информационно-психологического воздействия до начала агрессии явились правительства и широкая общественность стран НАТО, Россия, страны Ближнего и Среднего Востока, Пакистан.

Ориентируясь на приобретенный опыт, в преддверии военных действий США провели широкомасштабную информационную акцию по воздействию на международную общественность с целью склонения ее на свою сторону и обеспечения международной поддержки курса США в отношении Афганистана. С другой стороны США всячески пытались убедить мировое сообщество в том, что именно эта страна является основной базой международного терроризма, что именно в Афганистане находится осиное гнездо террориста №1 Усамы бен Ладена, которое необходимо уничтожить в первую очередь. Сами талибы представлялись в качестве средневековых варваров, уничтожающих культуру Афганистана, разрушающих экологию пустыни.

Устремления США нашли активную поддержку со стороны Великобритании, вооруженные силы которой совместно с американской стороной и составили основной «ударный кулак» коалиции. (Позднее на саммите ЕС в Бельгии было принято решение о создании многонациональных миротворческих сил ЕС для Афганистана, численностью в 3-4 тысячи военнослужащих. По заявлению главы МИД Бельгии Луи Мишеля, руководство силами взяла на себя Великобритания, а участие в миротворческом контингенте "примут все страны Евросоюза". С конца января 2002 г. военная операция в Афганистане практически перешла в миротворческую фазу, целью которой стало поддержание порядка и охрана важных объектов).

Правительства и общественное мнение, включая Россию, усиленно обрабатывались в целях создания благоприятных условий для размещения ударных сил США и НАТО на прилегающих к Афганистану территориях, включая территории бывших союзных республик СССР. Их усилия не пропали даром. Россия после недолгого колебания согласилась на американское присутствие в зоне ее интересов. Английская газета "The Guardian" отмечает, что по состоянию на начало 2002 г. в Узбекистане была создана постоянная американская военная база в Ханабаде, на которой располагались полторы тысячи военнослужащих. Манас, находящийся неподалеку от киргизского Бишкека, был определен будущим "транспортным узлом", на котором будут размещаться три тысячи солдат, боевые и разведывательные самолеты. Другие аэродромы в Таджикистане и Пакистане также уже находились под контролем Соединенных Штатов. Пентагон к этому времени начал регулярные перемещения и ротацию войск, придавая тем самым постоянный статус контингенту, который первоначально рассматривался как временный, размещаемый на время чрезвычайной ситуации.

Для достижения этих целей Вашингтон использовал не только пропагандистские, но и финансовые и экономические «соблазны». 27.10.01 г. Пакистан получает первую награду за содействие - Буш подписал закон об отмене санкций, наложенных на страну в 1999г., а 29.10.01 г. Госдеп объявил о миллиардной экономической помощи Пакистану. Узбекистан, на который США ранее не обращали внимания, получил в 2001 г. 64 млн. долл. в виде помощи от американского правительства, и 136 млн. долл. в виде кредита "Экпортно-Импортного Банка" США. 01.11.01 г. Азербайджан и Армения предложили расширить права ВВС США на использование их воздушного пространства во время кампании, в ответ на что Администрация Белого дома сразу же предложила снять запрет на военную помощь Азербайджану. 27.11.01 г. Йемен дал согласие на блокирование активов групп, связанных с Аль-Каедой. В ответ Йемен получает 400 млн. долл. экономической и военной помощи. В 2002 г. администрация Буша планировала предоставить Казахстану помощь в размере 52 млн. долл. с частичной оплатой военным оборудованием. Получив от правительств стран региона разрешение строить базы, Соединенные Штаты соглашаются обучать и экипировать местные

силы. Затем обещается экономическая помощь и торговые соглашения. А так как военное сотрудничество обычно осуществляется в обоих направлениях, то присутствие США в непосредственной близости от южных границ России, несомненно, будет носить долговременный характер.

Президент России В.В. Путин согласился (вразрез с советами своих некоторых высокопоставленных генералов) на переговоры с американцами о первой ограниченной военной базе в соседних с Афганистаном странах. Китай также, хоть и возражая принципиально на вмешательство США в дела региона, на деле дал понять, что осознает всю серьезность последствий попыток перечить США. Обе страны надеялись получить выгоды в разных сферах от помощи Соединенным Штатам - и в какой-то мере добились этого. Американцы начали общаться с В.В. Путиным как с партнером, предложив даже более тесное сотрудничество с НАТО. Споры с Пекином по поводу прав человека и торговли, имевшие место после инцидента с разведывательным самолетом на острове Хайнань, были прекращены. Быстро решился вопрос о членстве Китая в ВТО.

На региональном уровне в качестве основных объектов воздействия на этапе подготовки и проведения операции были определены правительство талибов, личный состав вооруженных сил и население Афганистана. Основная цель всех мероприятий сводилась к склонению талибов прекратить сопротивление, к привлечению на свою сторону афганцев, способствовать укреплению Северного альянса противников режима. Особой обработке подверглось правительство Пакистана с тем, чтобы удержать его от поддержки талибов, ликвидировать их базы на территории Пакистана.

Основным рупором информационно-психологической обработки мировой общественности явились современные средства массовой информации, включая Интернет, работе с которыми военно-политическое руководство США уделяло особое внимание. Посредством СМИ центр внимания был сосредоточен на террористической организации "аль-Каида", созданной Усамой бен Ладеном в конце восьмидесятых годов 20-го века с целью объединения арабов, сражавшихся в Афганистане против вторгшихся туда советских войск. Тогда она помогала финансировать, вербовать, транспортировать и готовить суннитских исламских экстремистов для афганского движения сопротивления. После вывода советских войск из

Афганистана «аль Каида» поставила перед собой цель создать во всем мире панисламский халифат путем сотрудничества с союзническими исламскими экстремистскими группировками для свержения режимов, причисляемых ею к "неисламским", и изгнания из мусульманских стран граждан западных государств и немусульман. Главным врагом были объявлены Соединенные Штаты Америки. В феврале 1998 года под знаменем "Всемирного исламского фронта за джихад против евреев и христиан" организация распространила заявление, в котором говорится, что долг всех мусульман - убивать повсюду граждан США, будь то гражданские лица или военные, и их союзников.

Деятельность "аль-Каида", описывалась в СМИ как особо опасной для всех стран мира, ибо она действует во всем мире, имеет ячейки в ряде стран и получает поддержку со стороны экстремистских суннитских сетей. Она служит координационным центром всемирной сети, в которую входят многие суннитские исламские экстремистские группы, такие как "Египетский исламский джихад", некоторые члены "аль-Гамаат аль-исламийа", "Исламское движение Узбекистана" и "Харакат уль-муджахидин". Со ссылкой на Центральное разведывательное управление в СМИ утверждалось, что на территории Афганистана за последние годы было подготовлено не менее 50-70 тыс. боевиков из 55 стран. Талибы разрешали действовать на афганской территории широкому кругу групп - от пакистанских мятежников до подчиненной бен Ладену организации "аль-Каида", что по-арабски означает "База". Сам бин Ладен и его главные помощники проживали на территории Афганистана, там же содержалась сеть лагерей для подготовки террористов. Здесь боевиков учили обращаться со стрелковым оружием и взрывчатыми веществами, готовить террористические акты.

В СМИ широко освещалась хронология терроризма с целью возбудить недовольство общественности к деятельности "аль-Каида". «Раскрутка» в СМИ злодеяний этой организации началась с событий декабря 1992 года, когда прогремели три взрыва, целями которых явились дислоцированные в Адене (Йемен) войска США. Потом вспомнили о сбитых американских вертолетах и убийстве американских военнослужащих в Сомали в 1993 году, о сорванных планах осуществить террористические акции против американских и израильских туристов, приехавших в Иорданию для

празднования наступления нового тысячелетия. (Иорданские власти сорвали запланированные нападения и предали суду 28 подозреваемых.) Особо остро подавался материал августа 1998 года, когда "аль-Каида" организовала и осуществила взрывы в посольствах США в Найроби (Кения) и Дар-эс-Саламе (Танзания), в результате которых погиб по меньшей мере 301 человек, а еще более 5 тыс. человек получили ранения. Проамериканская пресса вспомнила и о причастности "аль-Каида" к подготовке следующих терактов, которые не были осуществлены: убийство Папы Римского Иоанна Павла II во время его визита в Манилу в конце 1994 года, одновременные взрывы в посольствах США и Израиля в Маниле и других столицах азиатских стран в конце 1994 года, взрывы на борту более десяти американских самолетов над Тихим океаном в 1995 году, убийство Президента Клинтона во время его визита на Филиппины в начале 1995 года.

События 11 сентября 2001 года вызвали буквально взрыв активности СМИ вокруг тематики терроризма. Западная пресса, как и руководство США, не предоставила общественности никаких доказательств вины Усамы бен Ладена, мусульманских террористов, но сразу же, по существу, "назначило" виновных и стало готовить общественность к широкомасштабной антитеррористической операции.

С целью усиления координации деятельности федеральных министерств и ведомств по информационному освещению событий, Администрацией США был предпринят ряд мер, направленных на ограничение доступа к ряду информационных источников о ходе афганской кампании. Все права на трансляцию любых кадров из Афганистана были выкуплены представителями федерального правительства; в ряде СМИ была введена жесткая цензура; предпринимались попытки дипломатического давления на руководство Катара с целью закрыть телекомпанию Аль-Джазира. Против нее в ряде западных СМИ была развернута широкая пропагандистская кампания, призванная очернить ее репутацию связями с террористами.

Как сообщала газета Washington Post, 24 сентября 2001 года пресс-секретарь Белого дома Ари Флейшер лично обзвонил руководителей и главных редакторов всех ведущих эфирных телекомпаний США, газет New-York Times, Washington Post, Wall Street Journal и ряда других СМИ с

просьбой ограничить информацию о готовящейся в США военной операции против террористов. Флейшер просил также руководителей СМИ о том, чтобы телекомпании и газеты не сообщали график работы и перемещений президента США Джорджа Буша и вице-президента США Ричарда Чейни.

Президент США Джордж Буш также заявил, что теперь огласке не подлежат и сведения об источниках и методах сбора разведывательной информации, которую США получают для операции против террористов. "Я ставлю следующее условие прессе: любые источники разведданных и методы получения сведений разглашаться не будут. Моя администрация не будет рассказывать о том, как мы получаем секретную информацию, получаем ли мы информацию, и что нам стало известно. Это необходимо для защиты американских граждан".

Во время войны, заявил Флейшер, "администрация обязана предоставлять всю ту информацию, которая делает страну сильной, и в то же время мы должны быть уверены, что ни один обнародованный факт не приведет к потери жизней или срыву специальных операций".

Во исполнение указаний администрации Белого дома, по сообщению газеты The Washington Post от 1.11.01 г., председатель правления крупнейшей телекомпании CNN Уолтер Исаксон выпустил внутреннее распоряжение по телекомпании, в котором предписал своим сотрудникам не слишком фокусировать внимание на потерях среди населения или разрушениях в Афганистане, вызванных военными действиями США. Глава CNN сообщил, что все материалы о ситуации в Афганистане должны быть уравновешены информацией о том, что талибы используют людей в качестве "живых щитов" и укрывают террористов, которые были организаторами терактов в США. "Мы должны удвоить наши усилия, чтобы мы не выглядели передающими информацию, отражающую их (талибов) точку зрения или выгодную им, - говорится в распоряжении Исаксона. - Американские телезрители должны воспринимать страдания мирных жителей в Афганистане в контексте теракта, который вызвал огромные страдания в США". По его словам, CNN не должна использоваться талибами в роли "пропагандистской трибуны".

Проводимые США информационно-психологические операции не исключали и своей стороны. Примечательно, что бомбардировка горных массивов, в которых скрывалось ближайшее окружение Усамы Бен Ладена, проводилась преимущественно ночью, хотя ничто не мешало американцам с большей точностью выполнять их днем. Причина одна – разница во времени: когда в Америке день, в Афганистане ночь. Ночные кадры «наказания террористов», передаваемые в прямых репортажах с поля событий, могли видеть бодрствующие американские телезрители. Это внушало им гордость за мощь своей страны и способствовало укреплению патриотизма.

Однако в своем усердии американские СМИ замалчивали и замалчивают сегодня причастность самой Америки к возникновению террористических группировок на территории Афганистана. Об этом упоминает Анютин Юлиан в Информационно-аналитическом обзоре «Направленность, причины и цели кампании, связанной с событиями в США 11 сентября 2001 года». Оказывается, что еще в конце 80-х ЦРУ, через свою агентуру из числа сотрудников ООН в лагерях афганских беженцев на территории Пакистана, провело учет и отбор военных и гражданских специалистов, необходимых для организации административных и силовых государственных структур Афганистана. В это же время была организована подготовка вооруженных групп и отрядов пуштунов при помощи пакистанских и арабских военных инструкторов, которая финансировалась спецслужбами и проправительственными пакистанскими религиозными организациями "Джамаат-э-ислами" и "Джамаат-э-улема-э-Пакистан", а также спецслужбами США, пакистанскими и международными фундаменталистскими организациями. Идея сменить вывеску для объединения афганских племен, прекратить внутреннюю войну и перенести ее вовне с использованием движения послушников медресе принадлежала ЦРУ, финансировалась шейхами, а оружием обеспечивалась из Пакистана. Так, из представителей пуштунской национальности летом 1994 года была сформирована военизированная группировка во главе с одним из афганских духовных лидеров муллой Сеид Мухаммад Омаром (Ахундзада), которая и получила название Исламское движение Талибан.

Нынешний враг номер один бен Ладен полтора десятилетия назад был другом Америки номер один. Под руководством наставников из ЦРУ

представитель богатейшей семьи из Саудовской Аравии стал организатором исламского сопротивления СССР в Афганистане. Потом бен Ладен стал противником США. Но при этом некоторые братья "террориста номер один" преспокойно проживали в США и хранили свои миллиарды в известных американских и европейских финансовых учреждениях.

Отец нынешнего президента США Дж. Буш-старший, бывший госсекретарь Дж. Бейкер, бывший министр обороны Фр. Карлуччи в разное время побывали в штаб-квартире семьи Усамы бен Ладена в Джидде (Саудовская Аравия). Эти известные в мире люди тесно связаны с крупным инвестиционным банком Вашингтона Carlyle Group (эта группа имеет прямое отношение к военно-космической промышленности США), в котором семья бен Ладенов располагает немалым пакетом акций. В 1995 г. семья бен Ладенов инвестировала в Carlyle Group два миллиона долларов.

Усама бен Ладен обследовал и лечил почки в американском госпитале в Дубаи, куда он прибыл 4 июля 2001 г. из Пакистана. Во время нахождения в госпитале бен Ладена посещал региональный представитель ЦРУ. Сразу же после отъезда бен Ладена 14 июля встречавшийся с ним офицер американской разведки был вызван в Вашингтон. (Это сообщение, появившееся во французской газете "Фигаро", было опровергнуто ЦРУ).

Таковы факты. Их сопоставление наводит на мысль, что за разрекламированной СМИ операцией "Бесконечная свобода" стояли иные геополитические планы и стратегические задачи США.

4.3.3. Характер и особенности информационной войны в Афганистане

Формальная процедура в подготовке к военным действиям в Афганистане завершилась 18.09.01 г. Буш подписал резолюцию Конгресса о применении вооруженных сил и выделении средств на борьбу с терроризмом.

В этот же день министр обороны США Рамсфельд заявил, что *США столкнулись с совершенно новым типом конфликта,* так как сеть "аль-Каида" связана с 50-60 странами, что требует проведения широкомасштабной операции.

На следующий день министр иностранных дел России И.Иванов заявил о согласии на привлечение к военной операции бывших среднеазиатских республик. Формальное согласие подчеркивало участие России в международной коалиции, несмотря на то, что присутствие войск НАТО явно противоречит интересам России в Среднеазиатском регионе.

Подготовка к военной операции "Бесконечная свобода" началась с развертывания воздушных сил в Саудовской Аравии, Омане, Кувейте, острове Диего Гарсия, Таджикистане и Узбекистане. Отряд из 14 кораблей во главе с авианосцем "Теодор Рузвельт" направился в Персидский залив. Япония заявила о разведывательной и транспортной поддержке. Организация Американских государств задействовала Межамериканский договор о взаимной помощи 1947 г. (Rio Treaty). Канада для операции предоставила 2000 военнослужащих и 6 кораблей, Австралия - 1000 солдат, Франция - военно-морской флот в Индийском океане.

07.10.01 г. американские и британские бомбардировщики и крылатые ракеты атаковали позиции Талибана. Тридцать первых целей включали аэродромы, систему ПВО, лагеря подготовки и группы, противостоящие Северному Альянсу. А уже 09.10.01. генерал Меерс сообщил, что США добились полного контроля над воздушным пространством Афганистана. В последующих действиях для поражения намеченных целей использовались многоцелевые истребители F-15E, тяжелые бомбардировщики B-52. Во время бомбардировок пещерного комплекса Тора-Бора было применено одно из наиболее мощных видов оружия - 15000-фунтовая бомба BLU-82 "Daisy Cutter" и специальные бомбы с лазерным наведением.

Для информационно-технического обеспечения войск армия США использовала и беспилотные самолеты нового типа Predator" и "Global Hawk". Беспилотный летательный аппарат (БЛА) "Predator" может вести не только воздушную разведку, но и атаковать обнаруженную наземную цель противотанковой управляемой ракетой "Hellfire". На малых высотах БЛА незаменим при решении задач нарушения системы боевого управления противника, поскольку от его электронных глаз не могли укрыться даже малочисленные группы бойцов движения "Талибан" и террористов "Аль-Каиды". БЛА ВВС США "Global Hawk", воздушный разведчик, способен совершать полет на высотах более 20000 метров над землей. Однако при всех

их многообещающих возможностях БЛА не лишены недостатков: "Predator" плохо «видит» наземные объекты в плохих погодных условиях. Кроме того, эта машина стоимостью 3,2 млн. долл. имеет неприятную привычку внезапно устремляться к земле, когда никто этого не ожидает. Что касается высотного самолета-разведчика "Global Hawk", то из-за катастроф двух машин стоимостью 40,6 млн. долл. каждая весь парк этих БЛА больше сидит на земле в ожидании результатов расследования причин катастроф, чем летает.

В Афганистане армия США впервые апробировала солдата-робота в боевой обстановке. Радиоуправляемый солдат-робот, весом в 40 фунтов, «учится» выполнять функции разведчика при обследовании пещер или подозрительных помещений. Он может взбираться по лестничным маршам в здании, делать кульбиты и перемещаться со скоростью до 9 миль в час. Ударопрочный и водонепроницаемый корпус выдерживает попадание пуль и падение на землю из окна второго этажа. В перспективе планируется модернизировать солдата-робота, оснастив его подвижной рукой с видеокамерой, чтобы можно было приподнимать ее повыше, увеличивая дальность обзора, а также низкочастотной радиорелейной системой связи, которая улучшит его навигационные возможности при действии в пещерах. Кроме того, рассматриваются варианты вооружения солдата-робота, например, гранатометом или двуствольным полуавтоматическим ружьем. Стоимость робота в 40000 долл. считается приемлемой, так как он может предотвратить гибель солдата в бою. Пентагон ассигновал на программу разработки солдат-роботов, способных выполнять опасные для жизни задания, 50 млн. долл.

В Афганистане информационно-техническая борьба активно не велась из-за отсутствия у талибов мощной системы ПВО и сложных систем вооружения. Сразу же после начала боевых действий бен Ладен призвал всех мусульман к джихаду против США. Поэтому информационная борьба в дальнейшем сосредоточилась в основном в сфере информационно-психологического противоборства. *Характер этой борьбы со стороны агрессора отличался бескомпромиссностью, целеустремленностью, последовательностью, глобальностью, скрытностью истинных целей операции.* Талибы не смогли оказать противнику заметного информационно-психологического противостояния.

Основные особенности информационно-психологической борьбы, осуществляемой США и их союзниками в ходе подготовки и проведения войны в Афганистане, заключаются в следующем:

- информационная борьба организовывалась и проводилась по единому плану в виде заранее планируемых мероприятий, как правило, задолго до начала боевых действий;
- четко выделяются два этапа информационно-психологической борьбы:
  - до начала боевых действий, проводимый на глобальном и региональном уровнях, в обеспечение задуманной военной операции;
  - после начала боевых действий, проводимый в обеспечение боевых операций;
- руководство подготовкой и проведением информационно-психологической борьбы осуществлялось централизовано уже существующими гражданскими и военными структурами информационного противоборства в тесном взаимодействии между собой и соответствующими структурами своих союзников;
- эти структуры руководствовались уже отработанными уставными документами;
- особое внимание уделялось взаимодействию со средствами массовой информации, направляя распространение сведений и их освещение в выгодном для себя свете.
- основными объектами информационно-психологического воздействия до начала агрессии на геополитическом уровне явились правительства и широкая общественность стран НАТО, Пакистан, Россия, страны Ближнего и Среднего Востока.

Основными задачами, решаемыми агрессором на этом этапе, являлись:

- оправдание в глазах мировой общественности агрессивности задуманной акции;
- прикрытие истинных планов громкими лозунгами защиты «общечеловеческих ценностей»;

- укрепление коалиции государств союзников, привлечение их экономических и военных ресурсов для операции;
- втягивание в конфликт стран региона, расположенных вокруг страны-жертвы; разжигание межрегиональной розни и противоречий;
- изоляция противника от международной моральной, финансовой, военной и материальной поддержки;
- разрушение его союзных договоров и обязательств с другими государствами;

- на региональном уровне в качестве основных объектов информационно-психологического воздействия на этапе подготовки и проведения операции были определены правительство талибов, личный состав вооруженных сил и население Афганистана. Основными задачами этого уровня являлись:
  - устрашение противника военной мощью коалиции и боевыми возможностями суперсовременных средств поражения;
  - склонение талибов прекратить сопротивление и сдаваться в плен;
  - привлечение на свою сторону афганцев и населения региона;
  - укрепление северного альянса противников режима;
  - удержание правительства Пакистана от поддержки талибов;
  - ликвидация их базы на территории Пакистана.

В ходе подготовки и проведения операции «Бесконечная свобода» талибы были разбиты. По официальной информации Государственного департамента США, *результатом этой операции стало следующее*:

- Военная операция в Афганистане стала итогом усилий глобальной коалиции, участниками которой были вооруженные силы США, Великобритании, Австралии, Канады, Чехии, Франции, Германии, Италии, Японии, Новой Зеландии, Польши, России и Турции.
- Силы коалиции освободили афганский народ от насильственного режима Талибана. Коалиция достигла широкого военного успеха, задействовав в активных наземных операциях менее 3000 солдат.

- В считанные недели была практически разрушена сеть "аль-Каида" в Афганистане, а Талибан сдал основные афганские города, такие как Кандагар, Кабул, Кундуз, Мазари-Шариф.
- Были разрушены по меньшей мере 11 тренировочных лагерей террористов и 39 талибских командных и контрольных баз, на которых на протяжении последних лет прошли подготовку около 50000 террористов из более чем 50 стран.

Однако Джордж Буш неоднократно подчеркивал, что главная цель операции "Бесконечная свобода" заключается в том, чтобы Усама бен Ладен, его основные соратники из «аль-Каиды», а также члены правительства талибов предстали перед судом. С этой точки зрения результаты можно считать нулевыми. Режим талибов свергнут, но среди пленных и погибших в основном рядовые боевики. Среди погибших высокого ранга оказался только мулла Абдул Джалил, занимавший пост заместителя министра иностранных дел. Глава министерства Вакиль Ахмед Мутавакиль - жив, местонахождение его неизвестно. Министр обороны Обайдулла Аджам, которого считают самым близким к бен Ладену человеком среди талибов - тоже. Тайебе Агха, представитель духовного лидера талибов, покинул Кандагар с колонной вооруженных лиц. Исчез Амир Хан Муттаки, который занимал пост министра информации и культуры, а затем и образования. Ахмад Тураби и Нур Мухаммад Сакиб - самые радикальные члены Верховного совета Талибана - перешли через границу и обосновались в Пакистане. О судьбе самого муллы Омара неизвестно вообще ничего. Но в начале декабря 2002 г. катарская телекомпания Аль-Джазира стала регулярно передавать получаемые ею записи муллы с угрозами в адрес американцев по поводу назревающей агрессии США против Ирака.

Что касается «аль-Каиды», то здесь ситуация аналогична. Усама бен Ладен сумел скрыться. Высокая награда за голову бен Ладена (25 млн. долларов от правительства и 2 млн. от Ассоциаций пилотов и воздушного транспорта) и его сподвижников (также по 25 млн. долларов) не принесла результатов. Единственным высокопоставленным руководителем «аль-Каиды», погибшим во время операции, стал Мухамад Атеф, который руководил военными операциями этой организации. Впрочем, подтверждения этому не найдено, и он по прежнему числится среди наиболее

разыскиваемых террористов, а за информацию о нем обещана награда. Не найден главный идеолог Айман аль-Завахири, являющийся основателем "Исламского джихада" и правой рукой бен Ладена, хотя предполагают, что его семья погибла под американскими бомбами. Нет никаких следов, которые могли бы вывести на Абу Зубайдаха, еще одного близкого соратника бен Ладена.

К результатам операции можно отнести разгром лагерей подготовки террористов. Однако вряд ли стоит переоценивать значение для международного терроризма именно афганских лагерей. Во-первых, в регионе с перманентно продолжающейся войной большинство жителей с детства готовы к вооруженной борьбе. Во-вторых, подобные лагеря могут быть организованы в огромном количестве в других регионах земного шара, а контролировать всю планету невозможно даже силами анитеррористической коалиции. И, наконец, для современного терроризма совсем не обязательно готовить тысячи боевиков. Для нанесения серьезного ущерба достаточно десятка хорошо обученных фанатиков, которых невозможно отличить от законопослушных граждан (свидетельством этому - теракты 11 сентября).

Наиболее важным итогом операции для России является очевидная утрата российских позиций в Средней Азии. Завершая свой визит в Узбекистан, лидер сенатского большинства в конгрессе Том Дэшл прямо заявил: "Мы будем наращивать наше присутствие здесь в целях отстаивания интересов США в Средней Азии. Наше присутствие в регионе отныне носит долговременный характер, и с правительствами стран Средней Азии на этот счет уже существует необходимый уровень доверия". 12.02.02 г. США в очередной раз продемонстрировали свое полное пренебрежение мнением других государств. Представитель Белого дома Ари Флейшер заявил, что США могут подыскать себе других партнеров по антитеррористической коалиции в случае возникновения разногласий с президентом Владимиром Путиным по вопросу о принятии мер против стран, причисленных Вашингтоном к "оси зла". Флейшер предупредил, что "могут быть созданы различные коалиции с разными странами и для разных целей".

Очевидно и снижение уровня военной безопасности России. Возможное развертывание баз в Узбекистане, в других азиатских бывших советских

республиках, в северных провинциях Афганистана может снять необходимость создания НПРО США. Высокоточные ракеты средней дальности, размещенные на территории данных баз, перекрывают всю российскую территорию до Северного Ледовитого океана. Под прицел попадают все пусковые установки наших стратегических ракет.

Расширение контингента НАТО в бывших советских республиках, а также недвусмысленные и достаточно резкие высказывания американских политиков только подчеркивают сегодняшнюю слабость России и ее невозможность отстаивать свои долгосрочные геополитические интересы.

4.4. Анализ деятельности сторон по организации и ведению информационной войны в ходе агрессии коалиционных сил против Ирака[89]

Изучение и анализ доступной информации о деятельности сил коалиции в период подготовки и проведения агрессии против Ирака позволяет сделать вывод о том, что в возможных конфликтах текущего десятилетия роль и место сил и средств информационного воздействия и защиты будет постоянно возрастать.

Об этом, в частности, говорит масштаб развернутой США и странами коалиции информационно-психологической кампании в мировых СМИ в период подготовки и осуществления агрессии против Ирака.

Прежде всего, планированию операции против Ирака предшествовало детальное изучение общественного мнения и ситуации в регионе в целом.

4.4.1. Деятельность администрации США по изучению социально-политической и психологической обстановки в регионе

Результатом одного из таких исследований стал отчет, подготовленный корпорацией RAND – одним из ведущих аналитических центров администрации США. Отчет был подготовлен по заказу командования военно-воздушных сил США. Цель выполненных работ – до начала военной операции США против Ирака проанализировать развитие военно-

[89] Раздел подготовлен с использованием материалов ряда российских Интернет-изданий: Страна.ru, Lenta.ru, SMI.ru, RBC.ru, а также информационных сайтов www.iraq.ru и www.iraq-war.ru, на страницах которых активно обсуждался ход агрессии против Ирака.

политической и военно-стратегической обстановки в регионе Персидского залива, выявить тенденции развития, основные факторы, влияющие на стабильность региона в ближайшие десять лет.

Важным является оценка аналитиков RAND, согласно которой угроза применения военной силы в зоне Персидского залива на момент начала акции силами антииракской коалиции со стороны любой из стран региона была минимальной. По прогнозам специалистов, Ирак даже в случае, если Саддам Хуссейн останется у власти, в ближайшие годы не смог бы угрожать своим соседям, потому что его вооруженные силы находились в очень плохом состоянии. Причиной этого стали двенадцатилетние санкции ООН.

Вместе с тем, экспертами был сделан вывод о том, что рост экономических, социальных и политических проблем в регионе может уже в ближайшие годы поставить страны Персидского залива в трудное положение. Учитывая то, что реформы в большинстве этих государств маловероятны, вполне возможно, что в ближайшие 10 лет страны этого региона столкнутся с очередным серьезным кризисом. В связи с этим RAND рекомендовал администрации США резко уменьшить военное присутствие в регионе Персидского залива, чтобы не давать местным режимам возможность направлять общественное недовольство против американцев. Однако высшее военно-политическое руководство США впервые за много лет не прислушалось к мнению авторитетных экспертов в вопросе ближневосточной политики.

Вместо этого, учитывая неблагоприятный характер складывающейся обстановки, администрация США за несколько месяцев до начала агрессии приступила к наращиванию усилий в области подготовки и ведения информационно-психологических операций, направленных на поддержание имиджа США в условиях масштабной антитеррористической операции, проводимой США главным образом в исламских государствах.

Причиной, побудившей представителей администрации США и руководство Пентагона начать реализацию масштабной программы психологического влияния на мировое общественное мнение, стали результаты ряда социологических исследований, проведенных независимыми

компаниями более чем в 40 странах мира и показавшими повсеместный рост антиамериканских настроений.

Согласно проведенных опросов к концу 2002 года уже 19 стран мира, демонстрировали рост антиамериканских настроений и падение показателя благожелательного отношения. Так за последние три года благоприятный рейтинг США в Западной Европе устойчиво снижался и упал на 5-6 процентных пункта. В Турции - на 22 пункта, а в Пакистане - на 13. В Египте сегодня хорошо относятся к США всего 6 процентов населения. Отрицательно оценивают распространение американской идеологии 50 процентов опрошенных в Великобритании, в Германии - 67 процентов, в России - 68 процентов, во Франции - 71 процент. Особенно сильны антиамериканские настроения на Ближнем Востоке: в Турции - 78 процентов, в Пакистане – 81 процент, в Египте - 84 процента. Оказался очень высок процент мусульман, поддерживающих теракты-самоубийства в защиту ислама: 73 процента в Ливане; 43 процента в Иордании; 44 процента в Бангладеш; 47 процентов в Нигерии; 33 процента в Пакистане; 27 процентов в Индонезии, что свидетельствовало о значительном потенциале смертников-террористов, который может быть реализован, в том числе, и против США в случае начала военной акции в какой-либо мусульманской стране.

Ответом администрации США и Пентагона на столь внушительный рост антиамериканских настроений у значительной части населения планеты стала подготовка нового плана информационно-психологических мероприятий, направленных на манипуляцию мировым общественным мнением. Причем программой предусматривалось проведение мероприятий не только в потенциально враждебных США государствах, но и в государствах-союзниках, что значительно расширяет трактовку определения информационной операции, данное в известной министра обороны директиве 3600.1 «Информационные операции».

4.4.2. Подготовка сторон к ведению информационной борьбы

Основой новой программы стало создание сети мечетей и исламских школ, а также выплата значительных гонораров европейским журналистам за подготовку проамериканских материалов и компаниям, специализирующимся в области связей с общественностью, - для

организации проамериканских манифестаций в странах с низким рейтингом США.

В феврале 2003 года указом президента США было воссоздано управление Пентагона, отвечающее за организацию и проведение информационно-пропагандистских мероприятий в период проведения антитеррористической кампании, включая агрессию против Ирака. Ранее это управление было известно под названием «Офис стратегического влияния», однако после широкого протеста в средствах массовой информации, руководством Пентагона было принято решение о временном прекращении функционирования этого управления. Однако уже в феврале этого года управление было воссоздано, но уже под другим названием – «Офис глобальных коммуникаций». Вместе с тем, как отмечает ряд экспертов, цели и задачи, а также методы работы нового офиса остались прежними – управление восприятием целевой аудитории, в качестве которой рассматривается высшее военно-политическое руководство стран Азии, Ближнего и Среднего Востока, а также Западной Европы.

Большая роль отводилась новому проекту по созданию «Ближневосточной телевизионной сети» (MTN, Middle-East Television Network), возглавляемой Норманном Паттизом. Н.Паттиз является членом Совета управляющих радиовещания США (BBG, U.S. Broadcasting Board of Governors). Он также является член консультативного правления Центра ближневосточной политики корпорации RAND.

Реализация проекта создания MTN, как основного конкурента катарской телекомпании «Аль-Джазира» была начата с создания радиостанции SAWA. Основная аудитория радиостанции – арабская молодежь в возрасте до 25 лет (около 65 процентов населения арабских стран) в странах Ближнего Востока (Амман, Иордания. Кувейт, ОАЭ, Катар, Египет, Ливан, Ирак). Проведенный опрос слушателей радиостанции в Иордании показал, что за счет своеобразия репертуара музыки и грамотной подачи новостей радиостанции удалось занять 35 процентов аудитории, в то время как BBC в этой стране слушают только 5 процентов.

Как отмечают эксперты, одним из существенных достижений передач радиостанции SAWA явилась продуктивная работа по подмене ряда понятий,

характерных современной арабской молодежи. Так активно проповедуется замена понятия «мученическая смерть», почитаемого исламом, на «самоубийство», которое исламом строго запрещено.

Кроме этого в последнее время увеличилось вещание и ряда других радиостанций, таких как «Свободный Ирак».

До начала активной фазы операции Пентагоном была разработана информационная стратегия, которая, по мнению ряда экспертов, являлась беспрецедентной по своему охвату и координации.

Так, ежедневно до начала утренних информационных программ на американском телевидении пресс-секретарь Белого дома Ари Флейшер должен был проводить по телефону селекторный брифинг для главных телекомпаний.

После этого также по телефону с его участием должно было проводиться ежедневное внутреннее селекторное совещание руководства пресс-службы Белого дома с участием пресс-секретарей госдепартамента и Пентагона Ричарда Баучера и Виктории Кларк, а также пресс-секретаря премьер-министра Великобритании Тони Блэра Алистера Кэмпбелла.

Также ежедневно в штабе Центрального командования в Катаре планировался брифинг для прессы, приуроченный по времени к полуденным новостным программам на американском телевидении.

Ежедневный брифинг в Пентагоне по ходу военной операции проводился во второй половине дня, чтобы информация сразу попадала в главные вечерние выпуски телевизионных новостей.

Ряд высокопоставленных фигур администрации, включая советника президента США по национальной безопасности Кондолизу Райс, по мере необходимости также должны были проводить оперативные брифинги. Они также должны были быть готовы давать интервью, прежде всего, для арабских СМИ.

Схема скоординированной информационной работы администрации, разработанная специально для войны с Ираком, была одобрена президентом США Джорджем Бушем.

Агрессию против Ирака должны были освещать более 500 американских журналистов. Все корреспонденты были предупреждены о том, что работа средств массовой информации подлежит контролю в соответствии с правилами, применяемыми во время проведения военной операции.

Для журналистов, освещающих ход военных действий были установлены следующие правила работы.

Основные правила.

- Все интервью с военным персоналом должны записываться на магнитофонную пленку.
- Интервью с пилотами и экипажами самолетов могут проводиться только по окончании полетов.
- Временные ограничения для прессы, включая запрещение съемок и репортажей, могут устанавливаться из соображений безопасности.
- Ограничения будут отменяться сразу после решения проблемы безопасности.

Информация, разрешенная для публикации.

- Информация об объектах, которые подверглись бомбардировкам.
- Общее описание наземных баз.

Информация, не подлежащая публикации.

- Особая информация о количестве развернутых судов.
- Наименования и места расположения особых формирований.
- Информация о наступательных операциях.
- Информация об операциях, которые были отменены или отсрочены.

Отличительной особенностью конфликта в Ираке стало то, что впервые за время использования информационной войны в военных конфликтах министром обороны США Д. Рамсфелдом был поставлен вопрос о необходимости распространения Гаагских конвенции по правилам и нормам войны и на информационную сферу, определяющие правила ведения современных войн, распространяются на все их составляющие. Одно из правил — «принцип эскалации». Это означает поэтапный ввод средств

электронной войны. Так, еще до начала конфликта был проведен ряд специальных информационно-технических операций по блокированию зарубежных счетов Саддама Хусейна и его семьи. Поэтому Пентагон, несмотря на сомнения в правовом аспекте этой акции, уже осуществляет специально разработанные планы вторжения во внутренние сети ряда банков, в том числе и зарубежных.

Следует отметить, что ранее военно-политическое руководство США игнорировало любые предложения, направленные на установление любого контроля над приемами и методами ведения информационной войны. В частности были проигнорированы инициативные шаги России по подготовке специальной резолюции Генеральной Ассамблеи ООН.

План применения средств информационного воздействия в ходе эскалации конфликта был проработан специальной группой специалистов-компьютерщиков Пентагона. Одна из целей — отключение системы энергоснабжения Ирака, для того чтобы парализовать большую часть военных объектов. При этом речь шла как о вирусах, внедряемых через компьютерные сети, так и об электронном вторжении с воздуха по каналам радиосвязи. Самолеты ЕС-130 при помощи СВЧ-излучения проводили попытки отключить серверы иракской службы ПВО и компьютеры военной и гражданской инфраструктур. Ряд военных аналитиков отмечает, что соответствующие испытания радиоэлектронного оборудования для этих целей были проведены за несколько месяцев до начала конфликта и полностью устроили американских военных.

Доступ к военным информационным сетям, через которые американские военные организовывали внедрение вирусов, был облегчен тем, что большинство программ для них писались в самих США.

Следует отметить, что еще до начала конфликта была увеличена роль информационно-психологических мероприятий. При этом отчетливо проявилось смещение роли в проведении подобных операций от ЦРУ и Госдепартамента к Пентагону.

По мнению ряда зарубежных военных экспертов, во многом судьба Ирака была решена уже к 14 марта текущего года – за неделю до начала активной фазы операции, когда завершились переговоры представителей

американского командования с рядом высших чиновников администрации Ирака. Предполагается, что в ходе этих переговоров было получено согласие со стороны некоторых высокопоставленных иракских чиновников о быстрой сдаче ряда крупных населенных пунктов и о сохранении нефтяной инфраструктуры страны сразу после начала агрессии.

Вместе с тем, несмотря на то, что администрацией США был принят целый ряд мер, направленных на завоевание информационного превосходства, первые дни конфликта показали, что достичь этого им не удалось – иракское руководство достаточно успешно противостояло информационной агрессии США, а зачастую и активно контратаковало.

4.4.3. Деятельность сторон по ведению информационной борьбы в ходе агрессии

Иракское командование внимательно изучило опыт военных операций США в Сомали, Афганистане, Ливане и Вьетнаме. В результате Багдад пришел к выводу ***о возможности эффективно бороться с противником, обладающим абсолютным военным, экономическим, политическим и финансовым преимуществом***.

Центральным звеном оборонительной концепции иракского руководства являлось создание условий для образования всенародного движения сопротивления американским и британским войскам. Достигнуть этого Багдад намеревался за счет затягивания военных действий и переноса основных боев в крупные города. Также активно использовался и религиозный фактор: агрессия представлялась как очередной «крестовый поход» против ислама. Удачным также можно считать принятое решение о воссоздании тайного исламского религиозного ордена ассасинов, активно боровшихся с крестоносцами средних веков. Члены этого ордена – федаины – составили отборные подразделения специального назначения Республиканской Гвардии Ирака.

Серьезным успехом иракских сил стало поддержание устойчивой связи военно-политического руководства страны с армейскими частями в условиях активного радиоэлектронного и огневого подавления систем управления со стороны противника.

Этому способствовало то, что Ирак имел современную волоконно-оптическую сеть связи. Она начала создаваться еще во время войны с Ираном, и к настоящему времени в ее развитие вложены большие средства. Наличие сети связи на основе волоконно-оптических линий связи значительно повысило устойчивость управления к воздействию со стороны средств РЭБ.

Рисунок 23.Оперативные пресс-конференции иракского министра информации - удачный ход иракцев в информационной войне с коалицией

Также удачно была организована связь и с мировой общественностью посредством регулярных пресс-конференций и относительно свободной работы журналистов в Ираке. Успешными можно считать и регулярные пресс-конференции руководства Министерства информации Ирака для иностранных журналистов.

США также строили свою стратегию на завоевании поддержки широких масс Ирака, которые должны были восстать против режима Саддама Хусейна при вступлении американо-британских войск и тем самым привести к быстрой и легкой победе. Однако этого не произошло. Более того, эксперты считают, что Саддаму Хусейну в большинстве случаев удавалось «переиграть» американское командование в самом главном - усилении антиамериканских настроений среди населения страны и за ее пределами.

Признаком растущего отчуждения между народом Ирака и американскими войсками стало, в частности, изменение процедуры контактов военнослужащих США с местным населением. В отличие от первых нескольких дней войны американские военнослужащие в последующем останавливали любую приближающуюся к ним группу людей или машину и проводили длительные обыски. Это было вызвано тем, что небольшие группы иракской армии, переодеваясь в гражданскую одежду, начали атаковать американские части, используя зачастую и гражданские автомобили.

Рисунок 24.Ракетный удар по министерству информации Ирака – признание эффективности его работы

В условиях дефицита реальной информации с театра военных действий, завесы секретности, которая окружает цифры потерь и местоположение сражающихся частей, косвенным показателем оценки ситуации служил сам характер военной пропаганды, которую Пентагон предоставлял в качестве официальных сводок.

Характер этих сообщений в первые дни войны свидетельствовал о некоторой растерянности американского командования, отсутствии четкой информационной политики, а также о провалах на фронте, которые оказались неожиданностью для структур, занятых информационным освещением событий. Пресс-служба Пентагона не располагала заготовками, которые можно было использовать, чтобы снять негативное впечатление от военных неудач, что служило поводом для распространения слухов.

Путаница с расстоянием, якобы отделяющим передовые американские части от Багдада, заявления о взятых населенных пунктах, которые повторялись в последующие дни, дезавуируя тем самым предыдущие заявления, разнобой в цифрах признаваемых потерь, наконец, неуклюжие протесты по поводу демонстрации военнопленных иракским телевидением (при том, что США начали с первого же дня показывать некую группу штатских, объявленных «иракскими военнопленными») – все это говорит о том, что уровень информационного контроля над ситуацией в иракской кампании существенно отличался в худшую сторону от информационных возможностей, проявленных коалицией в 1991 году.

Причина этого, по мнению ряда экспертов, может исходить из деморализации среднего звена американской военной администрации, отвечающей, в том числе, и за «развитие общественных связей». Для этого, по мнению экспертов, есть три причины.

Первая и наиболее очевидная – это плохая подготовленность всей операции, спланированной авантюрно, в расчете на массовую капитуляцию иракцев и военный переворот против Саддама. Провал этих ожиданий

оказался шоком, от которого американцы не могли оправиться даже по прошествии нескольких дней с момента начала операции.

Второй причиной дезориентации американских информационных служб является осознание того, что США оказались изолированными морально от всего остального мира и понимание того, что многократно ошельмованный режим «багдадского тирана» опирается на солидарность всего мира.

Рисунок 25.Успешная пропагандистская акция иракцев с упавшим американским вертолетом

Третья причина – растущий внутренний раскол в администрации Белого дома и высшем американской командовании. Об этом расколе можно судить по критическим высказываниям в адрес текущей операции со стороны ветеранов «Бури в пустыне», в первую очередь, генералов Шварцкопфа и Барри МакКэфри. Косвенно, раскол в администрации США подтверждается и тем, что программная речь Буша о необходимости военной агрессии против Ирака была озвучена в Институте американского общества (AEI). Более двух десятков выходцев из AEI являются сегодня членами команды вице-президента США Дика Чейни и составляют большинство в гражданском руководстве Пентагона. Именно они сформировали видение Вашингтоном «войны за освобождение Ирака». Выходцы из AEI, теснейшим образом связанны с израильскими правыми из партии «Ликуд», победившей на выборах в израильский парламент в феврале 2003 года. Операции в Ираке координировалась заместителем министра обороны США по вопросам политики Дугласом Фейсом. Д.Фейс является одним из авторов письма Беньямину Нетаньяху, в котором израильскому премьеру рекомендовалось прекратить мирный процесс с арабами и вновь заявить права Израиля на палестинские земли. Председатель Совета по оборонной политике Пентагона Ричард Перл, часто называемый интеллектуальной движущей силой мировой политики президента Буша, долгие годы оказывал на американских и израильских лидеров давление с тем, чтобы те развязали войну против Ирака. Еще 8 июля 1996 года, сразу же после победы Беньямина Нетаньяху на выборах над Шимоном Пересом, Перл представил Нетаньяху документ,

озаглавленный «Мощный бросок: Новая стратегия государственной безопасности». Он назвал устранение Саддама Хусейна главной целью Израиля и средством ослабления Сирии. Призыв к нападению на Ирак был затем озвучен в 1997 году правой американской группой, называемой «Проект Нового Американского Века», в который вошли заместитель министра обороны Пол Вулфовиц, директор ближневосточного управления Совета национальной безопасности Эллиотт Абрамс, председатель Комитета по освобождению Ирака Рэнди Шёнеманн, и еще несколько влиятельных персон.

Имея в качестве своих сторонников министра обороны Дональда Рамсфельда и вице-президента Дика Чейни, а также при поддержке целого ряда правых аналитических центров, эта группа сформировала внушительных размеров влиятельную силу, оказывающую давление на политику. Террористические атаки на США 11 сентября 2001 года предоставили этим сторонникам американской империи и американо-израильского альянса шанс. Они смогли сделать неопытного президента Джорджа Буша, чья победа на выборах вызывает сомнения, средством проводки своих идей и реализации своих интересов. В результате – война. Конечная цель – изменение карты Ближнего Востока путем уничтожения или запугивания всех врагов США и Израиля.

О непростой ситуации, сложившейся в командовании коалиционными силами говорит и деятельность пресс-центра армии США в Катаре. По мнению ряда журналистов, аккредитованных в центре, он работал очень плохо, журналисты не получали не только правдивой информации, но даже и пропагандистские заготовки.

Неудачи американского военного руководства проявись в отставке Роберта Перла с поста главного советника министра обороны США.

4.4.4. Деятельность арабских телеканалов в ходе агрессии против Ирака

По мнению ряда экспертов, одним из ключевых отличий информационной кампании в ходе военной агрессии против Ирака от всех предыдущих явилось задействование в ней целого ряда арабских

спутниковых телевизионных каналов, что ликвидировало монополию американских СМИ на информацию из зоны конфликта.

В 1991 году, во время первой войны в Персидском заливе, весь мир следил за событиями в зоне Персидского залива только по новостным выпускам телекомпании CNN, которая вела прямые репортажи с передовой. Однако в ходе последней агрессии сил коалиции против Ирака благодаря медиа-революции увидеть войну в прямом эфире предлагали сразу несколько частных спутниковых арабских каналов, конкурирующих друг с другом. Причем их проарабская точка зрения на происходящее лишь усиливала антиамериканские настроения в арабском мире.

По мнению ряда аналитиков, арабская аудитория сразу оценила эти различия. Как отметило одно периодическое издание из Саудовской Аравии, американские СМИ делали упор исключительно на военных успехах США и Великобритании, в то время как катарская телекомпания "Аль-Джазира", главный поставщик арабских новостей, фокусируется на жертвах войны. Помимо общей оценки происходящего, арабские новостные каналы предлагали зрителям самую широкую информацию о том, что происходит на иракской стороне этой войны.

Журналисты арабских телеканалов передвигались не только по Ираку в составе американо-британских подразделений, но и по Багдаду и другим крупным иракским городам. Пять корреспондентов "Аль-Джазиры" освещали события на иракской стороне, двое были прикомандированы к американским частям. У телекомпании "Аль Арабия" в регионе работало сразу 25 корреспондентов, причем двое из них также находились вместе с американскими и британскими войсками.

Рисунок 26.Демократия по-американски

Объективы телекамер компаний "Аль-Джазиры", "Абу-Даби" и "Аль Арабии" постоянно передавали панораму Багдада, чтобы зрители могли видеть бомбардировки иракской столицы в прямом эфире. Зачастую американские и другие международные СМИ обращались к арабским

телекомпаниям за эксклюзивными кадрами для своих обзоров и срочных новостных сообщений, тем самым подтверждая превосходство арабских телеканалов.

Благодаря наличию корреспондентов в местах основных событий арабские телеканалы могли проверять сообщения американских и британских военных о ходе боевых действий. Что очень важно, это также позволяло опережать источники, из которых поступала информация для официального Вашингтона. Например, когда США впервые официально заявили о захвате города Умм-Каср, корреспондент "Аль-Джазиры", работавший в городе, опроверг это сообщение. В одном из репортажей "Аль-Джазира" показала в прямом эфире танк, стоящий возле склада, где происходила выдача продуктов населению. Затем ее корреспондент сообщил, что британский танк расстрелял этот склад, и продемонстрировал кадры, запечатлевшие горящее здание. А несколько часов спустя журналисты "Аль-Джазиры" взяли интервью у представителя британских военных, который заявил, что ничего подобного не было. Это во многом способствовало организации эффективной контрпропаганды.

Кроме того, Аль-Джазира" и другие компании транслировали не только брифинги и выступления американских и британских пресс-секретарей, но и полностью передавали речи иракских официальных лиц. Причем выступления американской стороны подавались в сопровождении, позволявшем сформировать негативное восприятие аудиторией американо-британской коалиции.

Так, во время брифинга министра обороны США Доналда Рамсфелда, половина телеэкрана занимал сам Д.Рамсфелд, а на оставшейся его части шли кадры того, как спасатели извлекают из-под обломков багдадского рынка окровавленные тела мирных жителей, погибших в ходе последнего воздушного налета. Интервью госсекретаря США Колина Пауэлла, данное специально для "Аль-Джазиры", было показано в сопровождении комментариев двух проиракских аналитиков.

В наибольшей степени точка зрения арабских телеканалов на события в Ираке отличалась от американской в том, что арабы главное внимание уделяли именно потерям среди мирных жителей и военных. У арабских

телеканалов практически отсутствовали кадры, демонстрирующие техническую сторону войны, которые столь часто проходили в американских новостях, - черно-белые съемки удачных воздушных налетов, снятые из штурманских рубок самолетов коалиции, и боевые машины, воюющие на земле. Арабских журналистов меньше интересовал вес сбрасываемых на Ирак бомб, чем тот урон, который они с собой несут, - в их репортажах часто встречаются подробные изображения последствий бомбардировок. Подобные кадры вызывали самый живой отклик среди арабской аудитории, решительно настроенной против войны, которую многие считали несправедливой, и привлекали симпатии к иракцам, которых многие арабы называли своими братьями.

Арабские телеканалы также решительно опровергли заявления о том, что жители иракских городов встречают американские войска как своих освободителей. Так "Аль-Джазира" продемонстрировала в прямом эфире радость иракцев, наблюдавших сбитый над Басрой американский беспилотный самолет. Она показывала куда более напряженные кадры того, как сотни багдадцев собрались на берегах Тигра, поджигая тростниковые заросли и стреляя в воду в поисках американских пилотов, которые, по словам свидетелей, катапультировались из подбитого самолета.

Те же арабские телеканалы показывали на удивление стойкое и организованное сопротивление иракской армии, затормозившей англо-американское наступление на Багдад, что в значительной степени способствовало поддержанию морального духа иракского народа.

4.4.5. Воздействие информационной кампании в ходе агрессии против Ирака на обстановку в мире

Агрессия против Ирака оказала огромное воздействие на весь мусульманский мир. По мнению ряда экспертов, при условии продолжения сопротивления еще в течение, по крайней мере, месяца, Ирак мог бы считать себя победителем. Затянувшаяся на месяц война привела бы к радикальному преображению политической картины мира в направлении, которое США явно не устраивало. Антивоенные выступления в исламском мире трансформировались в антиправительственные. Миллионы мусульман

требовали ухода своих беспомощных и коррумпированных режимов. Однако это далеко не все, что на самом деле содержится в социально-политических последствиях агрессии.

По мнению некоторых экспертов института Ляруша (Канада) ислам превращается сегодня в главную мобилизационную форму международного социального протеста. Многомиллионные выступления населения практически всех стран мира, включая США и Великобританию, явно указывают на то, что вектор солидарности и моральной поддержки «мировой улицы» все больше склоняется к политическому исламу. Именно ислам находится сейчас в прицелах силовых структур империализма и ведет борьбу на передней линии против прихода нового мирового порядка, в котором не будет места ни для демократии, ни для социальной защиты населения в любых странах, включая европейские.

Эксперты Ляруша отмечают также, что массы, выходящие на улицы с протестом против агрессии США, испытывают заново мощную реидеологизацию, впервые после молодежной волны протеста, прокатившейся по миру в 1968-м в связи с агрессией США во Вьетнаме и надеждами на обновление мирового коммунистического движения, связанными с именем Мао Дзедуна. Парадокс сегодняшней ситуации в том, отмечают эксперты, что отсутствие «красного полюса» СССР дает новые возможности для развития международного протестного движения, которое стихийно ищет в условиях постмарксистской ментальности новую идейную базу.

Рисунок 27.Мародерство в Багдаде - элемент психологической операции коалиции

Истеблишменту и нанятым им политикам нечего противопоставить набирающему размах снизу движению. Главным орудием современного контроля со стороны правящих кругов оказывается информация, монополия на которую практически полностью сосредоточена в руках так называемого «политического класса».

Однако в том-то и состоит специфика весны 2003-го, что эффективность воздействия информационных потоков на сознание широких слоев населения, участвующих в протестном движении, снижается ниже того порога, который считается критическим для сохранения государством способности манипулировать своими гражданами.

Результаты вооруженной агрессии против Ирака и, в первую очередь масштабная информационная кампания, сопровождавшая все действия вооруженных сил, привели и к серьезному переосмыслению роли и места средств информационной войны в ряде стран Западной Европы.

Рисунок 28Лицо американской «свободы для Ирака»

По имеющейся информации Франция решила создать собственный спутниковый телевизионный новостной канал. Правительство республики поручило национальным государственным, а также частным теле- и радиокомпаниям в течение ближайшего времени проработать и представить на рассмотрение кабинета министров детальный план нового проекта. Предполагается, что телезрителями французского новостного канала станут жители Европы, Африки и стран Ближнего Востока.

Проект создания «французского CNN» обсуждался в высших эшелонах власти на протяжении всего последнего десятилетия, однако до его реализации дело не доходило, так как создание высокопрофессионального международного новостного телеканала требует больших финансовых вливаний.

Однако резкая конфронтация Франции и США по поводу войны в Ираке послужила катализатором процессов по реализации этого проекта. Проект в настоящее время находится под личным контролем президента Франции. Для снижения издержек вещания планируется широко использовать мощности государственных Международного радио Франции (RFI) и France Television (FT), а также французского внутреннего новостного канала La Chaine Info, которым владеет крупнейший частный телеканал Франции TF1.

Организаторы «французского CNN» не скрывают, что, прежде всего, ориентируются на аудиторию стран Ближнего Востока и Северной Африки. Эти территории Париж считает зоной своего влияния и лоббирует их более тесную интеграцию в европейское пространство. Аналитики отмечают, что французский телеканал сможет легко завоевать здесь стабильную аудиторию. Ведь по-французски говорит значительная часть населения, а тем более элита Марокко, Туниса, Алжира, Ливана, Сирии, Израиля, Египта (египетские христиане традиционно поддерживают тесные связи с Францией).

Франция, претендующая на роль лидирующей европейской и даже мировой державы, в ходе иракских событий явно ощутила свою полную информационную беспомощность. В то время как CNN и BBC активно продвигают позицию американо-британского альянса, а «Аль-Джазира» отражает арабскую точку зрения, у Франции, да и у Европы в целом сегодня не оказалось своего сильного игрока на информационном поле.

Согласно правительственному документу, открытие франкоязычного канала должно донести «…оригинальную точку зрения Парижа на международные проблемы и усилить роль Франции на мировой арене…».

4.5. Оценка экспертами Национального центра защиты инфраструктуры США угрозы эскалации противостояния между различными общественно-политическими, этническими и религиозными организациями в глобальной сети Интернет

В октябре 2001 года Национальным центром защиты инфраструктуры США (http://www.nipc.gov) был опубликован доклад «Кибернетические протесты: угроза американской информационной инфраструктуре». В этом докладе дается анализ и оценка угроз, исходящих от одного из принципиально новых явлений последних лет – кибернетических протестов (или «хактивизм», в зарубежной литературе).

В работ отмечается, что в последнем десятилетии вместе со взрывным ростом числа пользователей Интернет, протесты и политическая активность общества получили новую область своего проявления. Политическая активность в Интеренет уже сформировала широкий диапазон деятельности:

от использования электронной почты и сайтов политических и общественных организаций для координации деятельности своих членов, до уничтожения web-страниц и кибернетических атак на сайты конкурентов. Такая активность создала новый политически мотивированный тип нападений на информационные системы, называемый в зарубежной литературе «*хактивизм» (hacktivism - новый «-изм», включающий в сферу идеологической борьбы и Интерент, от «Hacker»-хакер, взломщик компьютерных систем)*: объединение технологий взлома и политической активности.

В дополнение к нормальной долгосрочной деятельности политических групп в Интернет, им также свойственны краткосрочные периоды интенсивной политической деятельности, которая в западной литературе получила название «*кибернетические протесты»*. Кибернетические протесты стали глобальным явлением, доступным любому у кого есть компьютер, подключенный к Сети. Несдерживаемые государственными границами, протестанты получили огромную аудиторию для оглашения своих требований.

Кибернетические протестанты имеют широкий диапазон целей. Некоторые хакеры хотят подвергнуть критике правительственную политику или фундаментальное нарушение прав человека в разных регионах; другие только хотят взломать чей-нибудь сайт ради собственного интереса. Начиная с 1998 года, кибернетические протесты резко повысили свою популярность и стали обычными в сегодняшнем компьютеризированном мире.

Наиболее общий тип кибернетического протеста выражается в форме изменения содержания web-страниц. В таких сценариях, сайт компрометируется путем использования некоторого недостатка в защите системы, в результате чего хакер получает возможность изменять это содержание, размещая собственные пропагандистские лозунги. Это может стать как простой неприятностью и небольшим затруднением для политической организации, так и привести к серьезным экономическим потерям для бизнеса электронной коммерции.

В отчете отмечается, что разные формы протеста и гражданские беспорядки не новы для человеческой истории. Люди, недовольные своим

положением, как правило, всегда находили пути доведения своих требований до широкой аудитории, будь то мирная сидячая забастовка, кампания сбора подписей, пикеты или силовая борьба с властями. Теперь, с появлением Интернет и растущего числа людей, постоянно работающих в Сети, стало проще организовывать всякого рода протесты. При этом не следует думать, что каждое вторжение на сайт – организованное вторжение со стороны некоторой политической организации. Много подобных инцидентов совершены одинокими хакерами, которые не имеют никакого политического побуждения, кроме как создать хаос.

Этнические государства и их граждане, в силу разрастания этно-социальных кризисов, также были вовлечены в кибернетические протесты. Несколько стран вели продолжительные кибернетические сражения друг против друга путем разрушения сайтов и организации DoS-атак (Denial-of-Service Attack, атака с отказом в обслуживании, подробнее см. например журнал «Connect!Мир связи» №12, 2001 г.). Бомбардировка массивами электронной почты - популярная форма нападения в этих войнах. Огромные количества электронной почты направляются против определенного сайта, перезагружая и вызывая его паралич.

Однако, как замечают авторы отчета, следует отметить, что некоторые партии стали вовлекать в кибернетические протесты не только своих убежденных сторонников, но и простых хакеров. В последнее время увеличилось количество таких союзов. В которых хакерские группы выполняют роль кибернетической полиции отдельных политических партий и общественных объединений.

Среди наиболее активных и показательных конфликтов в информационной сфере за последние несколько лет, эксперты Национального центра защиты инфраструктуры США выделяют следующие:

- противостояние китайских и американских хакеров после разрушения китайского посольства в Белграде и инцидента с самолетом разведчиком ВМС США EP-3;
- противостояние китайских и тайваньских хакеров;
- противостояние израильских и палестинских хакеров;

- противостояние пакистанских и индийских хакеров.

4.5.1. Противостояние американских и тайваньских хакеров китайским хактивистам

По общему мнению, одним из весьма существенных инцидентов стал ряд событий произошедших в мае 1999 года после того, как Соединенные Штаты разбомбили китайское посольство в Белграде в ходе агрессии против Югославии. Целый ряд американских интернет-сайтов в этот период был разрушен от имени Китая. Были организованы массовые почтовые кампании с тем, чтобы объяснить мотивы и получить поддержку действий китайских хакеров. Атакам подвергались, прежде всего, правительственные сайты. Сайты Министерства энергетики, Министерства внутренних дел, Национальной парковой службы были парализованы. Кроме того, официальный сайт Белого дома был недоступен в течение трех дней после того, как его непрерывно бомбил почтовыми сообщениями.

В целом отмечается, что вся эта компания была относительно неорганизованной, достаточно непродолжительной и воздействовала на небольшое число американских сайтов.

Прокитайские хакеры также действовали и против Тайваня в ходе президентских выборов на Тайване в августе и сентябре 1999 года. Кибернетические протестанты атаковали 165 тайваньских сайтов в течение двух месяцев, главным образом изменяя содержание интернет-страниц. Основной целью акции по словам ее участников являлось затруднение нормального функционирования инфраструктуры Тайваня. Среди пораженных сайтов были сайты энергетических компаний, экономические учреждения, передачи данных и управление воздушным движением.

Нанесенный ущерб от проведенных акций был относительно небольшим, подобно имевшим место нападениям на американские сайты годом ранее. Однако в этом случае авторы особо отмечают стратегическое планирование и организацию сил, которые станут обязательными атрибутами подобных действий в будущем. Следует полагать, считают они, что участники эти событий, вероятно, станут более организованными и более успешными в будущих операциях.

В конце апреля и в начале мая 2001 года прокитайские хактивисты и кибернетических протестанты вновь начали нападения на американские сайты. Это последовало вслед за инцидентом в начале апреля, в котором китайский истребитель упал в море после столкновения с самолетом-разведчиком ВМС США. Вспышка киберактивности также совпала со второй годовщиной разрушения китайского посольства в Белграде и праздниками Первого мая и Дня молодежи в Китае. Во главе с Хакерским объединением Китая (HUC), прокитайские хакеры успешно атаковали, более сотни, выбранных наугад сайтов, главным образом в сегментах .gov и .com, путем организации DoS-атак. Некоторые из используемых инструментальных средств были достаточно опасны. Много атак было связано с отправкой на американские сайты фото погибшего китайского пилота Ванг Вея и предупреждений о неизбежном крахе Соединенных Штатов. Проамериканские хакеры отвечали на подобные атаки, нанеся ущерб более 300 китайским сайтам.

4.5.2. Противостояние израильских и палестинских хакеров

В октябре 2000 года после прекращения мирных переговоров, израильские и палестинские хакеры участвовали в ряде кибернетических атак на сайты противника. В ходе атаки 6 октября 2000 года было поражено 40 израильских сайтов и, по крайней мере, 15 палестинских сайтов. Эти события совпали со вспышкой физического насилия в регионе. Атаки стали проблемой и для США так как атакованные сайты располагались на серверах, физически размещенных на территории США. В этом проявилась характерная особенность глобализации информационного пространства, когда страна оказывается вовлеченной в конфликт независимо от ее близости или причастности к событиям.

Уровень сложности атак в израильско-палистинском кибернетическом конфликте располагался в широком диапазоне: от простого изменения содержания страниц до скоординированного, относительно сложному нападению типа захвата полномочий администратора системы. Ряд инструментальных средств взлома был разработан специально для этого случая. В этом конфликте были задействованы многие средства, включая вирусные атаки, нападения DoS с бомбежкой электронной почтой и др..

Сайты, содержащие различные инструментальные средства взлома были доступны для загрузки любому, кто хотел присоединиться к противоборству.

Пропалестинские хакеры разрушали любой тип израильских сайтов, который они были способны компрометировать, заменяя их содержание сообщениями типа: «За свободную Палестину» или «Свободный Кашмир». Программное средство проведения распределенных атак с отказом в обслуживании - FloodNet (подробнее см. например журнал «Connect!Мир связи» №12, 2001 г.), было главным инструментом, используемым израильтянами. Кибернетическому протестанту достаточно просто посетили сайт, и FloodNet будет неоднократно посылать запросы на заданный сервер. Этот тип виртуальной «сидячей забастовки» - популярная форма нападения с отказом в обслуживании. Многие из этих нападений были успешны. В качестве адресатов для распространения потоков ложных пакетов были включены сайты этнических организаций и финансовых учреждений, с целью разрушить инфраструктуру государств. Ряд сайтов электронной коммерции потерпели крах в результате чего был нанесен существенный экономический урон, что получило отражение на израильских рынках.

Все эти события привлекли широкие массы хакеров, стремящихся к объединению в борьбе. Обе стороны были хорошо организованы и использовали разведку для сбора сведений с целью повышения эффективности вторжений.

Ряд групп (типа пакистанской G-Форс) объединились с палестинцами, чтобы оказать им помощь в борьбе с Израилем. Как ни странно, но это становится уже все более и более обыденным. Некоторые сторонние группы присоединяются к общим усилиям потому, что они имеют подобные политические или этнические убеждения. Однако, это не всегда так. Некоторые группы участвуют во взломах просто из желания взломать или сделать себе рекламу.

В целом авторы отчета считают, что израильские и палестинские хакеры будут активны всякий раз, когда вновь будут возникать препятствия к восстановлению мира между их странами.

4.5.3. Индийские и пакистанские хакеры

Другой пример - Индия и Пакистан, участвующие в кибернетическом протесте, вызванном национальными и этническими различиями. После прекращения огня в штате Кашмир группы хакеров взяла на себя дело продолжения борьбы. В 2000 году про-пакистанские хакеры вторглись на больше чем пять сотен индийских сайтов. И наоборот - только один известный пакистанский сайт был взломан индийцами в этот же период. Что весьма странно, учитывая место, которое занимают индийские программисты в общемировой иерархии. Это иллюстрирует большое различие в технических подходах к организации взлома, способности или готовности использовать имеющиеся навыки для нанесения кибернетического удара по противнику. В этом случае уровень сложности проводимых атак с обеих сторон был относительно низок. Изменение содержания сайта - ведущая форма этого протеста. Пакистанская группа G-Форс была наиболее активной группой, отмеченной в причастности к событиям.

4.5.4. Стычки между корейскими и японскими хакерами

В течение первой недели апреля 2001 года, прокорейские хакеры напали на сайты ряда японских организаций, ответственных за одобрение нового учебника истории. Учебник изменил описание военных преступлений, совершенных Японией в ход Второй мировой войны в отношении Китая и Южной Кореи. Воспринятое нежелание Японии принять ответственность за ее действия запустило указанные события. Главными участниками инцидента были студенты корейских университетов, которые использовали почтовые бомбы для организации DoS-атак. Студенты разрушили несколько сайтов, включая сайты Министерства просвещения Японии, Либеральной Демократической партии и издательской компании, ответственной за учебник. Эти нападения не были достаточно продолжительными, при этом они в значительной степени не были организованы.

В начале августа 2001 года прокитайские хакеры вновь стали преследовать японские сайты после того, как премьер-министр Японии посетил военный мемориал Ясукуни. В короткий период времени хакеры разрушили несколько сайтов, принадлежащих, главным образом, японским компаниям и научно-исследовательским институтам. Это указывает на продолжающуюся готовность прокитайских хакеров использовать

киберпространство и инструментальные средства взлома как основу протестов и кибернетического гражданского неповиновения.

4.5.5. Кибернетические протесты, связанные с войной против терроризма

Изложенный далее материал основан на информационном сообщении, подготовленном экспертами Национального центра защиты инфраструктуры в ноябре 2001 года в качестве дополнения к опубликованному ранее отчету о проблемах эскалации хактивизма. Основной акцент в работе делается на анализе борьбы проамериканских и антиамериканских хакерских групп в ходе антитеррористической кампании.

Материал сосредотачивается на событиях, которые произошли после террористических нападений 11 сентября, результатом которых стало повышение уровня угроз американской информационной инфраструктуре, включать потенциал для проведения распределенных атак с отказом в обслуживании (DBoS, подробнее см. например журнал «Connect!Мир связи» №12, 2001 г.). Начиная с террористических нападений 11 сентября 2001 слухи относительно потенциала кибернетических нападений изменились от «небольших неприятностей» до «информационной войны», хотя в целом, по оценке экспертов Национального центра защиты инфраструктуры США, киберугрозы к настоящему времени находится на нижней стороне общего спектра угроз.

В описываемый период как проамериканские, так и антиамериканские протестанты были в равной степени активны. Однако эффекты их действий особенно не были разрушительны. В ходе рассмотрения этих событий, анализ тенденции, по мнению экспертов. указывает на то, что угрозы американским информационным сетям и сайтам остаются достаточно низкими, хотя в целом угроза выше, чем до 11 сентября 2001 года.

Действия проамериканских хакеров

Начинаясь с 11 сентября, патриотически-настроенные группы хакеров в интернет-чатах запросили поддержки в организации масштабного нападения на пакистанские и афганские сайты. Они выдвинули идею возмездия за террористические нападения в США на Центр международной торговли и Пентагон. Американский сайт, имеющий отношение к собаками афганской

породы был, по сообщениям прессы, первой жертвой проамериканских кибернетических протестантов.

12 сентября был разрушен официальный сайт правительства Пакистана. Ряд других сайтов, принадлежащих к компаниям Афганская сеть новостей, Афганская политика, а также сайты Taleban.com и Talibanonline.com, также подверглись нападению.

Активно использовался спам (массовое распространение электронные почты) с целью поощрить хакеров присоединяться к нападению на сайты, относящиеся к организациям исламского фундаментализма, и всех организаций, кто поддерживает терроризм. Получателей сообщения просили о дальнейшем его распространении с тем, чтобы убедить других присоединиться к борьбе любыми средствами: будь то активный взлом или обеспечение действий путем сбора информации.

В тот же день, 12 сентября, на официальный сайт президентского дворца Афганистана была организована DoS-атака, которая сделала его недоступным. Телеконференции Usenet, имеющие дело с исламом, также испытали нападения DoS. Телеконференция soc.religion.islam активно атаковалась множеством почтовых сообщений и впоследствии стала недоступной.

Запрос хакерам о поддержке был успешен. Группа, называющая себя «Dispatchers», возглавляемая хакером по прозвищу Rev, принялась за организацию атак против палестинских и афганистанских сайтов. Их первая известная атака была проведена уже 16 сентября, когда был атакован сайт иранского Министерства внутренних дел. Группа заявили о намерении продолжить разрушать сайты в качестве возмездия за террористические нападения.

Наиболее известные проамериканские группы взлома сформировались в конце сентября 2001 года. Одной из них является группа «Молодые интеллектуальные хакеры против террора» (YIHAT), основанная немецким хакером Кимом Шмицем (Kim Schmitz). Группа поставила своей целью организовать сбор информацию о террористических группах и передавать ее американским властям. Они утверждают, что взломали Суданский банк и нашли отчеты, связывающие учетные записи банка с Аль-Каидой и Осамой

Бен-Ладеном. Этой группой также был создан сайт www.kill.net для сбора информации о вех пострадавших от воздействия DoS-атак, проведенных противостоящими группами взлома, поддерживающих антиамериканские чувства, включая и Флуффи Бунни (Fluffi Bunni), одного из известных хакеров.

Впоследствии такая активность вынудила YIHAT перевести ее действия в «подполье» и использовать методы конспирации, чтобы защитить своих членов. Они вынуждены были прекратить поддержку сайта kill.net.

Хотя YIHAT и осуждает уничтожение информации на атакованных сайтах, все же был зафиксированы многочисленные факты, совершенные от их имени. YIHAT объявил также планы о поиске государственного финансирования от правительств тех стран, которые легализует действия по взлому в их усилии по борьбе с терроризмом. Также руководством группы планируется открыть учебный центр взлома, чтобы лучше подготовить своих членов. Было объявлено, что численный состав группы составляет около 800 зарегистрированных члена, хотя пресса говорит всего о 25-35 активных членах этой группы.

Деятельность антиамериканских хакеров

14 сентября Флуффи Бунни – хакер одиночка - перехватил адреса нескольких тысяч сайтов, скомпрометировав сервер доменных имен поставщика интернет-услуг, и стал переадресовывать запросы пользователей на те сайты к собственной web-странице, на которой была только одна фраза «Флуффи Бунни ведет Джихад». Эксперты отмечают, что это было самым крупным действием одиночки среди террористических протестов. Несмотря на то, что этот случай продолжался только час, однако число сайтов, на которые было оказано воздействие, было достаточно велико.

Также 14 сентября, компьютерный вирус LifeStages был переименован в WTC.txt.vbs, чтобы инфицировать пользователей из числа тех, кто был любопытен к событиями вокруг Центра международной торговли. Эффект от воздействия вируса на компьютерные системы был минимален.

15 сентября был атакован сайт электронной коммерции, принадлежащий компании First Responder Supplies, который был взломан группой,

утверждающей, что является бразильской группой хакеров Illegal Crew. Это типичный случай для хакерских групп, когда они беруться «за оружие», и при этом не связаны с конкретным случаем или причиной. К тому моменту бразильские хакеры были вовлечены в протесты против Соединенных Штатов уже около двух лет. Пакистанский клуб хакеров (PHC), включая «Доктора Нукера» и группу G-Форс, также был активен во взломе американских сайтов. G-Форс является пакистанской хакерской группой, которая сформировалась в феврале 2000 года и прежде всего известна как исполнитель атак на web-страницы израильских, индийских и американских правительственных сайтов. Первичный заявленный повод для их деятельности заключается в протесте, связанном с нарушением прав человека против мусульман в Израиле и Кашмире.

17 октября 2001 года сервер сети Национальной океанической и атмосферной администрации был взломан от имени G-Форс, которая угрожала нападениями и на другие сайты оборонных ведомств США и Великобритании, если ее требования не будут выполнены.

Несколькими днями позже, 20 октября, предположительно G-Форс разрушила один из сайтов Министерства обороны США.

Это атаки на web-страницы показали способность хакеров компрометировать серверы. Однако, как считают эксперты, маловероятно, что любые серверы высокого уровня сети Минобороны США будут успешно взломаны.

Другие известные хакеры указали, что они также присоединятся к нападениям на американские сайты. В связи с чем, серверы и другие компьютерные системы в зарубежных странах стали уязвимы также как и в Соединенных Штатах. Первый инцидент произошел 1 октября, в Венгрии, когда хакеры вторглись в сайт венгерского министерства национальной безопасности. Это указывает на готовность хакеров идти против тех государств, которые непосредственно не вовлеченных в текущую войну против терроризма, но сотрудничают с США.

Однако не все хакерские группы включились в борьбу против Соединенных Штатов. 14 сентября, группа немецких хакеров, известная как «Компьютерный клуб Хаос», запросила прекращения протестов от всех

компьютерных энтузиастов с целью остановить действия линчевателя. Они призвали по глобальной связи к разрешению конфликтов. Их мирные усилия были широко оглашены, но в значительной степени остались незамеченными хакерским сообществом. Cyber Angels, известная группа хакеров, продвигающих ответственное поведение, также выступили против взлома на основе политических убеждений. Они поддержали телевизионные объявления, убеждающие хакеров не подхватывать идеи по разрушению, а скорее, убеждая тех же самых хакеров помогать собирать сведения и информацию относительно преступников, кто участвуют в этом хактивизме.

Последние события в киберпорстранстве показали, что группы пакистанских хакеров объявили «кибернетический джихад» Соединенным Штатам и призывают всех хакеров мусульманской веры участвовать в этой борьбе. Среди них G-Форс сыграла наиболее значимую роль в формировании коалиции по борьбе против Соединенных Штатов. Их главные цели - американские сайты, но они также нападают на индийские сайты и сайты государств, поддерживающих Соединенные Штаты. Лидеры группы заявили, что они продолжат атаки на сайты Минобороны США и сайты, которые поддерживают критическую инфраструктуру.

Особо отмечается, что в ходе анализа событий, последовавших за 11 сентября, был выявлен эффект избытка протестов. При этом несколько ошибочных целей было уничтожено. Так, 16 сентября пострадала корпорация America-on-Line только потому, что слово "терроризм" было включено в универсальных указателях ресурса (Universal Resource Locator). Как известно эта компания сама потеряла около 200 служащих в своем офисе в Центре международной торговли. Группа, называющая себя «The Dispatchers» приносила извинения за ошибку. Эта ситуация отразилась и на сайтах других стран. Так австралийский сайт был атакован 27 сентября антиамериканскими хакерами только потому, что он имел словосочетание «торговый центр» в его универсальных указателях ресурса. Это – типичное для подобных видов атак событие, когда для выбора цели используются только ключевые слова, а не подробный анализ содержания того или иного сайта. Некоторые сайты были атакованы просто потому, что их названия показались достаточно подозрительными.

Проамериканские хакеры продолжают отвечать на конфликт в киберпространстве. Среди них достаточно велико было разрушение ошибочных целей среди американских сайтов, сайтов американских союзников или тех, кто вовсе не вовлечен в военные действия. В первые недели после террористических нападений, много говорилось о разрушении web-страниц множества сайтов. Однако общее число и сложность этих атак остались довольно низкими.

На многих сайтах, которые были атакованы проамериканскими протестантами, размещались фотографии Осама Бен-Ладена с приставленным к виску пистолетом. А многие из сайтов, разрушенных антиамериканскими протестантами, помещались изображения мертвых или умирающих арабских детей с описанием, утверждающими лицемерие действий Соединенных Штатов.

Множество экспертов по защите информации сходятся во мнении, что, начиная с 11 сентября, потенциал для более серьезных кибернетических нападений уже существует. Более того, такие атаки становятся неизбежными. Это ведет к тому, что кибернетические протесты и хактивизм продолжает развиваться, и общее число атак может даже возрастать, поскольку Соединенные Штаты продолжают военную операцию.

Потенциал будущих DDoS-атак остается высоким. Хактивисты отметили, что они планируют в качестве мишеней сайты министерства обороны США и организаций, которые поддерживают критическую инфраструктуру Соединенных Штатов, однако много предпринимателей и других организаций, совершенно не связанных с событиями, оказались жертвами нападений.

Таким образом, на основе материалов отчета Национального центра защиты инфраструктуры США можно сделать вывод о том, что политические события и усложнение международной ситуации будут все более и более способствовать росту числа протестов с использованием возможностей Интеренет (кибернетических протестов). Кибернетические протесты, которые были зарегистрированы к настоящему времени, имели относительно малое разрушающее воздействие на инфраструктуру. Вместе с тем, поскольку вычислительные технологии с каждым годом становятся

быстрее и лучше, а инструментальные средства взлома еще более распространенными и более легким в использовании, кибернетический протест и хактивизм станут более существенной угрозой национальным интересам ряда развитых стран.

Кибернетические протестанты становятся все более и более организованными, а их методы - более искушенными. Наиболее вероятно, что они продолжат разрушать интернет-сайты, а также организовывать масштабные атаки с отказом в обслуживании (DoS). Следует также ожидать увеличения числа несвязанных между собой хакерских групп, участвующих в кибернетических протестах. Национальные границы уже не будут явно присутствовать в нападениях на противостоящие структуры. Международная деятельность хакерских групп будет также иметь тенденцию распространяться на территории новых государств, ранее не участвовавших в этой деятельности.

Чаще всего целевыми являются сайты, принадлежащие правительственным, образовательным, коммерческим и культурным учреждениям. Однако, любой сайт с пригодной для использования уязвимостью, будет восприимчив к кибернетическому нападению.

Сайты, которые остаются открытыми для известных инструментальных средств взлома, будут иметь более высокую вероятность подвергнуться воздействию хактивистов. В этом случае, сетевые администраторы должны остаться высоко квалифицированными, а средства защиты не должны отставать в развитии от средств нападения. Хотя кибернетические протесты, замеченные сегодня уже вызвали ограниченный ущерб, потенциал для будущих нападений мог вызывать еще большие экономические потери и ущерб национальной инфраструктуре, воздействуя на глобальные рынки и общественную безопасность.

Авторы проведенного исследования отмечают, что в то время как ущерб от описанных выше нарушений до настоящего времени был минимальным, следует ожидать, что в будущем кибернетические протестующие и хактивисты все чаще будут ставить перед собой цель, состоящую в намеренном разрушении информационной инфраструктуры. Действенная сетевая защита и управление безопасностью обязательны для

предотвращения более серьезного ущерба инфраструктуре. Особо отмечается, что международное сотрудничество, а также сотрудничество между государственным и частным сектором в крайне необходимы для обеспечения нормального функционирования критической инфраструктуры.

4.6. Реализация принципов ноополитики: международный терроризм как инструмент глобального управления в информационную эпоху

В качестве реализации принципов ноополитики в новейшей истории можно привести деятельность администрации США в ходе антитеррористической кампании, последовавшей за террористическими актами 11 сентября 2001 года.

Анализ политической обстановки, деятельности общественных и политических деятелей, а также СМИ как в США, так и в других странах, показывает, что произошедшие в США 11 сентября 2001г. террористические акты есть ни что иное, как попытка навязать мировому общественному мнению алгоритм поведения с задачей получить строго заданные реакции на террористические акты, что в полной мере соответствует реализации базовых принципов ноополитики.

В свое время К. Маркс писал, что финансовый капитал ради нескольких процентов прибыли пойдет на любое преступление. Видные ученые, участники международной конференции, состоявшейся в Москве 15-16 мая 2001г. единодушно отметили взаимосвязь военных конфликтов с ситуацией на мировом финансовом рынке.[90] Небольшой ретроспективный анализ показывает, что данная тенденция отнюдь не нова.

За пять лет до начала Первой мировой войны попечители Фонда Карнеги за международный мир в течение года обсуждали вопрос: существует ли средство для изменения жизни целых народов более действенное, чем война? Протоколы этих заседаний свидетельствуют, что более действенного средства найдено не было.

Широкие банковские круги того времени были глубоко заинтересованы в мировой войне из-за огромных возможностей для получения крупных

прибылей. Международные банкиры во время войны наживались не только за счет получения выгодных контрактов, но и за счет предоставления правительствам воюющих держав больших кредитов, усиливая тем самым их финансовую зависимость.

Так, в результате Второй мировой войны долг США вырос с 43 млрд. долл. в 1940 г. до 257 млрд. долл. в 1950 г. (увеличение на 598%). За тот же период долг Японии увеличился на 1348%, Франции – на 583%, Канады – на 417%.[91]

Если в начале XX века для запуска механизма глобальной бойни достаточно было выстрела из пистолета (убийство наследника престола Австро-Венгрии, 1914 г., Сараево), для начала Второй мировой войны – более крупной провокации (операция «Гляйвиц», 1939 г., Польша), то в начале XXI века для поражения воображения искушенного кровавыми сценами обывателя потребовалось хорошо срежиссированное поражающее воображение супер-шоу в стиле Голливуда. Если в начале XX века для определения направления удара был подобран «сербский террорист», то в начале XXI века – «арабские террористы». Воистину все новое – это хорошо забытое старое!

Многие эксперты сходятся во мнении по поводу того, что военные конфликты современности инспирируются пресловутым «мировым правительством». Это подтверждают последние события на Балканах, где вдруг ниоткуда появляются какие-то неизвестные боевики, экипированные и вооруженные не хуже регулярной армии. Между тем, еще в мае 1996 года в Турции заседании Билдербергского клуба был поднят вопрос о ситуации в югославском крае Косово («Toronto Star», июнь 1999 г.). Обсуждение вопроса о судьбе Косово возникло по чисто экономической причине. Она заключалась в том, что ранее Запад получал стратегически важный металл хром в основном из Заира, однако в 1994 году после свержения режима Мабуту хромовые поставки оказались под угрозой. На территории же Косово (вместе с Албанией) находится до 90% разведанных европейских запасов этого сырья, стоимость доставки которого к европейским потребителям в 10 раз ниже, чем из Заира. Кроме этого, в середине 90-х годов масоны Греции

---

[90] «Общество и экология», № 24, 2001 г.
[91] «Знание – Власть!», № 7 (132), 2001 г.

открыто заявили о своей полной поддержке территориальных претензий Афин к бывшей югославской республике Македонии («Правда», 13.02.1996).

Известно, что провоцирование и организация военных конфликтов в конечном итоге ведут к доминированию валюты той страны, территория которой не задействована в военном конфликте. Именно этот рзультат в виде Бреттон-Вудского соглашения был получен в результате Второй мировой войны. Наиболее точно этот сценарий сформулировал американский историк А. Вульф: «Наилучший способ использовать преимущества войны заключается в том, чтобы всегда иметь войну, особенно если окажется возможным сделать это с минимальным участием в военных действиях».

Осознание факта, что дальнейшее широкомасштабное использование оружия против армий и народов в современных войнах ведет к глобальной катастрофе, гибели цивилизации и среды обитания, что человечество не сможет пережить еще одной мировой войны, тем более с применением ядерного оружия, вынуждают «сильных мира сего» прибегать к таким инструментам как «конфликты низкой интенсивности» и терроризм, поддержанных активными информационными операциями.

Современный передел мира повышает роль международного терроризма как инструмента политики даже у вполне нормальных демократических государств. Имеется достаточно много примеров, когда силы международного террора используются, что называется, «на заказ», в качестве тарана для разрушения существующих структур, нарушения сложившихся военно-политических балансов сил, перекраивания зон интересов, влияния и взаимодействия. В последующем такие государства стремятся сами заполнить образовавшиеся геополитические пустоты, встроиться в те или иные региональные структуры в качестве балансира, миротворца, регулирующей силы в управляемом конфликте.

В результате часто возникает симбиоз совершенно разнородных сил, например, исламских экстремистов и западных демократий, которые, каждая со своими целями, участвуют в своего рода разделении функций и взятых на себя полномочий в четко скоординированном процессе. Другое дело, что в силу различия стратегических целей, их несовпадения и даже стремления переиграть друг друга, использовать «втемную» в дальнейшем между

партнерами могут иметь место серьезные разногласия и конфликты. Сегодня очень многие не хотят понимать, что заигрывание с международным терроризмом, попытки использовать его в собственных интересах, чреваты серьезными просчетами и проблемами в перспективе.

Межэтнические вооруженные конфликты или конфликты между официальными властями и террористическими по своей сути вооруженными группировками и организациями - это эффективный способ дестабилизации обстановки в ряде регионов бывшего СССР. Имеется немало примеров того, как недоброжелатели России использовали эти возможности в качестве повода для воздействия на внутрироссийские события и политические процессы на всем постсоветском пространстве. С этой точки зрения терроризм следует рассматривать как один из инструментов неоглобалистской политики Запада, установления им т.н. нового мирового порядка.[92] Нет сомнения, что сентябрьские события в США того же порядка.

Вряд ли случайно совпадение масштабных терактов со значительным экономическим спадом в США, официальный долг которых на сегодня 32 трлн. долларов, и неуклонным ростом экономики Китая. За несколько месяцев до трагических событий произошло «схлопывание» американского фондового рынка высокотехнологичных корпораций, построенного по принципу финансовой пирамиды, что привело к падению индекса NASDAQ. Это в свою очередь повлекло за собой сокращение уровня потребления населения США, ухудшило положение американской промышленности, которая уже почти не выдерживает конкуренции с Европой и Азией, работает «на склад», что приводит к неустойчивости индекса Dow Jons и естественно, что долго так продолжаться не может.

Курс доллара на мировых валютных рынках начал устойчиво падать, а курс евро расти, чему способствовал перевод всей валютной выручки Китая за 2000 год из долларов в евро в особенности после того, как 1 сентября была начата печать наличных евро.

Все это вместе взятое приводит к быстрой потере инвестиционной привлекательности США и оттоку из них капитала. Единственным выходом

---

[92] Проблемы терроризма и борьбы с ним. Аналитический доклад. – М.: Центр стратегического развития. – 1999, с. 10.

в сложившейся ситуации для администрации Буша был переход с экономических методов доминирования в мире на силовые. Именно с этой целью американский президент начал срочное разворачивание программ ПРО.

Так, в начале сентября, всего за несколько дней до терактов, сенатский комитет по вооруженным силам США проголосовал за сокращение финансирования противоракетных программ на 1,3 млрд.долл. от запланированных администрацией Буша на начавшийся в США 1 октября финансовый год. Неудача, постигшая Буша на встрече глобалистов в Генуе, ставила экономику США в затруднительное положение.

Варварские бомбардировки Ирака, Афганистана, Судана, Югославии постоянно усиливали неприязнь к США в мире. Конфликты на Балканах, так или иначе, начали затухать и уже не могли принести тех дивидендов, что и раньше.

Экспансия НАТО на Восток практически достигла своего предела, дальнейшее расширение «оборонительного союза» за счет стран «второй волны», вполне очевидно, принесет ему больше минусов, чем плюсов.

Стремление Запада навязать свои «ценности» странам с сильной традиционной культурой встречает все более жесткий отпор.

В складывающихся условиях выход для международного финансового капитала, чьим инструментом являются США, оставался, по сути, только один: спровоцировать войну, которая, протекая на другом континенте, позволила бы ему в очередной раз выйти из кризиса с выгодой, в том числе, посредством массированных капиталовложений в военно-промышленный комплекс США, в развитие национальной противоракетной обороны. (Кстати, Первая и Вторая мировые войны были развязаны не без участия США с несомненной для них пользой).

Кроме того, описываемые события происходят на фоне изоляции США и Израиля на конференции в Дурбане (ЮАР); нарастания интеграционных процессов в арабском мире, сближения позиций Ирака, Ирана, Сирии и Саудовской Аравии; новой политики стран ОПЕК, приводящей к значительным деформациям на мировых биржевых рынках; усиления внешнеполитической деятельности России с Китаем, Индией и «странами-

изгоями» - КНДР, Ливией, Ираком, Ираном; начала новой интифады на Ближнем Востоке.

Многие военные эксперты, в том числе и в США, прогнозировали, что при нынешнем положении вещей США утратят лидирующее положение в мире уже к 2015 году. Их место будет занято активно развивающимся Китаем.

За несколько недель до начала крупнейшей в истории военной операции по упрочению мирового господства США начинается проведение информационных операций по ее обеспечению, что вполне логично укладывается в существующую военную стратегию США и НАТО. В конце августа CNN приглашает на должность ведущего военного эксперта отставного четырехзвездного генерала У. Кларка, известного своими радикальными взглядами. Это вполне может расцениваться как подготовка к освещению масштабных военных событий, которые должны развернуться в ближайшее время.

Кроме того, 6 сентября антитеррористический отряд ФБР устроил облаву в помещении компании InfoCom, на серверах которой размещаются многочисленные арабские веб-сайты. Корпорация InfoCom базируется в пригороде Далласа, штат Техас, и обеспечивала поддержку нескольких сотен сайтов, включая ведущий независимый арабский канал новостей. Среди временно закрывшихся оказались сайты телекомпании «Аль-Джазира» и газеты «Аль-Шарк» из государства Катар.

«Аль-Джазира» - главный источник новостей для арабо-говорящего населения в регионе. Ее называют "арабской CNN". Можно предположить, что данная операция, исходя из опыта конфликта в Югославии, была предпринята с целью обеспечить подавляющее господство проамериканских СМИ на начальной стадии конфликта.

Далее, за неделю до терактов Москву посещает с визитом А.Шарон с большой делегацией, однако программа визита резко меняется в ходе ее проведения. Ариэль Шарон проводит встречи и консультации с лидерами еврейских общин в России. 9 сентября совершается покушение на лидера Северного альянса Ахмадшаха Масуда. В связи с этим всплывает фигура

Усамы бен Ладена. Ему припомнили взрывы посольств США в Кении и Танзании…

Не менее интересные совпадения наблюдаются в действиях СМИ.

Однако, похоже, что именно в этой сфере организаторы провокации в виде грандиозного террористического акта переборщили, и тем самым, по сути, расписались в подготовке и проведении операции.

Поражает поспешность в стремлении направить гнев общественности на мусульманский мир: немедленно появляется сообщение о якобы найденном в г. Бостоне автомобиле, в котором был обнаружен Коран, инструкция по управлению «Боингом» на арабском языке, калькулятор для подсчета горючего в пассажирских лайнерах; буквально через ничтожно малый промежуток времени параллельно с плачущими американцами CNN начинает показ радующихся палестинцев; навязчиво, на протяжении нескольких часов осуществляется демонстрация руин Всемирного торгового центра и стреляющего из АКМ Усамы бен Ладена.

В момент терракта, наиболее подходящим для проведения корректировки сознания, СМИ вгоняют население США в шок, заявляя примерно о 50000 погибших. За два часа трансляции (с 19 до 21 часа, 11 сентября) 10 секундный ролик с кадрами тарана угнанным самолетом южного здания всемирного торгового центра были показаны только в российском эфире около 20 раз, хотя сам ролик не несет никакой актуальной информации. Основные эпитеты – апокалипсис. Впервые в прямом эфире были показаны кадры самоубийства людей, выпрыгивающих из окон пострадавших зданий.

За двое суток освещения последствий теракта общий информативный поток (то время, в которое сообщалась новая информация) не превысил 40 минут. Операторы с азартом отмечали, что число жертв должно быть не менее 10000 человек. В последствии эта цифра уменьшится до 5000. Реально извлекут из-под завалов торгового центра немногим более 300 человек (для сравнения, при взрыве жилого дома на ул. Гурьянова в Москве погибло 229 чел.).

Совершенно необъясним ряд фактов: попадание первого (!) самолета в здание Всемирного торгового центра оказалось снятым на видеокамеры с

нескольких ракурсов[93]; следует сообщение CNN о том, что террористы захватили 11 (!) «Боингов» и др.

Здесь явно просматривается задействование технологии манипуляции сознанием. Цель - вогнать американский народ в шок для дальнейшего внушения ему необходимости самых жестких мер против «террористов». Шок был необходим для того, чтобы американцы без размышлений увидели своим врагом того, на кого укажут власти. И власти, не имея никаких доказательств, указали на Бен Ладена, начав подготовку к войне против талибов, организации которых создавались и вооружались под непосредственным контролем спецслужб США.[94] Выбор Афганистана тоже не случаен. Во-первых, это страна с устойчивым имиджем террористического логова, созданного западными СМИ. Во-вторых малая численность населения, пустынный характер местности и практически полное отсутствие инфраструктуры, особенно информационной, позволяет американским стратегам сконцентрировать внимание именно на информационном освещении операции, так как для большинства населения будет доступна только официальная информация, поступающая по каналам CNN. Все альтернативные каналы (в частности «Аль-Джазира») запрещаются к трансляции на территории США и НАТО. Все это позволяет задействовать приемы манипулирования сознанием по типу «реальной виртуальности», когда информационное описание события в СМИ гораздо значимее самого этого события. Операцию в Афганистане проводит именно CNN, американские солдаты – бравые киногерои.

Однако менталитет и пацифистский характер психики американцев не позволяет проводить достаточно длительных операций, неизбежно нарастает протест против любого неоправданного насилия. В этом случае используется катализатор, поддерживающий измененное состояние сознания – информационный вброс по поводу бактериалогической атаки террористов. Однако очевидно, что преодолеть эпидемиологический порог неконтролируемого распространения выбранной инфекции в современных условиях невозможно, но достигается необходимая пролонгация требуемого психологического состояния.

---

[93] «Эксперт», № 35, 24 сентября 2001 г., с. 11.
[94] «Русский Вестник», № 37-38, 2001 г., с. 8.

Возникает еще ряд вопросов, наводящих на размышления: почему традиционно сильные спецслужбы США не сумели выявить никаких признаков готовящихся терактов? Как стал возможным таран Пентагона, имеющего собственную систему ПВО? Почему самолет, управляемый пилотом-камикадзе, на протяжении более чем 200 миль летел за пределами воздушного коридора и не был обнаружен средствами ПВО страны? Почему ни один из членов американской администрации в связи с явными провалами в различных сферах даже не заикнулся об отставке?

Вместе с тем, уже 11 сентября Г. Кисенжер отметил, что для осуществления акции требовалось многомиллионное финансирование, наличие доверенных людей во многих госучреждениях США для поддержки подготовки и проведения теракта, что не под силу никакой из ныне известных террористических организаций, действующей в одиночку.

Все это наводит на мысль, что теракты 11 сентября являются ничем иным, как провокацией нового глобального управляемого кризиса, спланированного в полном соответствии с одноименной концепцией, которая так популярна сейчас на Западе.

Удар был нанесен по стране, являвшейся мировым лидером. Результаты теракта, с одной стороны, потрясли весь мир, с другой, - продемонстрировали уязвимость Соединенных Штатов, серьезно подорвали их престиж и вынудили приступить к формированию широкой антитеррористической коалиции под лозунгом “кто не с нами, тот против нас”.

Наиболее вероятно, что США под предлогом возмездия террористам постараются извлечь максимум выгоды из сложившейся ситуации и решить ряд проблем геополитического, экономического и военного характера. Можно полагать, что они не ограничатся действиями только против террористических организаций и их лидеров, а используя международную поддержку, будут стремиться кардинально изменить обстановку на Ближнем Востоке, в Центральной и Средней Азии, расправиться с неугодными им режимами, закрепить там свое влияние и непосредственное военное присутствие, игнорируя интересы других государств, включая Россию.

В знаменитой теперь уже речи президент Буш отметил «… мы покажем всему миру, что наша страна с честью пройдет через эти испытания…, … это трусливое нападение на свободу…, …США найдут и накажут…». В речи перед Конгресом США звучит историческая фраза «кто не с нами, тот против нас!»

Все. Система миропорядка, сложившаяся после Второй мировой войны сломлена. Об ООН никто (кроме Китая) даже не вспомнил. Появились комментарии, что сегодня США может утвердиться в качестве мирового лидера, объявив крестовый поход против исламского фундаментализма, что очень выгодно Израилю. Теперь достаточно навесить ярлык (что очень популярно при планировании и проведении информационно-психологических операций) «страны-изгоя» или «международного террориста», чтобы устранить неугодного о своего пути. Тысячелетняя история права закончилась.

Есть опасение того, что в ходе так называемой антитеррористической кампании, террористические организации, созданные западными спецслужбами для дестабилизации обстановки в различных регионах мира, не только не будут ликвидированы, а наоборот получат существенную поддержку. Симптоматично, что после терактов в Нью-Йорке и Вашингтоне в выступлениях президента США не прозвучало прямой поддержки усилиям России по искоренению терроризма на Северном Кавказе, а было высказано лишь осторожное понимание позиции России.

В заявлениях лидеров и ведущих политиков стран Западной Европы вновь звучал тезис “о непропорциональности применения Россией военной силы”. Не были предприняты конкретные шаги по закрытию представительств Ичкерии и ликвидации на территории стран НАТО организаций и пунктов вербовки наемников для Чечни.

В странах ближнего зарубежья, ориентирующихся на Запад, прозвучали лишь заявления о нежелательности присутствия на их территории самых одиозных чеченских руководителей бандформирований, при этом даже не были предприняты попытки к их задержанию.

Поспешные популистские заявления Дж. Буша-младшего, оказываемое неприкрытое давление на руководство мусульманских государств уже

привели к консолидации экстремистских фундаменталистских организаций в различных странах, даже тех, которые ранее враждовали между собой.

Экстремисты уже заявили о возможности развязывания террористической войны против стран, объявивших о своей солидарности с Вашингтоном. Следствием этого может стать активизация и распространение исламского экстремизма на южные районы РФ с преобладающим мусульманским населением. Не исключается возникновение новых вооруженных конфликтов вблизи границ Российской Федерации и рост сепаратистских тенденций на национально-религиозной почве внутри России.

Анализ террористической деятельности в мире на протяжении последних десятилетий позволяет отметить следующие отличительные особенности современного терроризма:

- формирование глобальных и региональных руководящих центров, осуществляющих подготовку операций и организацию взаимодействия между отдельными группами и исполнителями, привлекаемыми к той или иной акции, при этом национальная и религиозная принадлежность исполнителей не является свидетельством принадлежности к конкретному государству или религиозному движению;

- использование права на политическое убежище для закрепления присутствия террористов в некоторых государствах;

- осуществление проникновения в общественные и государственные политические, экономические и силовые структуры; создание под прикрытием своих агентов в органах власти разветвленных сетей центров и баз по подготовке боевиков, складов оружия и боеприпасов, фирм, компаний, банков, фондов, используемых для финансирования проводимых операций;

- широкое использование наркобизнеса и торговли оружием для пополнения финансовых средств;

- появление тенденции перехода от осуществления отдельных террористических актов к масштабным акциям, приобретающим характер диверсионно-террористической войны, в ходе которой широко применяются методы информационно-психологического воздействия, в том числе для

создания атмосферы всеобщего страха, возбуждения антиправительственных настроений в обществе в целях успешной борьбы за влияние и власть.

Теракты в США отличают:

- необычайно высокий уровень планирования, подготовки и проведения;
- высочайшая синхронизация действий;
- предварительная игра на рынке ценных бумаг в предвидении их обесценивания (кстати, об итогах расследования по этим фактам, а также названия конкретных компаний-игроков так и не слышно);
- демонстрационный характер терактов (разрушение символа мировой банковской системы);
- продуманное до мелочей информационное обеспечение (в том числе, заранее в течение продолжительного времени раскручиваемый символ «исламского фундаментализма») и др.;
- подготовка террористов на территориях как самих Соединенных Штатов, так и ряда развитых стран Европы (Англии, Германии).

Все это позволяет сделать некоторые выводы.

1. Еще до террактов общество оказалось на грани всемирного системного кризиса, существовавщие модели социального устройства полностью себя изжили, а нарастающее недовольство масс грозило вырваться из под контроля и уничтожить «мировое зло».

2. Организация подобного масштабного преступления вряд ли под силу какой-либо из известных террористических организаций (речь идет о десятках миллионов долларов). Только одна подготовка пилотов-камикадзе требует немалых капиталовложений и времени (как минимум год). За это время о планах террористических организаций, и тем более на территории США, должны были бы узнать спецслужбы, агенты которых есть почти в каждой подобной организации.

3. Вероятность, что подобная акция могла быть совершена даже такой крупной и богатой террористической организацией как "Аль–Каеда",

возглавляемой Усамой бен Ладеном, очень мала. Можно лишь утверждать о ее участии.

4. Характер подготовки и проведения операции позволяют предположить, что акции 11 сентября были организованы некой могущественной транснациональной структурой при участии международных финансовых организаций типа Федеральной резервной системы, МВФ, Всемирного банка и т.п. Это косвенно подтверждается молниеносностью и редкой слаженностью действий мировой финансовой элиты сразу после терактов, а также тем, что теракт практически никак не повлиял на экономику и состояние финансовой системы США.

5. Совершенно очевидно, что международный терроризм является инструментом глобальной политики. На протяжении нескольких десятилетий он взращивался структурами соответствующих спецслужб, неправительственных организаций и направлялся для решения различных задач: в Европе руками "Красных бригад" ликвидировались неугодные политики, в Афганистане организовывалось противодействие советским войскам (суннитское движение "Талибан" создавалось под непосредственным контролем США для обеспечения противостояния шиитскому Ирану, Бен Ладен проходил подготовку в центрах ЦРУ), в Чечне действуют формирования, прошедшие подготовку на территориях различных государств, преследующих цели дестабилизации обстановки в России и т.д.; руководство террористическими организациями стало осуществляться спецслужбами не напрямую, а через неправительственные организации.

6. Террористические акты в США 11 сентября 2001 года являются ни чем иным, как крупномасштабной провокацией, преследующей цели:

- Ускорения построения нового мирового порядка: концепция «золотого миллиарда» с последующим переходом от демократии к силовому подходу (диктатуре) в глобальном масштабе при решении любых проблем; ограничение «прав» и «свобод» будет осуществляться и уже осуществляется под предлогом необходимости борьбы с «международным терроризмом». В этом свете следует рассматривать отказ США от подписания Киотского протокола, стремление дезавуировать Договор по противоракетной обороне 1972 года, а также их готовность к отказу от практики подписания тех или

иных соглашений, призванных регламентировать на основе международного права основные принципы современного мироустройства во главе с ООН, падение авторитета которой, инспирированное опять-таки США, наблюдается в настоящее время. Только за первый месяц после терактов в США в разных странах Запада под эгидой борьбы с международным терроризмом был принят ряд законодательных актов расширяющих возможности и права специальных служб по использованию различных средств, которые по ряду характеристик могут быть отнесены к средствам ведения информационной войны (прежде всего, системы типа Carnivore). Сам факт использования панического состояния населения и парламентов этих стран в интересах расширения влияния специальных служб может быть расценен как акт информационно-психологического давления.

- Реализации принципа «разделяй и властвуй» посредством использования США, подконтрольных международным банковским структурам, в качестве инструмента глобальной политики, расширяя понятие «международный терроризм» от отдельного «террориста № 1» до длинного списка арабских стран. В качестве промежуточного результата этой политики можно отметить тот факт, что единственная в Сомали интернет-компания и крупнейший телекоммуникационный оператор были вынуждены закрыться, поскольку они фигурируют в "черном списке" компаний, подозреваемых в поддержке террористов. "Интернет-компания Сомали" и "Аль-Баракат" обвиняются в финансовой поддержки сети организации "Аль-Каеда". Помимо отключения Интернета, серьезные ограничения наложены на международную телефонную связь и услуги по переводу денежных средств: "Аль-Баракат" был крупнейшей компанией, предоставлявшей эти услуги. После того, как администрация Буша опубликовала 7 ноября список 62 организаций, подозреваемых в финансовых связях с "Аль-Каедой", все банковские счеты "Аль-Бараката" были заморожены, а его телефонная сеть лишилась доступа к международному шлюзу, который находится в совместном владении AT&T и British Telecom. И это только начало.

- Глобализации мировой экономики в интересах получения максимальных прибылей международным банковским капиталом в условиях кризиса мировой финансовой системы. Инструмент глобального управления экономикой – война. Под предлогом необходимости объединения усилий и

координации борьбы с международным терроризмом планируется значительно ускорить продвижение идей глобализации. Антиглобалисты будут поставлены в тяжелое положение и будут расцениваться как пособники террористов.

- Совершенствования системы глобального рабовладения - за последнее десятилетие соотношение уровня доходов богатых и бедных, "золотого" и нищего миллиардов планеты не только не сократилось, но заметно увеличилось: с 13:1 в 1960 г., до 74:1, хотя по сравнению с серединой столетия совокупный объем потребления, судя по тем же оценкам ООН, вырос приблизительно в 6 раз. Однако 86% его приходится сейчас на 1/5 часть населения, на остальные 4/5 – оставшиеся 14%. Доля мирового дохода, находящаяся в распоряжении беднейшей части человечества, не просто мала – она имеет тенденцию к уменьшению: в настоящее время примерно 1,3 млрд. людей живут в условиях абсолютной нищеты. Таким образом, в мире помимо западной витрины цивилизации стран семерки существует другой мир, населенный голодным миллиардом.[95] Нищета, дискриминация, безусловно, способствуют проявлениям терроризма, но не являются его главными причинами (в чем очень пытался убедить слушателей В. Познер в одной из своих передач).

Основная причина возникновения феномена международного терроризма кроется не в пресловутом "столкновении цивилизаций"[96], как пытаются нас убедить, не в еще более пресловутой «монополярности» или «многополярности», а в столкновении двух основополагающих концепций мироустройства на планете Земля:

- реализации замысла жизнеустройства в ладу с природой, всех народов друг с другом, когда созданы условия для реализации каждым человеком его генетически заложенного потенциала;

- упорствовании в построении мирового порядка, обостряющего глобальный экологический кризис, когда человечество своими руками уничтожает природу, одни люди живут за счет других, реализуется паразитарная концепция "золотого миллиарда"[97].

---

[95] Р.Г. Яновский. Наука и нравственность. - "Безопасность Евразии", № 2-2000, июль-декабрь. – с. 108-109.
[96] Huntington S. The Clash of Civilization. Foreign Affairs, vol.72, #3, Summer 1993.
[97] Концепция общественной безопасности. – М: 1998.

Именно такого концептуального толкования старательно избегают всевозможные эксперты, политологи и обозреватели.

В этой связи "исламский фундаментализм" действительно представляет собой угрозу ростовщическому Западу. Разве может Запад, развивающийся по библейской концепции, смириться с народами, в Священной книге которых черным по белому написано: "Те, которые пожирают рост (занимаются ростовщичеством – прим. автора), восстанут такими же, как восстанет тот, кого повергает сатана своим прикосновением. Это за то, что они говорили: "Ведь торговля – то же, что рост. А Аллах разрешил торговлю, но запретил рост". (Сура 2, аят 276).

6. Выбор Афганистана в качестве объекта возмездия (при том, что участие Бен Ладена в организации терактов является лишь предположением) полностью укладывается в рамки геополитической стратегии США по расчленению Евразии, отрыва России от Средней Азии, созданию вокруг нее пояса нестабильности, кольца войн малой и средней интенсивности. Налицо использование американскими стратегами чрезвычайной ситуации для реализации своих планов мирового господства. Кроме того, преследуется цель втянуть в длительную конфронтацию с соседями великие державы – Россию, Китай и Индию, создав своим потенциальным конкурентам целый комплекс не только чисто военных, но и экономических, социально-политических и прочих трудностей.

7. Россия занимает ключевое место в планах центров глобального управления. В результате их целенаправленной деятельности за последние 15 лет: разрушен Советский Союз, подорван экономический базис России, сведена к минимуму боеспособность Вооруженных Сил, деморализована большая часть населения и т.д.

Удар, нанесенный по Америке, обязательно будет направлен и на Россию. Чтобы продолжить реализацию своих планов по дальнейшему ослаблению и возможному расчленению нашей страны глобальные центры силы будут предпринимать целый комплекс мер с целью втягивания России в «коллективную» борьбу с «международным терроризмом».

4.7. Операция «Silver Key». Деятельность спецслужб Запада по нейтрализации интеллектуального потенциала ряда стран мира

Вторая половина двадцатого века прошла под знаком противостояния двух сверхдержав - СССР и США, распространивших свое влияние на значительной части политической карты мира. По своему накалу, напряжению ресурсов и бескомпромиссности это противостояние имело характер мировой войны; оно и вошло в историю под названием «Холодная Война».

Спектр противостояния в Холодной войне охватывал практически все сферы жизни общества - от пропаганды, создающей противнику образ «империи зла», до напряженной гонки вооружений, изматывающей экономику противника и имеющей целью создать стратегический перевес. Однако паритет технологий в области вооружения и колоссальная разрушительная сила ракетно-ядерных сил сделали исход прямого вооруженного конфликта неприемлемым для Соединенных Штатов: в случае массированного термоядерного удара территория Северной Америки могла превратиться в радиоактивную пустыню.

В этих условиях ставка была сделана на тайные методы «внутреннего разложения» научно-технического потенциала противника. Успеху этой операции содействовала иллюзорная идеология, на которой была построена внутренняя политика Советского Союза, отдающая приоритет абстрактным идеям в ущерб национальной безопасности. С учетом этой политики, аналитическими центрами США и НАТО была разработана концепция подрывной деятельности, имеющей целью ослабить, а в последствии полностью ликвидировать, интеллектуальный потенциал СССР.

В одном из документов эпохи Холодной войны под общим названием «Silver Key» представляющего собой свод инструкций для разного рода фондов и научных сообществ, разворачивающих свою деятельность в Советском Союзе. В этом документе имелся раздел, содержащий изложение методов подавления интеллектуального потенциала.

Часть задач, определяемых этим документом, приводится ниже.

“False aim” – «Ложная цель». «... Важно навязать противнику ложные ориентиры научных исследований. Для этого можно использовать рекламу

той или иной научной теории, концепции технологического развития, методики исследований. Определив противнику неверное направление исследований (или заведомо недостижимую цель этих исследований) можно нейтрализовать работу целых научных коллективов (лаборатории, КБ, НИИ).

Ложная цель, поставленная перед научным коллективом (или даже перед целой отраслью), является действенным механизмом «омертвления» финансовых и материальных средств, выделяемых на научно-технические разработки... Попутно это дискредитирует в глазах начальства конкретный научный коллектив...

Неверная методика исследований приводит к консервации перспективной научной идеи и способна отбросить противника в той или иной отрасли на годы (и даже десятилетия)...

Психологической обработке легче всего поддаются руководители научных коллективов, которые, как правило, мало разбираются в конкретной тематике и осуществляют лишь общее (партийное) руководство. Однако это не лишает их амбиции «крупного ученого», каждое слово которого коллектив должен воспринимать как руководство к действию... Его (руководителя научного коллектива) можно пригласить на международную конференцию (симпозиум), где исподволь внушить необходимое нам направление исследований... Эффективными являются так же совместные публикации - это привязывает соавторов к определенному научному направлению. Даже если в дальнейшем научная несостоятельность данного направления будет очевидна, «соавтор» все равно будет его отстаивать, используя все (в частности, административные) возможности...».

Другой раздел упомянутого выше документа носит название **“Our Leader” – «Наш лидер»**. В этом разделе предписывается в каждой научной школе, в каждом научно-исследовательском коллективе, для каждого перспективного направления исследований «создать своего лидера». Под «своим лидером» в рассматриваемом документе предполагается человек, ориентированный на «западные ценности». Спектр этого понятия достаточно широк: от национальной принадлежности (желательно, чтобы это был, по меньшей мере, нерусский) до материальной заинтересованности (например, счет в западном банке и вид на жительство в другой стране).

Авторы документа предлагают разные пути продвижения «своего лидера» - зеленая улица его научным публикациям в западных журналах из этих способов - самый примитивный.

«Свой лидер» - фигура весьма полезная. Он может вовремя посоветовать при выборе направления или методики исследований (важный элемент в организации «False aim»); может он при случае и остановить не в меру прыткого начинающего научного сотрудника, шепнув кому надо, что исследования, проводимые этим сотрудником, не представляют научной ценности и, вообще - это бред какой-то, или задержать публикацию статьи. Поле деятельности «своего лидера» в науке весьма широко.

И еще одна рекомендация в упомянутом выше документе.

“Spoilt weapon” – «Испорченное оружие». В этом разделе его пользователям (руководителям «обществ», «фондов», «академий») предлагается сконцентрировать свои усилия на внедрении «рыночных» методов руководства наукой. С неприкрытым цинизмом составители документа утверждают, что русских, не имеющих устойчивых «деловых» навыков, просто захлестнет необузданная стихия рынка. Деньги - испорченное оружие, с которым русские проиграют стратегическую битву за научное лидерство, считают авторы рекомендаций. Деньги помогут на корню скупить научные идеи и технологические разработки, деньги закроют дорогу в большую науку «нежелательным элементам», превращая русскую нацию в отсталую массу мелких торговцев, деньги дадут ключ к обладанию материальными и интеллектуальными ресурсами разоренной страны.

Вообще, «рыночная экономика» - это тот рычаг, при помощи которого аналитики Пентагона и ЦРУ мечтают установить новый мировой порядок, идолом которого станет Золотой Телец. Под знаком Золотого Тельца Соединенным Штатам Америки удалось реализовать известный план бывшего шефа ЦРУ Алена Даллеса - план разложения изнутри великой державы. «Демократические преобразования» и сепаратистские движения региональной номенклатуры, расшатавшие и подорвавшие институты центральной власти СССР, были оплачены долларами, марками, фунтами.

Президент США не скрывал гордости за победу в Холодной войне, когда заявил, что Америка теперь стала единственной в мире сверхдержавой

и должна принять на себя функции по установлению и поддержанию «нового мирового порядка». Этот новый порядок, само собой, должен базироваться на системе ценностей американского образа жизни, где Золотой телец возглавляет пантеон идолов религии стяжательства, насилия и беззастенчивой эксплуатации, прикрываемой демагогией о демократии и общечеловеческих правах.

Однако натовские стратеги прекрасно понимают, что Россия потенциально остается сверхдержавой и в недалеком будущем, преодолев временные экономические и политические трудности, может снова стать грозным соперником США на пути к мировой гегемонии. В преддверии этого нового (и, очевидно, решающего) противостояния наиболее актуальной задачей Запада является наращивание своего научно-технического потенциала и, самое главное, - подавление потенциала своего будущего противника.

Именно поэтому тайная война против интеллектуального потенциала России не ослабевает и приобретает все более ожесточенный характер. К традиционным методам (изложенным, например, в упомянутом выше документе) добавляются методы прямого воздействия: проникновение западных специалистов в космические и ядерные программы России, интенсивная перекупка передовых технологий и разработок, массированная шпионская деятельность западных спецслужб под прикрытием различных «фондов» (типа фонда Сороса), интенсивное разрушение системы образования и науки под видом рекомендаций по «оздоровлению экономики» и даже прямое уничтожение наиболее перспективных ученых и специалистов - все это звенья невидимой войны против возрождающейся России.

Описанная картина тайной войны в науке была бы неполной, если не упомянуть об одной характерной ее особенности. Основным направлением этой войны, ее главным вектором, является именно подрывная деятельность против интеллектуального потенциала противника, а вовсе не развитие собственного научно-технического потенциала.

Иллюстрацией этому может служить создание западными аналитическими центрами специальных банков идей и технологий. В таких

банках аккумулируются различные перспективные научные разработки, идеи и теории, которые остаются в них невостребованными, без дальнейшего развития и реализации.

Этому есть две основные причины. Во-первых, научная элита Запада зачастую не только не может воспользоваться той или иной теорией или научной идеей, но не способна даже понять внутренний смысл и динамику ее развития. В этом случае идея подвергается обструкции и осмеянию. Пользуясь гигантским пропагандистским аппаратом, не сложно внушить «научной общественности» убежденность в абсурдности той или иной научной теории.

Есть и другая, более глубинная причина деструктивного развития западной науки. Что бы не говорили апологеты нового язычества, поклоняющиеся Золотому тельцу, об идеологическом противостоянии Востока и Запада, «тоталитарной империи» и «свободного мира», причиной Холодной войны был передел жизненного пространства и, как следствие, ревизия итогов Второй мировой войны. Обществу непомерного потребления «цивилизованного» Запада необходимы источники сырья, энергоресурсы, дешевая рабочая сила, удаленные от процветающих городов Запада места свалок радиоактивных и токсичных отходов и полигоны для размещения экологически опасных производств. Западная цивилизация превратилась в вампира, высасывающего жизненные соки других народов. В качестве основной жертвы аналитики «свободного мира» видят Россию.

4.8. Сценарий учений вооруженных сил США по отработке приемов ведения информационной войны

Настоящий материал является одним из сценариев военных игр, проведенных в 1995 году сотрудниками корпорации RAND (США). К этим играм привлекались ведущие специалисты США в области компьютерной безопасности из корпораций, государственных организаций и Министерства обороны США. На учениях отрабатывались вопросы выработки стратегии защиты США в случае развязывания информационной войны. В качестве потенциального противника рассматривался Иран. Естественно, что борьба шла вокруг Персидского залива и нефтяных месторождений – области

извечных «жизненных интересов» Соединенных Штатов. Этот материал приведен в качестве примера возможного сценария информационной войны.

Политический фон

Сейчас середина весны 2000 года.

В конце 20 века политические изменения и продолжающиеся волнения в регионе Персидского залива, в Пакистане, в исламских странах бывшего Советского Союза и Северной Африке привели к созданию нового и очень беспокойного региона, который часто назывался "исламской кризисной дугой".

Проблем для США и европейских стран добавило и то, что один из потенциальных агрессоров в регионе разработал средства использования Глобальной Информационной Инфраструктуры (GII) для проведения стратегических военно-политических операций.

Сложившаяся ситуация вызвала особенное беспокойство в США о безопасности и секретности Национальной Информационной Инфраструктуры (NII) и сложившейся Оборонной Информационной Инфраструктуры (DII).

В 90-е годы произошла Сотовая революция из-за быстрого появления групп низкоорбитальных и стационарных спутников, таких как Iridium, GlobalStar и Teledesic обеспечивших доступность глобальных коммуникаций через сотовые телефоны. По оценкам около 25% населения США, Европы и Японии используют сотовые телефоны в повседневной жизни. Аналогичный рост использования сотовых телефонов наблюдается и в других регионах.

Интернет стал основной инфраструктурой как для NII, так и для GII. Теперь все страны имеют собственные интернет-порталы. Установлено, что около 70% всего населения планеты находится на расстоянии телефонного звонка от шлюза в Интернет.

Феномен WWW продолжает усиливаться, уже создано около 40 миллионов "домашних страниц" информации, обеспечивающих ссылки на базы данных по всему миру. Многие из этих страниц включают файлы с видео и аудиоизображениями, специально сделанными удобными для воспроизведения.

Одной из самых значительных тенденций в последнем десятилетии стал рост электронной коммерции. Приблизительно треть всех коммерческих сделок в США производится электронным способом как с помощью стандартных средств обмена данными, так и специальными средствами взаимодействия между компаниями, реализовавшими большое число стандартов шифрования.

Попытки правительства США установить стандарт аппаратного шифрования (аналогично инициативе CLIPPER CHIP) потерпели неудачу из-за противодействия со стороны общественных организаций и компаний-разработчиков программных продуктов.

NII и GII активно используются новым поколением активистов из различных политических групп. Многие такие группы объединены транснациональными сетями связи, с помощью которых они обмениваются информацией по вопросам окружающей среды, гражданских прав и многим другим темам.

Интернет и WWW стали объектом исследования программными "агентами" различных типов. Десятки тысяч таких агентов были созданы для сканирования Интернета и WWW-страниц в поисках элементов, соответствующих профилю интересов их пользователей или блокирующих такой доступ.

В 1998 году президент разрешил передавать в мирное время основную часть информационных потоков Министерства обороны и административных данных по коммерческим телефонным сетям и общественным сетям передачи данных. Поэтому теперь основной поток данных в DII передается по коммутируемым сетям, используя различные уровни шифрования для защиты секретной информации.

В период с 1995 по 2000 года было предпринято несколько, в основном неудачных, попыток повысить безопасность коммутируемых телефонных сетей. Эти усилия были затруднены тем, что телефонные сети находятся в собственности и обслуживаются большим числом конкурирующих компаний, включая кабельные сети, сотовые сети и спутниковые каналы, поэтому нужные изменения оказалось тяжело реализовать. В результате безопасность телефонных сетей, за исключением использования

межконцевого шифрования канала связи договорившимися сторонами, практически не увеличилась с 1996 года.

Эта проблема усложнялась несколькими тенденциями:

- широким распространением открытых стандартных систем, чьи протоколы и техническое описание являются широко известными;
- использованием удаленного управления и обслуживания из-за его дешевизны (то есть через коммутируемые порты) в телекоммуникационных и энергетических системах;
- повышением доверия между различными провайдерами телефонного сервиса;
- более частыми изменениями в программном обеспечении телефонных сетей из-за конкуренции, вызываемыми появлением новых особенностей.

В 1998 году возможность создания в США «Минимально Необходимой Информационной Инфраструктуры» (MEII) - для того, чтобы существовали "запасные пути на скоростном информационном шоссе" в случае возникновения различных аварийных ситуаций - стала предметом серьезных дискуссий. Главной причиной возникновения предмета дискуссий явилось понимание необходимости наличия такой инфраструктуры для поддержки широкомасштабных операций вооруженных сил США и Многонациональных сил.

Хотя дискуссии по поводу разработки различных архитектур MEII и критериев их работоспособности продолжаются, серьезная работа по созданию реальной MEII еще не началась. Существуют значительные расхождения во мнениях по поводу того, что следует включать в эту структуру. При этом основные дискуссии ведутся относительно следующих вопросов:

- нужно ли защищать только военные и иные коммуникационные каналы и информационные системы для успеха основных операций сил быстрого реагирования или нет;
- повлияет ли защита другой инфраструктуры информационных систем на простое население США или нет;

- этот же вопрос в отношении защиты информационных систем союзников и потенциальных партнеров по коалиции.

Также идут широкие дебаты по вопросу способности поддерживать надежность и эффективность MEII, которая будет разработана, в основном из-за динамического характера продолжающейся информационной революции.

В свете всего вышеописанного, в последние несколько лет все больше осознавалась растущая зависимость от телефонной сети системы подачи электричества, сетей передачи данных, обеспечивающих управление воздушным движением, системы глобального позиционирования и других ключевых элементов инфраструктуры США. Как следствие - Агентство Национальной Безопасности (АНБ), спецслужбы и правоохранительные органы в США (а также в других странах) выделяют все большие ресурсы в попытках оценить и противостоять национальным и международным угрозам применения информационного оружия.

Основные особенности ситуации в мире в контексте безопасности

Тяжелое положение в Саудовской Аравии

Правительство Саудовской Аравии недавно сделало ряд шагов для создания в этой стране общества открытого политически, экономически и социально. Новые независимые широковещательные телевизионные центры вещают с помощью направленных спутниковых приемников и сотовых телекоммуникационных систем. Различные слои общества все больше используют доступ в Интерент.

Саудовской монархии был нанесен большой урон из-за внутреннего раскола после смерти в 1997 году короля Фахда. Его слабый наследник сейчас борется как за установление своей власти в семье, так и за сплочение своего королевства, которое раздирается растущими противоречиями между оппозиционным движением исламских фундаменталистов и "модерн-националистов", которые сейчас доминируют в саудовском правительстве.

С 1998 года большая часть саудовской оппозиции (особенно в университетах) стала разделять цели и задачи становящейся все более значимой Кампании за Исламское Обновление и Демократию (CIRD). Международная коалиция CIRD, созданная в 1997 году на встрече исламских

государственных и общественных организаций в Дамаске, стала серьезной силой определяющей социальные и политические изменения в Персидском заливе, а также во всем исламском мире. CIRD хорошо финансируется, в основном из североамериканских и европейских исламских источников, а также из национальных источников в Саудовской Аравии, Иране и Пакистане. CIRD использует разнообразные информационные и коммуникационные технологии для организации, финансирования, выступлений в средствах массовой информации и установлении связей с организациями в исламском мире и с общественными организациями. Несколько лидеров CIRD имеют большое влияние на исламистов в Северной Америке.

Цены на нефть оставались стабильными в 90-е годы, что заставило саудовскую монархию урезать амбициозные национальные и социальные программы, выдвинутые для достижения национального примирения.

Саудовский режим серьезно обеспокоен своей уязвимостью в отношении общей безопасности и финансов после того, как в начале 1998 года Банк Саудовской Аравии был ограблен на 1.2 миллиарда долларов с помощью хитроумной электронной атаки, которая в течение двух месяцев успешно использовала ряд технологий "ограбления банка из киберпространства" перед тем, как была выявлена британской финансовой службой безопасности. Позднее саудовское правительство обнаружило серьезные доказательства причастности к этой атаке Ирана и Сирии.

Финансовое положение саудовской монархии осложняется еще и мнением, сложившимся в кругах правительства, которое диаметрально противоположно мнению сторонников CIRD в том, что оборонная мощь страны должна оставаться высокой перед лицом все возрастающей военной и политической силы Ирана.

Господство в Персии

Мощь и влияние Ирана в Персидском заливе сильно возросли после начала гражданской войны в Ираке из-за внезапной смерти Саддама Хусейна. В результате очень умелого вмешательства Ирана в эту гражданскую войну Ирак по существу расчленен. Слабое центральное пост-баатистское правительство находится в Багдаде, а курды на севере и шииты на юге имеют свои автономии.

Иран открыто поддерживает радикальные исламистские фундаменталистские группы в большинстве стран Персидского залива и пропагандирует панисламистскую стратегию создания широкомасштабной военно-политической коалиции для сопротивления гегемонии Америки и Европы в исламском мире.

Намерения Ирана создать свое атомное оружие широко известны, хотя на настоящее время нет доказательств того, что иранцы имеют готовые ядерные бомбы. Иранцы продолжают поддерживать свою быстро развивающуюся ядерную инфраструктуру, которая находится под контролем МАГАТЭ - для "мирного использования атомной энергии".

Иран продолжает наращивать свой арсенал средств доставки оружия, который сейчас включает:

- 36 русских Ту-22М BackFire;
- 20 северокорейских ракет HoDong II;
- 200-300 ракет HoDong I.

Доказательства того, что Иран разрабатывает информационное оружие, появились в 1999 году. Тогда в Индии три сотрудника одной фирмы (включая программиста мирового класса) были арестованы полицией после проникновения в, считавшуюся защищенной, индийскую компьютерную сеть военного назначения. Они признались, что продали Ирану ряд средств ведения информационной войны.

У Ирана имеются сложные взаимоотношения с CIRD, который сопротивляется попыткам Ирана сделать его более фундаменталистским. Кроме того, ряд лидеров CIRD в частных беседах критикуют медленные темпы демократизации в Иране. Тем не менее, разведывательные источники сообщают, что Иран финансирует отдельные группы в коалиции CIRD.

Алжир

Популярность правления в стране военными увеличивалась в 1996 году, в июне 1996 года происламистская группа полковников, совершив переворот, пришла к власти вместо "римской коалицией" оппозиционных групп. В конце 1996 года в результате выборов в стране было формально создано исламское правительство.

Летом 1998 года отношения между Алжиром, США и Европой начали ухудшаться по мере того, как алжирский режим стал проводником геостратегических и политических интересов Ирана и военное сотрудничество между двумя этими странами стало более широким.

Летом 1999 года французские разведывательные службы получили информацию о предположительной установке компьютерного "троянского коня" в последнюю версию программного обеспечения управления самолетом AB-330 AirBus Industries, судя по всему, алжирскими агентами во Франции, действующими по указаниям Ирана. Расследование установило, что Aerospatiale пользуется услугами нескольких индийских субподрядчиков при разработке программ, которые имели доступ к считавшимися "безопасными" компиляторам и исходным текстам программ.

Ливия

В ноябре 1998 года при инспектировании нового завода по производству химического оружия в южной Ливии президент Каддафи получил серьезные травмы в результате аварии вертолета и вскоре после этого умер. В последовавшем после этого политическом хаосе победу одержало исламистское правительств, которое быстро установило контроль над страной.

Для многих наблюдателей явилось сюрпризом, что новое ливийское правительство взяло курс на проведение выборов и "исламскую демократию". Оно теперь считается одним из наиболее серьезных сторонников CIRD в борьбе за создание единой исламистской политической силы.

Пакистан

В 1997 году режим Бхутто был свергнут в результате военного переворота из-за "политической нерешительности и неадекватной военной помощи" во время подавленных волнений в Кашмире в конце 1996 года.

После смены режима Бхутто военное правительство стало проводить активный исламистский курс и сильно расширило военно-политические связи с Ираном.

Израиль и арабы

Израиль подписал мирные соглашения с Сирией и Ливаном в 1997 году. Летом 1999 года израильское правительство стало объектом (по

терминологии Моссад) воздействия "нового вида стратегического оружия" - серии электронных атак на военные системы управления и связи Израиля с помощью хитроумных анализаторов пакетов и логических бомб неизвестного происхождения.

Российская Федерация

К власти пришли националисты на выборах 1996 года и стали предпринимать шаги по объединению страны и "ближнего зарубежья".

В 1997 году в Министерстве обороны было создано новое командование радиоэлектронной борьбы в обязанность которому была вменена "разработка средств ведения как наступательной, так и оборонительной информационной войны в 21 веке". Попытки русских разработать информационное оружие отчасти являлись подтверждением продолжающихся национальных проблем использования все более сложных технологий "бандитов киберпространства" русской организованной преступностью. Когда такие атаки внутри России были подавлены, преступники начали проводить успешные атаки на американские и европейские банки (ущерб от которых составил около 2 миллиардов долларов в 1999 году). Правоохранительные органы США и Европы сильно подозревают, что некоторые "хакерские таланты мафии" перешли на службу в русские разведывательные службы.

Китай

Жесткое, прагматичное и националистическое руководство, которое консолидировало страну после Дэн Сяо Пина, продолжает вести Азию по пути экономического роста.

Среди политического и военного руководства Китая существует мнение, отражающее все увеличивающуюся самостоятельность Китая, что Китай должен стать "второй по величине военной мощи в мире державой" в начале 21 века.

Новой "стратегической ценностью 21 века" является профессионализм нового поколения китайских компьютерных специалистов, которые в состоянии обеспечить китайские торговые и финансовые круги и правительство оборонительными и наступательными средствами ведения информационной войны мирового класса.

Япония

Интерес японского правительства к потенциальным угрозам, связанным с информационным оружием, сильно возрос после "большого кризиса йены 1998 года", когда курс йены после двухдневного падения зафиксировался на 22% от прежнего курса. Только несколько месяцев спустя после этого были найдены доказательства того, что стремительное падение йены было отчасти вызвано очень хитрым компьютерным вирусом, авторами которого является альянс нескольких китайских и азиатских преступных группировок.

Корея

Ким Джонг Ил продолжает удерживать основные рычаги власти в КНДР, хотя идет внутренняя борьба между ним и различными группами в северокорейской элите, которая продолжает сопротивляться попыткам объединения.

Реализация соглашения 1994 года между США и КНДР о ядерной программе идет с трудом, но продолжает рассматриваться как средство заморозить ядерную программу Северной Кореи. Тем не менее, КНДР ведет разработку и производство примитивных ракет и участвует в обширной программе по сотрудничеству с Ираном в области разработки и экспорта ракет.

США

После драматических выборов президента в 1996 году, верхние эшелоны власти пришли к общему мнению, что США должны продолжать поддерживать представление о себе, как о "мировом жандарме". В то же время общественное мнение в США из-за острых национальных проблем сильно настроено против финансирования дорогостоящих военных проектов. В этой сложной политической обстановке в 1997 году появился Консорциум за Планетарный Мир (CPP), необычная политическая коалиция "зеленых", пользующаяся поддержкой как правых, так и левых, и придерживающаяся следующих взглядов:

1) роль "мирового жандарма" противоречит национальным интересам США;

2) следует применять "современные методы улаживания конфликтов" в международной политике.

При поддержке большого числа групп борцов за мир, за гражданские права, за экологию и других активных групп CPP быстро стал организующим началом для групп подобного рода в США, Канаде и Мексике. Используя Интернет для координации действий, ими была проведена операция по улаживанию острого политического конфликта в южной Мексике. В конце 1998 года CPP имел большой престиж из-за роли, которую он сыграл при подписании мирного соглашения между мексиканским правительством и движением "третья запатистская революция".

Добившись успеха в Мексике, CPP за прошлый год стал активным участником "миротворческих коалиций" в ряде региональных конфликтов во всем мире (в ходе которых он установил тесные неформальные связи с исламской коалицией CIRD).

В 1998 году в рамках КНШ была создана организация с задачей контроля за разработкой оборонительных и наступательных операционных концепций "технологии электронной войны" и новых требований к ней. Эта организация работает с различными группами по созданию дополнений по планированию ведения РЭБ или информационной войны для стратегических военных планов. Проблемы с контролем над нераспространением ядерного оружия привели в 1998 году к серьезному пересмотру планов структуры ВС США с целью оставить место пакету инициатив, направленных против его распространения:

1) проект создания высотной системы ПВО на всем ТВД;

2) большие продажи за рубеж ракет «Пэтриот» и обычных тактических анти-ракет;

3) ускоренная разработка беспилотных самолетов с большой продолжительностью полета и дополняющих автоматизированных систем датчиков наземного базирования многоцелевого назначения.

В конце 1999 года из-за описанного ранее инцидента с компанией French AirBus авиакомпании США провели обследование программ, разрабатывающихся для использования в системах управления полетом, для получения гарантий его целостности. Кроме нескольких мелких ошибок в программах, ничего найдено не было - но это привело к усилению бдительности в авиастроении в отношении защиты этих систем.

Безопасность в Персидском заливе

В 1999 году перед лицом все увеличивающейся политической и военной мощи Ирана, США, Франция и Великобритания обновили военное соглашение.

Теперь военные планы для региона включают переброску большого числа дополнительного военного оборудования в регион и обязательства по быстрому развертыванию под кодовым названием «Грин Хорнет» для США и «Силвер Сейбр» - для Великобритании и Франции.

британская аэромобильная дивизия и французская моторизованная дивизия вместе с несколькими эскадрильями тактических перехватчиков составляют основные европейские военные компоненты «Силвер Сейбр».

В 1998 году КНШ одобрил план действий при информационной войне, включающий как электронные, так и физические атаки: «Операция Форсе Филд» - основной план борьбы с системами управления на всем ТВД, который должен обеспечить "информационное доминирование в радиусе 500 км" и, в частности, сделать неработоспособными ключевые элементы систем управления войсками, ПВО и тактической разведки будущего противника.

Кризис

4 мая 2000 года министры ОПЕК на встрече в Каракасе пересмотрели политику добычи и продажи нефти. Иран, Ирак, Ливия и Алжир решили резко сократить производство с целью довести цену минимум до 60 долларов за баррель.

Каракасская встреча закончилась ничем после трех дней яростных дискуссий, заметных особенно в телевизионной трансляции встречи министров Ирана и Саудовской Аравии.

7 мая Иран заявил, что он вскоре будет проводить военные учения из-за эскалации ситуации в заливе.

8 мая глава Саудовской Аравии встретился в послом США и высказал свою глубокую озабоченность действиями Ирана, который, как он опасается, может использовать проблемы в ОПЕК как предлог для усиления своей военной мощи в заливе.

10 мая тегеранское радио и телевидение объявило, что министр иностранных дел Ирана вылетел в Райад с инициативами, которые помогут разрешить противостояние в ОПЕК и снизить напряженность в регионе.

Вечером этого же дня посол США в Саудовской Аравии узнал содержимое иранских инициатив:

•Иран, Ирак, Саудовская Аравия и другие страны консультативного совета Персидского залива (GCC) должны немедленно сократить добычу нефти на 20%.

•страны GCC должны расторгнуть свои военные соглашения с США и заявить о своем нейтралитете или отсутствии связей с США.

•в ответ Иран заявит, что страны GCC находятся под защитой иранской системы безопасности в Персидском заливе.

На следующий день, 11 мая, разведка США обнаружила подготовку к мобилизации трех из шести иранских дивизий, размещенных возле Дезфула в юго-западном Иране, включая мобилизацию нескольких полков, оснащенных мощными тягачами, способными быстро перебрасывать бронетехнику и артиллерию.

11 мая в 20:30 по местному времени, Саудовская Аравия начала развертывание одной мотострелковой дивизии на границе с Ираком и частичную мобилизацию резервистов. Двумя часами позже Кувейт перевел свою армию в повышенную готовность.

Позднее ночью Каир на несколько часов почти лишился электроэнергии (на 90%). Посол США в Каире в своем сообщении отметил, что "непонятно, что явилось причиной аварии - случайность или саботаж"

Вечером 11 мая Кризисный Центр Белого Дома получил сообщение от посла США в Райаде о том, что в телефонной сети Райада произошла серия серьезных сбоев.

Центр Национальных Коммуникаций США сообщил, что почти одновременно с авариями в Саудовской Аравии основная телефонная сеть в Форт-Льюисе стала объектом серьезной телефонной атаки с помощью персональных компьютеров - по-видимому начавшейся с АТС для работы

BBS, которая имела входные телефонные линии - которая парализовала работу телефонов на несколько часов.

По поводу проблем в Саудовской Аравии ЦРУ сообщило о подозрениях, что использовался люк в программе, который, судя по всему, был вставлен в последнюю версию программ для управления основными АТС в Саудовской Аравии. Этот код позволяет использовать неавторизованные пароли для получения доступа при удаленном техническом обслуживании АТС. Причины этой проблемы неизвестны, хотя радикальная анти-американская группа взяла на себя ответственность и сообщила об этом по Интернету.

12 мая в 5 часов утра в Заливе две саудовские канонерские лодки были обстреляны иранскими боевыми судами, которые явно находились в разведке у берега Эль-Дубай.

Через несколько минут появились 12 саудовских F-15 и в завязавшемся сражении обе саудовские канонерские лодки и три иранских судна были потоплены. После этого появились 15 иранских Миг-29 и Миг-31 - в результате были сбиты 9 иранских самолетов и 5 саудовских F-15.

В 6:30 по местному времени S-3B Viking с корабельной группы «Рональд Рейган» был сбит иранским ракетным фрегатом при проведении им разведывательного полета в воротах Ормуз.

Через 30 минут F/A-18 и F/A-14 с корабельной группы обнаружили фрегат пятнадцатью милями южнее Бандара-Аббаса.

Самолеты США вступили в бой с 8 иранскими МИГ-29. После короткой схватки 3 МИГ-29 были сбиты, а фрегат затонул после попадания в него 3 ракет «Гарпун».

13 мая в 11:00 на самом большом нефтеперегонном заводе ARAMCO возле Дхахрана произошел катастрофический выход из строя системы управления, который привел к колоссальному взрыву и пожару в районе новых баков для перегонки. За этим последовало заявление радикальной исламистской группы, связанной с Ираном, что "враги ислама вскоре почувствуют всю мощь воинов ислама". Это заявление завершалось фразой, что "экономика Саудовской Аравии может быть поставлена на колени простым нажатием кнопки".

В своем отчете посол США в Саудовской Аравии предупредил, что саудовская элита крайне напугана перспективой того, что Иран может нанести серьезный урон экономике, даже без единого выстрела и начинает сомневаться в способности США помочь саудовском правительству справиться с новой угрозой.

На пресс-конференции 13 мая министр иностранных дел РФ призвал Совет Безопасности ООН урегулировать конфликт.

14 мая в 7:30 по местному времени Иран разослал сообщения всем членам GCC, а также США, Франции и Великобритании, в котором требовал:

- прекращение огня всех сил обоих сторон;
- немедленное замораживание дальнейшего развертывания "зарубежных военных сил" в регионе;
- немедленную встречу на нейтральной территории для "обсуждения мирного разрешения кризиса".

Заявление заканчивалось фразой о том, что "если не будет положительного ответа в ближайшие 12 часов", то Иран "предпримет действия в соответствии с его правами и обязанностями в Персидском заливе".

В заявлениях лидерам Кувейта и Саудовской Аравии была также фраза о том, что Иран вскоре продемонстрирует тщетность опоры на американских империалистов при защите от современного оружия.

Вскоре после полуночи Иран запустил 3 ракеты HoDong I с полигона вблизи Тегерана. Две из трех ракет успешно достигли верхних слоев атмосферы, продемонстрировав неизвестные ранее возможности Ирана.

14 мая в 18:12 новый скоростной пассажирский немецкий поезд «Зигфрид», имевший скорость 300 км/ч, столкнулся с направленным на неправильный путь грузовым поездом возле Франкфурта-на-Майне.

Германская федеральная полиция установила, что при столкновении погибло 60 человек и серьезно пострадало еще 120.

Через 3 часа ЦРУ сообщило, что имеются прямые доказательства того, что грузовой поезд был направлен на тот же путь, что и пассажирский с

помощью проникновения в систему управления железной дорогой «Бундесбах».

В середине дня 15 мая на приеме, организованном с помощью СРР, посол Ирана в ООН нечаянно сказал, что США и Европа, как самые технологически развитые регионы на планете, очень уязвимы к атакам 21 века, организуемыми государствами, владеющими современными компьютерными и телекоммуникационными технологиями.

Позднее 15 мая в предварительном отчете DCI о крушении немецкого поезда было указано, что в компьютерную систему была помещена логическая бомба, возможно кем-то из своих, и следы ведут в Иран.

При передаче отчета Президенту этим вечером Советник по Национальной безопасности (NSA) отметил, что АНБ имеет серьезные подозрения относительно происхождения атаки. Более того, он заметил, что центр ЦРУ по борьбе с международным терроризмом приготовил отчет, в котором высказываются сильные подозрения относительно того, что эта трагедия была результатом деятельности тайной организации, которая может быть связана с событиями с Персидском заливе.

16 мая в 11 часов директор Скотланд-Ярда сообщил премьер-министру Великобритании, что Bank of England обнаружил три пакетных анализатора нового образца в своей основной сети для передачи электронных денег и, что руководство банка очень обеспокоено тем, что неавторизованные люди смогли проникнуть в систему передачи электронных денег, до этого считавшуюся неуязвимой.

Через несколько часов в Атланте и Лондоне CNN и ITN в специальном выпуске рассказали о крушении немецкого поезда и проблемах в системе передачи данных Bank of England. В сообщении CNN было сказано, что некоторые западные разведывательные службы полагают, что Иран мог нанять компьютерных экспертов у русской мафии и в Индии для того, чтобы создать угрозу всей экономике США и Западной Европы.

Эффект от этих сообщений был усилен интервью с большим числом экспертов по компьютерной безопасности.

Индекс на Лондонской бирже упал на 10% в результате того, что инвесторы стали вкладывать деньги в более безопасные места.

В 14:30 16 мая на Нью-Йоркской бирже разразился сильнейший кризис после 1987 года. Индекс Доу упал к концу дня на 17 процентов. Аналитики CNBC и других сетей деловой информации делают выводы, что основные инвесторы пытаются уйти с рынка, управляемого с помощью вычислительной технике.

К 15:00 цена на нефть достигла 75 центов за баррель. Золото возросло в цене на 10 процентов.

В 17:00 кризисная группа SEC информировала секретаря по торговле, что имеются признаки того, что имели место манипуляции инвестициями, осуществлявшиеся через европейские и ближневосточные банки, и именно они явились главной причиной быстрого падения индекса Доу.

Этой ночью имело место прекращение подачи электричества в район Германии, в котором находится авиабаза США на Рейне. Хотя электроснабжение было быстро восстановлено, имеются признаки того, что причиной сбоев было проникновение в систему управления энергосистемой.

Ночью 17 мая CPP объявил мобилизацию всех членов в течение следующих 48 часов, чтобы остановить ненужную и потенциально кровопролитную войну.

Двумя часами позже CPP послал формальный запрос на митинг 21 мая для демонстрации поддержки против интервенции США в Саудовскую Аравию с числом участников около 100 тысяч.

Аналогичные запросы были посланы в полицию в 10 других городах США.

Заявки CPP были одобрены, и началась мобилизация членов CPP через средства массовой информации и Интернет.

В начале вечера 18 мая после получения сообщений о массированном вторжении вооруженных сил Ирана в южный Ирак, увеличения активности Ирана на море вблизи ворот Ормуза и "стратегического предупреждения" Ирана КНШ послал сообщение, рекомендующее немедленно приступить к фазам 1 и 2 плана «Грин Хорнет» по развертыванию союзных сил в Персидском заливе.

В 14:40 в Делавере в телефонной сети также произошел ряд сбоев из-за атак неизвестного происхождения. Основной целью атак были АТС, чей выход из строя приводил к невозможности управления воздушным движением на авиабазе «Довер».

В 15:00 была проведена экстренная встреча NSC для выработки рекомендаци при решении кризиса в Персидском заливе.

Встреча началась с заявления представителей разведки, описавших сложности с установлением источника атак и отметивших, что пока нет возможности узнать наверняка, являются ли происходящие события:

- проверкой стратегических возможностей информационного оружия кем-либо;
- началом информационной операции по срыву планов развертывания войск США в Персидском заливе;
- максимальным эффектом от стратегической информационной операции, организованной Ираном;

Проблема усложняется тем, что антиинтервенционистские группы как в США, так и в Европе могут стать организаторами большого числа инцидентов с применением информационного оружия.

Председатель КНШ подчеркнул, что план по развертыванию очень сильно зависит от способности оперативного взаимодействия частей и не сможет быть выполнен вовремя при невозможности этого. Он также выразил озабоченность в отношении проблем с мобилизацией самолетов и экипажей ВВС, являющейся ключевой при выполнении фазы 2 плана «Грин Хорнет», которые могут возникнуть, если кто-либо сможет проникнуть с систему управления основными авиалиниями США.

В завязавшейся дискуссии стало ясно, что хотя есть косвенные доказательства причастности Ирана к происходящим инцидентам, сохраняется неопределенность относительно степени участия в них Ирана.

После этого перешли к военной ситуации в Персидском заливе и Президент принял следующее решение:

- приступить к фазам 1 и 2 плана «Грин Хорнет»;

•развернуть половину имеющихся сил CONUS в Египте и Саудовской Аравии;

•организовать видеоконференцию с британским премьер-министром и президентом Франции для выработки соглашения с этими правительствами по выполнению плана «Силвер Сейбр»;

•немедленно собрать Североатлантический совет;

•отвергать любые дипломатические инициативы от Ирана и CIRD.

Президент также отметил, что он хочет получить разрешение Конгресса на свои действия. После этого он начал более глубокое обсуждение ситуации, сложившейся после применения информационного оружия. Президент выразил озабоченность последствиями возможных успешных атак против США и их союзников в Персидском заливе и национальной информационной инфраструктуры США, а также их европейских союзников и коалиционных партнеров в Персидском заливе. Он подчеркнул необходимость продемонстрировать чем скорее, тем лучше, что дальнейшие информационные атаки, такие же, как те, что уже имели место, не смогут серьезно помешать военной стратегии США в этом кризисе.

В ходе этого обсуждения Президент потребовал от пресс-секретаря прекратить спекуляцию относительно уязвимости США к атакам из киберпространства и происхождения этих атак. Он отметил, что дальнейшие решения могут оказаться более трудными, если в обществе начнется паника относительно угрозы информационного оружия для США и они будут связываться с Ираном, когда их настоящим источником могут являться антиинтервенционистские политические силы.

Эскалация конфликта

Утром 20 мая Сенат США дал разрешение на посылку войск в Персидский залив. Этим утром банкоматы самого большого банка в Джорджии вышли из строя из-за постоянных ошибок порядка тысяч долларов при каждой транзакции. Это заставил банк закрыть всю сеть банкоматов.

Официальные лица банка заявили, что это действия своих сотрудников, так как они недавно установили новую версию программ в банкоматы и подозревают наличие логической бомбы, включенной каким-то образом.

вскоре после полуночи центр CNN в Атланте вышел из строя на 12 минут.

20 мая Министерство обороны обнаружило, что компьютерная база данных для плана развертывания сил серьезно искажена. В предварительном отчете КНШ было указано, что компьютерный червь не установленного происхождения попал внутрь программы работы с этой базой данных через персональный компьютер, временно подключенный к системе, где находилась эта база, на котором был запущен популярный коммерчески пакет для работы с базами данных, имевший известное уязвимое место.

Утром 21 мая посол США в Египте уведомил госсекретаря, что президент Египта очень обеспокоен возможностями Ирана нанести экономический и политический урон Египту.

Утром Пентагон впервые столкнулся с проблемами из-за задержек в развертывании сил в Заливе из-за информационных атак на ЛВС и АТС в ряде главных авиабаз и военно-морских баз.

Вскоре после полуночи 21 мая в новом самолете АВ-340, совершающем полностью автоматическую посадку в аэропорту О'Хара, произошел выход из строя систем управления, и через несколько минут он разбился, убив 236 пассажиров и 36 человек на земле.

После этого FAA запретило полеты всех последних моделей АВ-340 и 330 из-за подозрений на то, что программное обеспечение могло быть заражено сложной логической бомбой.

Этим вечером Министерство юстиции сообщило об аресте двух подозреваемых в программистской фирме в Сан-Антонио, которая делала последние изменения в программах управления полетом для АВ-340 (оба недавно получили большие суммы денег через шведский банк). Хотя тексты программ тщательно исследовались перед установкой, подозреваемые имели доступ к компилятору и, видимо, модифицировали его таким образом, что скомпилированная им программа начинала выполнять незапланированные команды.

21 мая в Вашингтоне прошла анти-интервенционистская демонстрация в которой приняло участие около 400 тысяч человек. Также прошло большое число демонстраций в ряде других городов страны.

На утренней встрече 22 мая Президент был уведомлен о планах:

- операция «Айрон Ланс» - упреждающий ракетно-бомбовый удар по силам Ирана, угрожающим Саудовской Аравии;
- операция «Форсе Филд» - план атаки на системы управления войсками.

Планы были обсуждены, но пока по ним не было принято никакого решения.

В 19:20 22 мая в ходе трансляции новостей двумя правительственными ТВ-сетями на экранах неожиданно появилось изображение главы CIRD, призвавшего граждан Саудовской Аравии свергнуть монархию. Начались широкомасштабные демонстрации против Саудовской монархии в Райаде, Джиддахе, Мекке и Дхахране.

В тот же день телефонная сеть в Саудовской Аравии опять вышла из строя. Причиной снова была неавторизованная модификация систем через «люки» в программах, управляющих ими АТС, которые были похожи на те, что уже были причиной более ранних сбоев в телефонной сети (саудовская телекоммуникационная сеть была приобретена у компании, производящей около 30% всего телекоммуникационного оборудования для США).

Этим вечером сторонники само-провозглашенной временной исламской республики Аравии захватили власть в Дхахране и Мекке.

Этим вечером начались серьезные столкновения в Райаде между полицией и членами национальной стражи, которая заявила о поддержке новой республики. Посол США сообщил о попытке государственного переворота.

Утром 23 мая КНШ сообщил о полномасштабной информационной атаке из неизвестных источников против почти каждой военной базы США, задействованной в планах «Грин Хорнет» и «Силвер Сейбр». В отчете открыто сообщалось, что весь план развертывания провалился к чертям, и они не знают, как спланировать теперь развертывание.

Утром в Атланте была организована пресс-конференция СРР, на которой его представители заявили, что СРР мобилизует всех своих членов для проведения акций гражданского неповиновения, чтобы остановить действия правительства США по развязыванию войны, а также для поддержки недемократического режима Саудовской Аравии.

В 12:30 на Чикагской товарной бирже произошли самые большие беспорядки за всю ее историю. Торговля остановилась полностью из-за того, что биржа стала жертвой серьезного электронного манипулирования неизвестными лицами.

В полночь телефонная сеть в районе Балтимора, включая все сотовые системы, вышла из строя. Атака была совершена с помощью «люков», похожих на те, что вызвали выход из строя телефонной сети в Саудовской Аравии. Предварительное расследование установило, что только около 70% АТС отключено, но оставшиеся - сильно перегружены.

Что будет дальше?

Литература

1. Батурин Ю.М., Жодзижский А.М. Компьютерная преступность и компьютерная безопасность. - М.: Юридическая литература, 1991.- 169 с.
2. Большаков А.А., Петряев А.Б., Платонов В.В., Ухлинов Л.М. Основы обеспечения безопасности данных в компьютерных системах и сетях. Часть 1. Методы, средства и механизмы защиты данных.- СПб.: Конфидент, 1996.- 166 с.
3. Викторов А.Ф. Информационная война в современных условиях // Информационное общество. - 1997. - №1.- С. 58-59.
4. Герасименко В.А. Комплексная защита информации в современных системах обмена данными // Зарубежная радиоэлектроника. – 1993. - № 2. - С. 3-29.
5. Герасименко В.А. Проблемы защиты данных в системах их обработки // Зарубежная радиоэлектроника. - 1989. - №12. - С. 5-21.
6. Оружие будущего: Тайны новейших военных разработок / Авт.- сост. В.Н. Соколов. – Мн.: Литература, 1998. – 512 с. – (Энциклопедия тайн и сенсаций).
7. Доктрина информационной безопасности России. Утверждена Указом Президента РФ от 9 сентября 2000 г.
8. Ефремов А. Сетевые атаки и средства борьбы с ними // Computer Weekly. – 1998. - № 14. - С. 14-17.
9. Ефремов В.В, Караяни А.Г., Размазнин А.Н., Целыковский В.А. Информационно-психологическое противоборство: сущность, содержание, методы. - М.: 2000 г. – 225 с.
10. О безопасности, ФЗ № 2446-1 от 5.3.1992.
11. О государственной тайне, ФЗ №5485-1 от 21.7.1993.
12. Защита государственных и промышленных секретов. Методы обнаружения вторжений в вычислительные системы. // Ин. печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средств разведывательных служб капиталистических государств. / ВИНИТИ. - 1993. - №7. - С. 8-15.
13. Защита информации в компьютерных системах. Выпуск 2. Элементы криптологии / Под ред. П.Д.Зегжды. - СПб.: ГТУ, 1993. - 147 с.
14. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф Шаньгин. – М:АНКАД, 1999 г. – 340 с.

15. Защита информации в компьютерных системах / В. В. Мельников. – М, 1997. – 150 с.

16. Завадский И.И. Информационная война - что это такое? // Защита информации. Конфидент. - 1996. - №4. - С.13-20.

17. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб.: Издательство СпбГУ, 1999. – 368с.

18. Костин Н.А. Теория информационной борьбы: Монография. – М: ВАГШ, 1996. – С.230.

19. Крис Касперски «Вирусы: вчера, сегодня, завтра» // BYTE Россия. – 1999. - № 6(10). - С. 52-55.

20. Колин К.К. Эволюция информатики и проблемы формирования нового комплекса наук об информации // Научно-техническая информация. ВИНИТИ, Серия 1. – 1995. - № 5. – С.1-7.

21. Компьютерная преступность и информационная безопасность / Под общ. ред. А.П. Леонова. – Мн.: АРИЛ, 2000. – 552 с. – (Библиотека журнала «Управление защитой информации»)

22. Кучер В.А., Бардаев Э.А. Безопасность информационных технологий. - 1997, №1.

23. Месси Дж. Л. Современные методы защиты информации. - М: Советское радио, 1980.- 264 с.

24. Минский М.Л., Пейперт С. Персептроны. - М: Мир, 1971.- 250 с.

25. Морозов Ю.В., Глушков В.В., Шаравин А.А. Балканы сегодня и завтра: военно-политические аспекты миротворчества. – М., 2001. – 376 с.

26. Палий А.И. Радиоэлектронная борьба. - 2-е изд. переработанное и дополненное - М.: Воениздат, 1989. - 384 с.

27. Петряев А.Б. Общая концепция управления защитой информации.// Вопросы защиты информации. – 1997, № 3-4.

28. Проблемы безопасности программного обеспечения / Под ред. П.Д. Зегжды.- СПб.: ГТУ, 1995. - 200 с.

29. Прокофьев В.Ф. Тайное оружие информационной войны. Воздействие на подсознание. – М: СИНТЕГ, 2003. – 430 с.

30. Расторгуев С.П. Информационная война. - М: Радио и связь, 1999. - 416 с.

31. Российский энциклопедический словарь / Гл. ред. А.М. Прохоров. 2-е изд. - М: Сов. энциклопедия, 1999. - 1400 с.

32. Теоретические основы информатики и информационная безопасность: Под ред. В.А. Минаева, В.Н. Саблина. – М.: Радио и связь, 2000. – 468с.

33. Толковый словарь по информатике. – М: Финансы и статистика, 1991. – 200 с.

34. Федеральный закон “Об информации, информатизации и защите информации”. № 24-ФЗ от 20.02.95 г.

35. Филимонов А.Ф. О разработке в США системы мер по защите национальной информационной инфраструктуры // Информационное общество. - 1997. - №1. - С. 60-64.

36. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. - М: “Диалог-МИФИ”, 1996. – 256 с.

37. Хофман Л.Дж. Современные методы защиты информации. М.: Советское радио, 1980.- 264 с.

38. Цыгичко В.Н., Черешкин Д.С., Смолян Г.Л. Новости информационной борьбы // Конфидент, - 1996.- № 6.- С. 19-21.

39. Морозов Ю.В., Глушков В.В., Шаравин А.А. «Балканы сегодня и завтра: военно-политические аспекты миротворчества». – М.. 2001, 376 с.

40. В. Хозиков Информационное оружие. – СПб: Издательский дом «Нева», М: Издательство «ОЛМА-ПРЕСС», 2003. – 480 с. (Серия «Досье»).