

# Концепция защиты от воздействия информационного оружия



Армянский научно-исследовательский институт  
научно-технической информации и технико-  
экономических исследований  
(АрмНИИНТИ)  
Республиканская научно-техническая библиотека  
(РНТБ)

Ереван 1998

**Автор:** Н. В. Джаганян  
**Научный руководитель:**  
к.т.н. Р. В. Арутюнян

**УДК** 355.40:001.9

**ББК** 69:73

355  
Д 40

*В обзоре рассматривается концепция информационной войны, виды информационного оружия и комплекс мероприятий по защите от воздействия информационного оружия, осуществляемых в США, России и Китае.*

<b>ИНФОРМАЦИОННЫЕ ИЗДАНИЯ АРМНИИНТИ, РНТБ</b>	
<b>N</b>	<b>Наименование издания</b>
1.	Инвестируйте в экономику Армении. Справочник (англ.)
2.	Объективные факторы для инвестирования в экономику РА. Справочник (русск., англ.)
3.	Информация о предприятиях, приватизированных в виде акционерных обществ открытого типа. 1995, 1996, 1997 гг. (арм., русск., англ.)
4.	Арутюсова Э. Д., Арутюнян Р. В. Бытовые фильтры для доочистки питьевой воды. Аналитический обзор
5.	Геворкян Р. Г. Прогнозная оценка офиолитовой ассоциации на алмаз. Аналитический обзор
6.	Арутюнян Р. В., Саркисян А. П. Основные тенденции в развитии мирового энергетического хозяйства. Аналитический обзор
7.	Лалаян Ж. Е. Утилизация, переработка и хранение радиоактивных отходов. Обзор
8.	Арутюсова Э. Д., Арутюнян Р. В. Пастеризация молока в условиях мелкого хозяйственника-фермера. Информационный обзор
9.	Хачатрян Н. Л., Арутюнян Р. В. XX век в зеркале geopolитики. Аналитический обзор
10.	Мелоян В., Арутюнян Р. В. Раскрывая завесу над колокольным звоном. Обзор
11.	Арутюнян Р. В. Российские производства черных и цветных металлов. Информационный обзор
12.	Арутюнян Р. В. Индустрия гражданской авиации. Обзор
13.	Рак можно победить, но нужно обязательно верить в победу
14.	Հայ գինվորի գրադարան. Մատենաշար, թողարկումներ թիվ 1-12 Թիվ 1 - Հոգեբանությունը և գինվորը Թիվ 2 - Տարածաշրջանի հարևանների մոտ Թիվ 3 - Գիտության և տեխնիկայի նորույթներ. Լրատվական զենքը XXI դարի գենքն է: Միջուկային վառելիքի վերամշակումը Ֆրանսիական եղանակով Թիվ 4 - Մարտական ուղղաթիռներ Թիվ 5 - Աշխարհաքաղաքական ռազմավարություն Թիվ 6 - Ռուսաստանի ռազմաարդյունաբերական համալիրը Թիվ 7 - Իրական է, արդյոք, ՉՖՕ-ների ֆենոմենը Թիվ 8 - Արդյունաբերության պաշտպանական ձյուղերը Թիվ 1(9) - Հրե գմբեր: «Շիլկա» Թիվ 2(10) - Ռուսաստանի ինքնազնաց հրետանային կայանքները Թիվ 3(11) - Դինամիկ պաշտպանությամբ սարքավորված տանկերի դեմ պայքարի եղանակները Թիվ 4(12) - Ես հավատում եմ մեր հայրենիքի նոր քոհչքին: Պատերազմը և արդի միջազգային հակամարտությունը
15.	Иванова Е. А., Арутюнян Р. В. Технология и оборудование первичной обработки шерсти. Информационный обзор
16.	Бутейко В. К., Бутейко М. М. Дыхание по Бутейко. Методическое пособие для обучающихся методу волевой ликвидации глубокого дыхания

ISBN 99930-3-001-6

© Лрату

## **ВВЕДЕНИЕ**

Информационная война - действия, предпринимаемые для достижения информационного превосходства в интересах национальной военной стратегии и осуществляемые путем влияния на информацию и информационные системы противника при одновременной защите собственной информации и своих информационных систем.

Информационное пространство четких государственных границ не имеет и может быть нарушено в любой момент.

Вероятно, что в XXI веке главные угрозы государствам будут формироваться в информационной сфере. Информация на всех этапах исторического развития являлась объектом борьбы.

Информационная борьба велась практически во всех войнах. Заметные количественные и качественные изменения информационная борьба стала пре-терпевать по мере создания единого мирового информационного пространства. А современная научно-техническая революция произвела подлинный переворот в информационной борьбе.

Не случайно в военно-политическом противоборстве государств сейчас заметна тенденция смещения центра тяжести с традиционных силовых методов и средств борьбы к нетрадиционным, в том числе информационным. Их воздействие незаметно, проявляется постепенно, экономически менее обременительно, экологически безопасно. Но самое главное-трудноустранимо. На открытое применение военной силы все чаще идут в том случае, когда уже исчерпаны все другие имеющиеся возможности воздействия или военные действия наверняка будут скоротечными и беспроигрышными.

Информация и информационные технологии сегодня становятся реальным оружием. События последних лет за рубежом и в нашей стране показывают, что особая роль в информационном воздействии на общественное сознание принадлежит телевидению, т.к. мы живем в условиях, когда получение информации из других официальных источников затруднено. Во все времена в кризисных ситуациях из-за нарушения работы официальных источников информации основным источником удовлетворения информационных потребностей общества становились слухи. В современном информационном пространстве они, овладевая массовым сознанием, способны стать своеобразной "пятой властью". Информация теперь считается стратегическим национальным ресурсом, одним из основных богатств страны.

## ИНФОРМАЦИОННАЯ ВОЙНА

За последнее время в прессе все чаще и чаще стали встречаться такие сравнительно новые термины, как "информационное оружие" и "информационная война", которые, в сущности, означают кардинальные изменения, можно сказать революцию, в военном искусстве. За этими терминами скрываются принципиально новые формы противоборства, борьбы вообще, в которой победа, "подавление противника" будут достигаться не с помощью классического (или даже ядерного) оружия и традиционных способов ведения войны, а путем широкомасштабного, массированного использования радиоэлектронных средств-информационного оружия, которые в США, Германии, Франции, Японии, Великобритании и других странах, располагающих новейшей технологией в области "искусственного интеллекта", считаются "решающим фактором владения современным миром".

Итак, что же такое "информационная война" и "информационное оружие", которое сейчас стало модно называть "троянским конем" XXI века? Для начала напомним некоторые факты и события из недавнего прошлого. Эти экскурсы представляются необходимыми для того, чтобы вскрыть истоки появления упомянутых терминов и понять их суть.

Из недавнего прошлого (1970-1990гг):

1. Американская ракета отклонилась от заданного курса только потому, что в программе ее ЭВМ вместо семерки оказалась единица. Ракета была взорвана по команде с наземного пункта управления.

2. Советский космический аппарат "Фобос", почти долетевший до района Марса, не выполнил свою последующую задачу: в посланном ему сигнале была пропущена всего одна буква, в результате чего произошло отклонение системы ориентации.

3. Американский космический корабль, направленный на Венеру, прекратил свой полет только потому, что в модуле системы управления оператор вместо запятой поставил точку.

4. В сентябре 1988г. многие компьютерные центры на восточном и западном побережье США в течение нескольких часов были "заражены" так называемой "вирусной инфекцией". "Эпидемия" охватила более шести тысяч компьютеров и 70 компьютерных систем. "Вирусы" стали быстро размножаться, забивая каналы информации. Более того, "вирусная программа" позволяла узнавать секретные пароли и таким образом подключаться к компьютерным системам, обеспечивающим управление военными объектами. Злоумышленником оказался 23-летний студент Калифорнийского университета, который ради развлечения ввел составленную им "вирусную программу" в компьютерную систему университета.

Эта "атака на ЭВМ" вызвала большой переполох среди научно-технического персонала, занятого обеспечением безопасности ЭВМ, особенно ядерных ракет США.

5. В системах ПВО, закупленных Ираком в одной из западноевропейских

стран, были заложены так называемые "логические бомбы", в результате чего во время войны в зоне Персидского залива эти системы не могли быть задействованы, и, таким образом, прикрываемые ими объекты оказались беззащитными.

Что общего в изложенных выше пяти фактах? Ответ напрашивается сразу: искаженная информация, причем искажение было привнесено либо случайно, либо преднамеренно. Случайные искажения могут иметь место в результате ошибок оператора, программиста (человеку свойственно ошибаться), неисправностей, стихийных бедствий...

Но если искажение преднамеренное, то это как раз то, что в принципе можно назвать информационным оружием. Это оружие технического, радиоэлектронного класса, которое, по определению американских экспертов, представляет собой комплекс программно-информационных средств, созданных для поражения информационных ресурсов противника. Это уточняющее определение представляется необходимым, поскольку в мире существует, так сказать, "обычное" информационное оружие пропагандистско-психологического воздействия, которое общеизвестно под названием "дезинформация", имеющей свою давнюю, можно сказать древнюю историю. Конечная цель дезинформации заключается в том, чтобы заставить противника поверить той информации, которой его умело снабжают извне с тем, чтобы он проводил свою политику или вел войну, будучи сначала "слепым", а затем оказался парализованным. В военно-исторической литературе и публицистике описаны многие известные примеры успешно осуществленной дезинформации во время войны и в мирное время. Дезинформация и сейчас продолжает сохраняться в арсеналах спецслужб. Но вот где-то на рубеже 1960-1970-х годов в обычное информационное оружие вторгается "искусственный интеллект", происходит компьютерное и микрокомпьютерное оснащение информационных систем, в результате чего информационное оружие обретает качественно новые свойства, позволяющие не только безгранично расширить сферы его применения, но даже заменить собой сегодняшние средства массового поражения. Наиболее точное и конкретное определение информационного оружия сделано российскими экспертами.

Информационное оружие - это "средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всего высокотехнологичного обеспечения жизни общества и функционирования государства".

В настоящее время в США созданы и приняты на вооружение различные системы информационного оружия (Information weapon, далее для краткости - ИНФОР), обладающего перечисленными возможностями. Эти системы ИНФОР по предназначению и сферам воздействия можно условно подразделить на три вида.

1. ИНФОР, нарушающее и парализующее информационные системы и

сети, обеспечивающие функционирование органов управления государственных и военных объектов, промышленности, транспорта, связи, энергетики, банков и других учреждений. К этому классу ИНФОР относятся компьютерные вирусы, логические бомбы и другие средства.

Компьютерный вирус (КВ)-специальная программа, внедряемая в "чужую электронную среду". КВ способен передаваться по линиям связи и сетям обмена информацией, проникать в электронные телефонные станции и системы управления. В заданное время или по сигналам КВ стирает хранящуюся в памяти ЭВМ информацию либо заменяет ее произвольно или целенаправленно. Например, КВ, внедренный в банковский компьютер, может изменить в пользу автора денежный счет или перевести деньги с одного счета на другой. Такой КВ способен также заполнить другими данными всю память компьютера-жертвы и в конечном счете блокировать его.

Логическая бомба (ЛБ), так называется программная закладка, заблаговременно внедряемая в информационные системы и сети, обеспечивающие управление объектами военной и гражданской инфраструктуры. ЛБ по сигналу или в установленное время приводится в действие, стирая или искажая информацию в поражаемом компьютере, и в итоге выводит его из строя.

"Троянский конь" (разновидность ЛБ) - программа, позволяющая осуществлять скрытый, несанкционированный доступ к информационным ресурсам противника для добывания разведывательных данных.

Существуют средства, позволяющие внедрять и КВ, и ЛБ в государственные (гражданские и военные) информационные системы и сети и управлять ими на расстоянии. Для этих средств наиболее уязвимы автоматизированные системы обнаружения и управления, постоянно действующие в установленных режимах реального времени. По оценкам западных специалистов, вероятность восстановления нарушенных функций таких систем, в частности СПРН (система предупреждения о ракетном нападении), систем управления ПРО довольно низкая, поэтому целенаправленное вторжение в их работу может иметь особо тяжелые последствия, сопоставимые с последствиями применения оружия массового поражения.

2. ИНФОР, оказывающее психологическое воздействие, влияние на психику людей, позволяющее управлять их поведением. Как сообщалось в печати, после окончания войны в зоне Персидского залива в научно-исследовательских учреждениях Пентагона разработаны средства, позволяющие, в частности, создавать на небе голографические изображения исламских мучеников, которые "с небес будут призывать своих единоверцев прекращать сопротивление".

В феврале 1993г. во время песчаной бури в районе Могадиши (Сомали) солдаты морской пехоты США заметили на небольшой высоте изображение человеческого лица размером около 150 метров, которое было "не просто знакомым лицом, а являлось изображением Иисуса Христа, каким оно обычно дается в религиозных изданиях, на картинах и скульптурах во всем мире".

Изображение сохранялось в течение пяти минут, но этого было достаточ-

но, чтобы вызвать сильное потрясение среди американских солдат, даже самых неверующих. Западные эксперты полагают, что это было "голографическим рисунком", созданным подразделением психологических операций американских войск, действовавших в Сомали. Имеются также сообщения о так называемом "вирусе N 666", который обладает способностью губительно воздействовать на "психофизиологическое состояние" оператора ЭВМ. Этот "вирус-убийца" выдает на экран особую цветовую комбинацию, погружающую человека в своеобразный гипнотический транс и вызывающую у него такое подсознательное восприятие, которое резко изменяет функционирование сердечно-сосудистой системы вплоть до блокирования сосудов головного мозга.

3. Радиоэлектронное подавление (РЭП). Это особый вид радиоэлектронной борьбы, призванный нарушать или затруднять функционирование электронных средств противника путем излучения, отражения электромагнитных, акустических и инфракрасных сигналов. РЭП осуществляется автоматически наземными, корабельными и авиационными системами постановки помех. Впервые широкомасштабное применение РЭП было продемонстрировано Соединенными Штатами в 1991г. во время войны в зоне Персидского залива, в итоге которой американцы довольно быстро достигли своих стратегических целей: контроль за нефтяными ресурсами на Ближнем Востоке и установление постоянного военного присутствия в этом регионе. По общему мнению экспертов, успех этой войны (известной как операция "Буря в пустыне"), был обеспечен массированным применением современных средств радиоэлектронной борьбы и высокоточного оружия, основным элементом которого, обеспечивающим его высокую эффективность, также являются электронные информационные системы. За несколько суток до начала операции в результате мощного РЭП на территории Ирака были выведены из строя системы государственного и военного управления, системы ПВО и связи. Это был такой мощный радиоэлектронный удар по Ираку, штурм в эфире, что глушились даже отдельные радионаправления в южных округах СССР. В целом, оценивая роль компьютерной оснащенности ВС США, задействованных в данной операции, американские специалисты образно отмечали, что война в зоне Персидского залива была первой, где унция кремния в компьютере оказалась эффективней тонны урана в боеголовках.

Итак, имеющиеся факты и события показывают, что радиоэлектронное информационное оружие-реальность нашего времени. Но если это оружие появилось и совершенствуется, то, естественно, возникает понятие, а следовательно, и угроза информационной войны (1).

Кратко суть информационной войны можно сформулировать таким образом: это использование новейших технологических достижений XX века для быстрой, скрытой, широкомасштабной атаки на военную и гражданскую инфраструктуру противника с применением информационных технологий и одновременно - защита своих собственных информационных сетей. Рождение идеи информационной войны было предопределено глубокими военно-политическими,

экономическими и историческими причинами. Выделим главные из них.

Вся международная и внутренняя политика США базируется на идеи лидерства Америки на планете, в том числе лидерства военно-экономического. Идея ИВ (информационная война) направлена прежде всего против тоталитарных режимов, потенциальных обладателей ядерного и другого оружия массового поражения. Практическое воплощение этой составной части ИВ-операции "Буря в пустыне".

Высокотехнологическое оружие XXI века, каковым по праву можно считать оружие информационное, дает мощные импульсы электронной промышленности США, переживающей сегодня сложные времена: ее теснят на мировых рынках производители информационных технологий Японии, Юго-Западной Азии и Западной Европы.

Государственной идеологии и общественному настроению американцев присуще стремление выигрывать войны за счет технического превосходства, сохрания при этом жизни своих солдат. Таким образом, налогоплательщики с пониманием отнесутся к расходам на "кнопочную войну".

ЦРУ работает над секретной программой по установке закладок в виде интегральных схем в системы оружия противника, которые могут быть проданы потенциальному противнику. Другая секретная программа ЦРУ связана с вербовкой зарубежных программистов в компьютерные системы противника.

Национальная ядерная лаборатория в Лос-Аламосе разработала портативное устройство, генерирующее мощный электромагнитный импульс для выведения из строя электронных систем банков в столице противника. Устройство достаточно компактно-для его размещения достаточно стандартного кейса.

В министерстве обороны США горячо обсуждается вариант использования в информационной войне элементов биологического оружия; речь идет о микробах, в чей рацион питания входит электроника. Сбор разведывательной информации можно будет вести с применением распыления аэрозолей над вражеской территорией. Эти химикаты, попав в пищу, могут отслеживаться биодатчиками и давать информацию о перемещении сил противника.

Надо сказать, что американцы достаточно самокритичны к себе в вопросе собственной уязвимости в ИВ. Два года назад головное ведомство, ответственное за организацию обороны в США против информационной войны, провело военную игру, в которой приняли участие Белый дом и минобороны США. Вывод по итогам компьютерных маневров был однозначен: США, равно, впрочем, как и другие страны, очень слабо подготовлены к информационным войнам. Более того: святая святых-ситуационная комната Белого дома - в любой момент может подвергнуться информационному воздействию извне через сети Интернет. Так что американские власти всерьез озабочены своим нынешним состоянием информационной безопасности (2).

Таким образом, Соединенные Штаты, создав принципиально новые средства ведения войны, поставили мир перед новой опасностью, которая называется информационной войной. Впервые термин "информационная

"война" (Information war) начал употребляться в американских военных кругах в 1991г. после окончания операции "Буря в пустыне". Первым официальным документом по этой проблеме является директива министра обороны США от 21 декабря 1992г. под названием "Информационная война" (далее для краткости - ИНФОРМВ), в которой, в частности, указывалось на "необходимость учета информационных ресурсов при организации планирования и функционирования систем управления ВС в условиях противодействия противника". Позднее, в 1993 году, в директиве Комитета начальников штабов N30 уже были изложены основные принципы ведения информационной войны. И наконец, в проекте будущего устава армии США дано следующее определение информационной войны: "Действия, предпринятые для достижения информационного превосходства в интересах национальной стратегии и осуществляемые путем влияния на информацию и информационные системы противника при одновременной защите собственной информации и своих информационных систем".

### **Подготовка к информационной войне в США**

В настоящее время в США осуществляется обширный комплекс мероприятий по подготовке к информационной войне. Эта подготовка ведется по трем направлениям: в вооруженных силах, в спецслужбах и в национальном масштабе. В вооруженных силах подготовка включает теоретические, организационные и материально-технические мероприятия. Так, в американских уставах изложены способы применения ИНФОР и принципы ведения информационной войны. В армии, на флоте и в ВВС введены должности офицеров, занимающихся проблемами информационной войны. В 1995г. в Национальном университете обороны состоялся первый выпуск специалистов по информационной войне. В конце 1995г. в Пентагоне обобщены результаты более десятка секретных штабных игр по ведению ИНФОРМВ, проводившихся в течение 1994-1995 годов. И наконец, пожалуй, самое главное - ВС США интенсивно оснащаются ИНФОР. Еще в 1994г. финансирование ВС на приобретение информтехнологий получило приоритетный характер, опередив даже ракетно-ядерные и космические программы.

В спецслужбах ведется особая и интенсивная подготовка к ИНФОРМВ. Агентство национальной безопасности разрабатывает способы внезапного "заражения" компьютеров и компьютерных систем, а также различные схемы "закладок" для компьютерных вирусов и логических бомб. В ЦРУ подготовка ведется по двум программам:

1) "Чипинг (Chipping), предусматривающая способы внедрения легко инициируемых в нужное время логических бомб и компьютерных вирусов в информационные системы ВПК противника;

2) Программа по разработке способов воздействия на программистов, работающих на предприятиях ВПК, чтобы в кризисных ситуациях привлечь их для внедрения вирусов и логических бомб в информационные системы этих

предприятий. Подготовка к ИНФОРМВ в национальном масштабе США заключается, как указывается в иностранной печати, в "совершенствовании национальной информационной инфраструктуры", включающей все электронные СМИ, банковские системы, системы связи, транспорта, энергетики, весь спектр электроники в промышленности и сфере услуг. И наконец, эта структура фактически дополняется непрерывно разрастающейся сетью "Интернет", клиентура которой исчисляется миллионами пользователей, разбросанных по всему миру. Таким образом, кибернетическое пространство, в котором может разразиться будущая информационная война, уже не будет ограничиваться государственными границами.

В связи с этим представляется целесообразным несколько подробнее остановиться на характеристике сети "Internet", играющей далеко не последнюю роль в национальной информационной инфраструктуре США. Сеть "Internet" зародилась в 1973г., когда в рамках Управления перспективных исследований и проектах МО США была создана сеть ARPAnet, устойчивая к частичным повреждениям, возможным при бомбардировках или даже ядерных ударах. Эта сеть в течение десятка лет функционировала в закрытом режиме среди специалистов по вычислительной и военной технике. В этот же период создавались сети в рамках НАСА (Национальное управление по аeronавтике и космическому пространству), НОРД (Система ПВО Североамериканского континента) и других военных структур. Все эти сети по принципам построения и методике функционирования основывались на "Интернет протоколе" (ИП), представляющем собой свод правил и принципов работы сетей, согласно которому действовала ARPAnet. Поэтому вскоре ИП сделался единственным способом для связи разнородных компьютеров, которые постепенно объединялись в "сеть сетей". Именно в то время получило широкое распространение название "Интернет", что в переводе означает "межсеть", которую стало уже невозможно и нецелесообразно сохранять в рамках Пентагона. Так "Интернет" сделалась общедоступной, в частности для учебных заведений США (в настоящее время в США около полумиллиона человек, в основном студентов и старших школьников, обучаются с помощью сети "Интернет" в так называемых "виртуальных классах", то есть у дисплея персональных компьютеров). Каковы возможности "Интернет?" Как подчеркивают западные эксперты, в "Интернет" в принципе возможно все: посыпать в любой регион страны электронную почту, использовать любой удаленный на тысячи километров компьютер как свой собственный, покупать и продавать товары, получать необходимую информацию, читать "электронные публикации", участвовать в различных дискуссиях по самой разнообразной тематике, вплоть до военно-стратегических проблем и вооружений, получать тексты документов и видео-изображения и т.п. Все эти "путешествия по информационному пространству" осуществляются с помощью "всемирной паутины"-самой популярной сейчас глобальной гипертекстовой информационной системы, иначе говоря, "программного инструмента", который вполне можно назвать глобальной планетарной энциклопедией. Процессы подключения к

сети "Интернет" и получения информации сравнительно просты. Каждый пользователь сети может в считанные секунды подключиться с помощью своего модема к любому электронному адресату ("серверу"), например к резиденции президента США, к библиотеке американского Конгресса и другим адресатам, находящимся в любой стране, имеющей информационную структуру.

Особо следует отметить два важных и опасных свойства сети "Интернет": живучесть и возможность произвольного подключения к сетям управления военными объектами стратегического значения. О живучести "Интернет": во время войны в зоне Персидского залива Соединенным Штатам, несмотря на мощное радиоэлектронное подавление, так и не удалось полностью изолировать Ирак от внешнего мира. Правительство Ирака по сети "Интернет" закупало оружие, перечисляя фирмам-поставщикам деньги, хранящиеся в иностранных банках. Так что американцы создали, на свою голову, устойчивую к "частичным повреждениям" информационную сеть. Об опасности произвольных подключений через "Интернет" к сетям стратегических объектов свидетельствуют следующие из многочисленных фактов, отмечавшихся в американской прессе. В 1994 году была своевременно обнаружена попытка датских школьников подключиться через "Интернет" к американской метеорологической информационной системе. Это подключение могло иметь катастрофические последствия для сотен самолетов, находящихся в воздухе. В результате несанкционированного подключения к компьютерной сети фирмы "Дженерал электрик" последняя была парализована в течение трех суток. Количество произвольных подключений к компьютерам НАСА составляет более 1000 в месяц. В министерстве обороны США уже создана специальная группа для регистрации "компьютерных ЧП" в федеральных и военных информационных системах. Группа ежедневно регистрирует десятки таких ЧП.

В общей оценке постоянно разрастающейся американской информационной инфраструктуры обращает на себя внимание вполне определенное противоречие. С одной стороны, администрация США за счет широкого использования новейших информационных технологий предполагает сэкономить в год около 15 млрд. долларов на содержание государственного аппарата. С другой стороны, распространенность электронной автоматизации федеральных служб и ведомств создает условия для "компьютерного шпионажа" и информационных диверсий с помощью простых компьютерных вирусов, количество которых сейчас исчисляется в тысячах.

Причем все эти шпионские акции могут осуществляться как внутри страны, так и извне. По оценкам американских экспертов, в настоящее время в мире насчитывается 50 государств, которые в определенной мере считают США объектом компьютерного шпионажа. По другим данным, в 25 странах уже созданы и действуют подпольные группы так называемых "хакеров"-потенциальных информационных террористических групп, или, как их еще называют, "электронных взломщиков". Здесь будет уместно привести весьма многозначительный вывод, сделанный в 1994г. в отчете Объединенной комиссии США по вопросам

национальной безопасности" "Комиссия признает безопасность информационных систем и сетей в качестве важнейшей угрозы безопасности в этом десятилетии и вероятнее всего в следующем столетии, полагать недостаточно осознанной степень риска, которому мы подвергаемся в этой области". В отчете даются рекомендации по созданию и развитию специальных средств обнаружения "незаконных закладок" в информационных системах, а также по разработке соответствующих методов нейтрализации акций вторжения в эти системы. И все же США настойчиво продолжают развивать и совершенствовать национальную инфраструктуру, подчиняя ее новой военной политике, основой которой, судя по всему, является информационная война. Более того, в администрации США, Пентагоне и спецслужбах идея информационной войны приобретает приоритетное значение. Каковы же причины такой упорной "информационной политики" Соединенных Штатов? Где истоки возникновения и живучести идеи информационной войны? Судя по различным оценкам, фигурирующим в иностранной прессе, таких причин несколько.

Во-первых, следует отметить, что основой всех концепций внутренней политики США является идея американского лидерства в мире.

Информационное оружие, созданное в США в результате крупного технологического прорыва, вполне способствует материализации этой идеи в обозримом будущем.

Во-вторых, идея информационной войны имеет прямую направленность против государств, где господствуют тоталитарные режимы (Ирак, Ливия, Иран, Северная Корея) и где наиболее вероятно появление ядерного оружия и других видов ОМУ. Подтверждением такой направленности информационной войны отчасти может служить операция "Буря в пустыне", в которой впервые было использовано информационное оружие.

В-третьих, экономичность информационного оружия позволяет, с одной стороны, в определенной мере сокращать военный бюджет, а с другой - создавать высокоэффективное оружие XXI века, применение которого сулит многообещающие результаты. Кроме того, первостепенное развитие получает электронная промышленность США, которая сейчас с трудом выдерживает конкуренцию с электронными технологиями Японии и Западной Европы.

В-четвертых, массированное применение информационного оружия, как утверждают западные эксперты, дает возможность сравнительно быстро подавлять противника, парализовать его, вынуждать к капитуляции без задействования ВС, без обычных сражений, типичных для классических войн, без гибели людей и разрушений гражданской инфраструктуры и, наконец, без потерь личного состава американских ВС, которые весьма болезненно воспринимаются американским обществом (1).

В 1996г. в США проходила 5-я Международная конференция по информационным войнам, в которой приняли участие и представители ряда других государств. На этой конференции подчеркивалось, что появление нового компонента военного потенциала-информационного оружия способно не

только повысить эффективность традиционных средств ведения вооруженной борьбы и содействовать достижению успеха в "горячих войнах", но и заменить их в большинстве ситуаций политической нестабильности.

"...Сети передачи данных превращаются в поле битвы будущего,-говорится в докладе Объединенной комиссии по безопасности при Центральном расследовательном управлении США,-информационное оружие, стратегию и тактику применения которого предстоит еще тщательно разработать, будет использоваться с "электронными скоростями" при обороне и нападении. Информационные технологии позволяют обеспечить разрешение геополитических кризисов, не производя ни одного выстрела. Наша политика обеспечения национальной безопасности и процедуры ее реализации должны быть направлены на защиту наших возможностей по ведению информационных войн и на создание всех необходимых условий для воспрещения всем противостоящим США государствам вести такие войны..."

Информационное оружие - это прежде всего "атакующее оружие", способное уничтожать и искажать информацию, а также заниматься хищением информационных массивов и, преодолевая системы защиты, добывать из них конфиденциальную информацию, а также разрушать телекоммуникационные сети и компьютерные системы.

Информационное оружие способно также влиять на все средства массовой информации того или иного государства, изменять ее политическую ориентацию и создавать у населения превратные представления о политической и социально-экономической жизни, провоцируя возникновение серьезных социальных конфликтов.

Необходимо также учитывать то обстоятельство, что при ведении информационной войны, так же как и при возникновении ядерной войны, значительные выгоды получает та сторона, которая применит информационное оружие первой. Таким образом, чрезвычайно важное значение приобретают способы защиты от информационного оружия и информационной агрессии и методы противодействия информационному оружию, способы его нейтрализации (3).

### **Пентагон на страже информационного пространства Америки**

Сегодня, когда границы в едином информационном пространстве фактически утратили свое значение благодаря всемирной компьютерной сети Интернет, многие руководители государств начинают проявлять серьезную обеспокоенность по поводу безопасности своих национальных информационных систем. По мнению американских экспертов, проблема компьютерной защиты в начале нового столетия по степени потенциальной угрозы национальной безопасности будет стоять на втором месте после распространения оружия массового поражения. На разработку эффективных технологий в области компьютерной защиты в США ежегодно выделяется свыше 100 млн. долл. в федеральном бюджете.

Весьма характерным в этом плане является решение об ужесточении контроля за доступом в Интернет в российских федеральных структурах и ведомствах. Предшествовавшая ему серия публикаций об "ужасных" последствиях услуг Интернета в России только накалила страсти. Некоторые авторы до того увлеклись, что представили бесплатный доступ в Интернет, организованный Фондом Сороса в крупнейших российских библиотеках как диверсию американских спецслужб.

Безусловно, защита информационных ресурсов становится одной из приоритетных государственных задач. Однако, попытки ее решения могут принести больше вреда, чем пользы.

Для того, чтобы лучше разобраться в этом, обратимся к опыту США, где в настоящее время сосредоточено свыше 60% всех пользователей Интернета, включая федеральные ведомства.

Следует вспомнить, что своим появлением сеть Интернет обязана работам, проводимым Пентагоном на рубеже 60-70 годов по использованию пакетной коммутации сообщений для создания высокоживучей национальной компьютерной сети военного назначения.

В дальнейшем на ее основе были разработаны и усовершенствованы многие из известных в настоящее время телекоммуникационных стандартов (протоколы, интерфейсы, форматы передачи данных).

Примечательно, что пик гонки ядерных вооружений в разгар холодной войны совпал с активизацией использования сетей с пакетной коммутацией в военных целях для обеспечения национальной безопасности.

Но если в США эти работы в конечном итоге из военной области очень скоро перекочевали в гражданский сектор экономики, создав колоссальный задел для прибыльных инвестиций в индустрию телекоммуникаций, то в России они продолжали оставаться в ранге чисто оборонных программ до начала 90-х годов.

После окончания холодной войны Пентагон сделал ставку на использование так называемых технологий двойного назначения (военного и гражданского). Опыт широкого использования коммерческих информационных и телекоммуникационных технологий в боевых действиях в Персидском заливе подтолкнул Пентагон всерьез заняться вопросами информационной безопасности, рассматривая их в качестве важнейшей составляющей концепции ведения информационной войны. Поражение вооруженных сил Ирака, как это неудивительно, породило глубокую обеспокоенность прежде всего в руководящих кругах США, где призрак информационной войны принял весьма угрожающие и вполне реальные очертания.

Отключать свои компьютеры от Интернета американцы не стали. А вот защитой их занялись всерьез.

И, как всегда, законодателем в этом начинании выступил Пентагон, взяв на себя функции координатора программ в области информационной безопасности INFOSEC. Управление информационных систем (УИС) министерства обороны США вместе с агентством национальной безопасности

(АНБ) осуществляет широкомасштабную программу по защите национально-информационной инфраструктуры.

По инициативе УИС были проведены эксперименты по изучению возможности проникновения в боевые информационные системы и закрытые компьютерные сети через Интернет. Результат превзошел все ожидания, когда в ходе учений были заблокированы все лифты для подъема самолетов на палубу одного из авианосцев, находившегося за сотни миль от побережья США. Обобщив результаты других экспериментов, специалисты пришли к весьма неутешительным выводам о том, что 88% проверенных компьютеров доступны для несанкционированного проникновения через сетевые средства защиты, при этом 96% всех вторжений не регистрируются администраторами сетей и пользователями компьютеров.

Управление информационных систем МО США поставило перед собой цель создать к началу третьего тысячелетия надежную многоуровневую систему безопасности, исключающую несанкционированный доступ к информационной инфраструктуре.

Созданный в настоящее время при УИС центр информационной безопасности осуществляет круглосуточный мониторинг за обстановкой в информационном пространстве, периодически отключая незваных гостей от серверов, коммутаторов и каналов Пентагона. В состав центра входят три департамента противодействия, сертификации и обучения.

Рассматривая информационную безопасность как оборонительный аспект ведения информационной войны УИС закладывает организационно-технологический фундамент в концепцию создания единого информационного пространства участников поля боя. Первоочередное внимание уделяется таким ресурсам, как глобальная система управления (GCCS), информационная система ВС (DISN), система передачи сообщений (DMS) и телефонная система объявления тревог.

Одним из направлений является создание технологии так называемых огнеупорных стен, представляющих фактически специализированные серверы, в основу работы которых положена многоуровневая защита, реализованная аппаратно-программным методом в виде операционной системы, управляющей внешним доступом.

Другое направление работы связано с технологией объектно ориентированного моделирования и имитации в распределенной сети. В ее основе лежит принцип распределенной архитектуры локальных вычислительных сетей (ЛВС), создаваемой на основе специализированных серверов: связи, баз данных, гипермедиа, ситуационного планирования, моделирования, картографического, почтового. В настоящее время такая архитектура уже проходит испытание в управлении АРПА, под эгидой и при участии которого разрабатывается данная технология. По оценкам специалистов, внедрение этой технологии позволит вдвое сократить стоимость разработки программного обеспечения для автоматизированных комплексов управления сводными формированиями, в состав которых на период выполнения боевых задач могут входить отдельные

корабли, авиационные эскадрильи и подразделения сухопутных войск.

Серьезной проблемой в обеспечении информационной безопасности остается организация распределенного доступа к базам данных коллективного пользования. До сих пор во всем мире широко использовалась практика физического разделения массивов данных, имеющих различную степень секретности. При этом безопасность работы в таких сетях гарантировалась ограниченным кругом пользователей, подключенных к тем или иным носителям информации. Однако сейчас, когда требование прозрачности ресурсов и оперативности доступа к ним начинает доминировать в развитии сетевых технологий, подобный подход начинает терять свою привлекательность. Для устранения назревших противоречий в федеральных ведомствах США (ФБР, таможенной службе, федеральном суде и др.) осуществляется переход на новую версию реляционной системы управления базами данных (СУБД) "Оракул-7" повышенной криптостойкости.

В новой версии этой СУБД впервые появилась возможность одновременной обработки информации различной степени секретности на одном компьютере.

Не менее важным аспектом информационной безопасности является создание специальных криптографических аппаратно-программных средств, выполняющих как функции защиты операционных систем в ходе их загрузки, так высокоэффективного перепрограммируемого шифрования данных. Внедрение этих устройств в полевые системы АСУ позволит командирам всех степеней эффективно обмениваться любой зашифрованной информацией.

Для защиты от несанкционированного доступа к компьютеру непосредственно на рабочем месте компанией "Интегрейтид технолоджис оф Америка" разработана специальная магнитная карточка-электронный ключ с пятью уровнями безопасности. В случае нарушения правил регистрации пользователя возможно как частичное блокирование и стирание информации в памяти, так и полное физическое разрушение самой карточки. При этом вся информация, хранящаяся в компьютере, кодируется с помощью криптографического алгоритма с аппаратной реализацией на электронной плате, вставляемой в системный блок компьютера. При регистрации в зависимости от уровня доступа и степени секретности информации пользователь должен ответить на вопросы, последовательность и содержание которых устанавливается администратором сети. Для блокирования компьютера достаточно только вынуть карточку-ключ. После этого необходимо повторить всю процедуру заново.

Приведенный выше далеко не полный перечень разрабатываемых аппаратно-программных средств защиты дает наглядный пример гибкости в выборе способов достижения главной цели-безопасности информационных ресурсов на всех этапах и уровнях их использования. Тем самым проблема подключения к Интернету федеральных ведомств в США уже давно решена.

Открытым остается только вопрос об эффективности средств защиты, набор которых расширяется по мере роста количества пользователей Интернета (4).

## Традиции информационного противоборства

Лучший способ победить противника-сорвать его замыслы.

В Китае с древних времен с большим пониманием относились к информационным формам и способам борьбы с противником, справедливо предпочитая их кровопролитным схваткам на поле боя.

В одном из китайских трактатов можно прочитать: "Страна управляетя справедливостью, война ведется хитростью". Обман, военная хитрость-не что иное, как один из способов информационного противоборства, состоящий в регулировании информации о себе с целью введения противника в заблуждение относительно истинного состояния своих войск, их возможностей, планов и намерений командования. Выигрывает тот, кто умеет вести войну, не сражаясь.

В военных действиях атака на умы-главная задача, атака на укрепления - второстепенная задача. Психологическая война - это главное, бой - это второстепенное.

Как видим, оперативная маскировка, дезинформация противника (хотя и в других, не вполне современных терминах) дополняются у древних китайцев понятием психологической войны.

Еще одним проявлением информационного противоборства в древнем Китае было поддержание высокого морально-психологического духа собственных войск. Древнекитайские военные мыслители считали эту работу важной предпосылкой успеха в войне.

При оценке уязвимости своей страны американский эксперт Фредерик Коэн подсчитал, что десять хакеров со 100 тыс. долл. могут в течение нескольких недель нанести серьезный урон вплоть до парализации американской информационной инфраструктуры. Двадцать хакеров с 1 млн. долл. могут поставить США на колени за две недели, а ста хакеров и 30 млн. долл. хватит для разрушения всей информационной структуры Соединенных Штатов, после чего потребуется несколько лет для проведения комплекса восстановительных работ.

Китайская военная наука активно занимается разработкой проблем информационного противоборства. Прежде всего, изучается американский опыт, приобретенный в зоне Персидского залива. Накануне войны в КНР полагали, что американские войска увязнут в затяжной войне, как это произошло с советскими войсками в Афганистане. Однако то, с чем столкнулись китайцы в этой войне, неприятно их поразило. Они увидели в действии современные, насыщенные электроникой вооружения и военную технику, включая высокоточное оружие, системы раннего обнаружения ивойсковой ПРО, глобальные системы разведки и т.д.

Подобные перспективы не могут не беспокоить военно-политическое руководство Китая, которое учитывает уровень военно-технического развития своей страны и ассоциирует себя скорее с Ираком, опасаясь столь же неблагополучного исхода в гипотетическом военном конфликте с противником, имеющим явное технологическое превосходство.

## **КНР и США присматриваются друг к другу**

С особым вниманием следят в Китае за развитием на Западе средств программно-математического воздействия на объекты информационного ресурса других стран. Это не проходит незамеченным в США. В газете "Филадельфия инкуайрер" рассказывается о работе китайского ученого Чжоу Си "Исследование и анализ компьютерной безопасности и защиты от вирусов в военной области".

Автор утверждает, что в США завершена работа над программными продуктами ударного познания, с помощью которых поражаются компьютерные сети и системы управления противника, а также искажается информация, циркулирующая в системах боевого управления.

Разрабатывается новая программа создания боевых компьютерных вирусов, скрытно размещаемых в средствах вычислительной техники и ином электронном оборудовании, поставляемом на экспорт. Подобные закладные устройства могут быть приведены в действие в случае начала военного конфликта, выводя из строя технику, в которой они установлены.

Китайский ученый формулирует некоторые рекомендации по нейтрализации возникающей угрозы. Во-первых, он призывает с большей осторожностью подходить к компьютеризации вооруженных сил. Во-вторых, автор настаивает на принятии специальных мер обеспечения безопасности, используемых аппаратно-технических и программных средств - установке специальных фильтров и предварительной сертификации импортируемого электронного оборудования.

Под прикрытием информационного бюро Госсовета КНР министерство общественной безопасности регулярно организовывало поездки специалистов в Сингапур и Гонконг для изучения наиболее эффективных методов контроля сети Интернет, перехвата электронной почты, обеспечения безопасности компьютерных сетей и циркулирующей в них информации.

США, обладающие наиболее развитым информационным ресурсом, не менее озабоченно следят за тем, что происходит по другую сторону Тихого океана.

В Америке относят Китай к числу наиболее опасных соперников в области информационного противоборства. По данным начальника штаба ВВС США, всего около 100 стран имеют те или иные наступательные оборонительные возможности ведения такого противоборства, в том числе около полусотни стран рассматривают США в качестве возможного объекта атаки средствами специального воздействия. Меры противодействия продумываются уже сейчас на самых различных уровнях. Прямое оперативное предназначение против КНР имеют американские силы и средства информационного противоборства, развернутые на Тихом океане. Главнокомандующий военно-морскими силами в этом районе адмирал Арчи Клеминз зарекомендовал себя как активный сторонник внедрения новых информационных технологий. Одной из его инноваций стала глобальная сетевая инициатива (GNI), реализованная в его объедине-

нии. В рамках этой "инициативы" была создана система боевого управления со средствами видеоконференц-связи и аппаратной передачи документальной информации, которая впервые прошла практическую проверку в ходе китайско-тайваньского кризиса, разразившегося в начале 1996г.

Система GNI, безусловно, обеспечит на Тихом океане некоторое информационное превосходство ВМС США над противостоящим противником. Но удастся ли трансформировать преимущества, приобретенные оперативно-стратегическим объединением на конкретном участке в общее преимущество одной державы над другой? Ведь до боевого применения американских ВМС, в котором они могли бы продемонстрировать чудеса управляемости, дело может просто не дойти.

Массированный программный удар многомиллионной армии китайских пользователей с одновременной активизацией множества заблаговременно внедренных программных и аппаратных закладок может привести к дезорганизации всей системы государственного и военного управления США. Очень важный первоначальный успех в войне будет достигнут без разгрома войск в форме срыва замыслов противника, расстройства его планов (5).

### **Задача информационного пространства России**

Но существует ли вообще эффективная и надежная защита от воздействия этого своеобразного оружия? Совершенно очевидно, что в настоящее время решение этой проблемы становится высокоприоритетной задачей для любых государств современного мира, в том числе и для России. И прежде всего необходимо надежно обеспечить защиту информационного оборудования на территории нашей страны от возможного проникновения "скрытых элементов" информационного оружия.

Таким образом, главной отличительной чертой атакующего информационного оружия является универсальность и радикальный характер воздействия, скрытность, возможность широкого выбора места и времени его применения, а также очевидная экономичность в сравнении с использованием других современных вооружений.

Необходимо также учитывать, что организация единого международного информационного пространства требует высокой степени унификации информационных и телекоммуникационных технологий (3).

В чем же заключается потенциальная опасность информационной войны для России? В оценке этой опасности можно было бы принять за основу следующие соображения.

1. Прежде всего, необходимо четко представлять себе, откуда может исходить опасность информационной войны. Хотя согласно основным положениям военной доктрины РФ ни одно государство не рассматривается Россией в качестве вероятного противника, тем не менее отнюдь нельзя не учитывать по-

литику и стратегию государств, располагающих весьма развитой информационной инфраструктурой. При этом следует иметь в виду "информационную политику" США, главная цель которой заключается в соединении и развитии национальной информационной инфраструктуры, включая информационное оружие. Достижение этой цели обеспечит Соединенным Штатам не только сохранение политического, экономического лидерства, военного и информационного превосходства в XXI веке, но и создаст выгодные условия развязывания информационной войны.

2. Следует учитывать особенность так называемого "стратегического партнерства" США и России, суть которого заключается в том, что российские геополитические интересы могут признаваться и поддерживаться Соединенными Штатами только в тех случаях, если они отвечают американским стратегическим интересам. США всегда и всюду стремятся играть по своим правилам, что никак нельзя назвать "равноправным партнерством". Эти правила, естественно, распространяются и в отношении глобального информационного пространства, контроль за которым постепенно захватывают США.

3. Судя по всему, информационная война может начаться внезапно, без какой-либо осозаемой подготовки. В самом деле, началу обычной войны предшествует обширный комплекс довольно продолжительных подготовительных мероприятий, скрыть которые практически невозможно.

Информационная же война может начаться сразу, без особой подготовки (которая в принципе не нужна), с массированного применения различных систем ИНФОР, которые не требуют предварительной переброски, сосредоточения, а действуют мгновенно по командам либо с удаленных от объектов поражения специальных пультов управления, либо по сигналам от портативных пультов, которыми заблаговременно оснащены особо законспирированные агенты.

4. В создавшихся в настоящее время условиях "прозрачности" российских границ и ослабления контрразведывательного режима иностранные спецслужбы располагают широкими возможностями для скрытого внедрения различных систем ИНФОР в электронные сети управления стратегических объектов РФ.

5. Довольно серьезную опасность представляет сеть "Интернет", которая уже дотянулась до России, хотя ее паутина еще "чрезвычайно тонка и крупноячеиста" (может быть, в этом пока заключается наша "противоинформационная оборона"). Но, судя по материалам, публикуемым в нашей прессе, уже сейчас речь идет об "интернетизации всей страны". В связи с этим обращает на себя внимание деятельность известного американского "филантропа и биржевого спекулянта" Дж. Сороса, создавшего Международный научный фонд для поддержки фундаментальных научных исследований в России. Дж. Сорос считает, что наиболее выгодные инвестиции для приближения России к открытому обществу-это создание информационной и коммуникационной инфраструктуры, независимой от государства. Здесь есть над чем задуматься... Обычно инвесторы-самые осторожные и даже пугливые дельцы, а тут такая благотворительность

на сотню миллионов долларов. К чему бы это? Оказывается, суть в том, что создаваемая г-ном Соросом в России информационная инфраструктура должна подключаться... к сети Интернет и таким образом Россия должна стать частью мирового информационного пространства, в котором фактически могут оказаться не только электронные сети учебных заведений, но и парламентские и правительственные сети. Почва для этого уже подготовлена. Так, составление документов в аппарате правительства ведется в рамках отдельной сети. Госдума РФ также имеет свою сеть, региональные администрации-свои. Теперь задача, по Соросу, состоит в том, чтобы накинуть на все эти пока разрозненные сети общую паутину и привязать ее через "Интернет" к глобальному информационному пространству.

Таким образом, центральные и местные информационные сети РФ вполне могут оказаться объектами воздействия информационного оружия. Итак, в свете перечисленных опасностей, которые таит в себе информационная война, естественно возникает закономерный вопрос: что делать, каким образом Россия могла бы парировать эти патентиальные угрозы? (1)

Борьба за информацию-реальность нынешнего дня. Сегодня правомерно утверждать: чем большими возможностями в информационной сфере обладает государство, тем вероятнее оно может добиться геополитических стратегических преимуществ.

Работы в сфере информационного противоборства в России начаты с запозданием. Они ведутся рядом ведомств без должной координации и целевого бюджетного финансирования, что в целом может привести к ослаблению национальной безопасности России. В настоящее время отсутствует единая система обеспечения информационной безопасности; определяющая координатора решения вопросов в этой области, роль и полномочия различных ведомств с учетом специфики их деятельности. Кроме того, отсутствует законодательная и правовая база, определяющая порядок организации работ.

В 1994г. при Совете безопасности России была создана Межведомственная комиссия по информационной безопасности, имеющая статус коллегиального совещательного органа.

Сознавая политическое значение формирования современной инфраструктуры России и обеспечения ее информационной безопасности, Федеральное агентство правительственный связи и информации (ФАПСИ) при Президенте РФ с 1993 года провело комплекс работ по анализу вопросов, связанных с информационным обеспечением органов государственной власти РФ, экономически значимых структур, субъектов финансового и фондового рынков. Итоги этой работы нашли свое отражение в разработанной ФАПСИ Программе создания и развития информационно-телекоммуникационной системы специального назначения (ИТКС). Указом Президента РФ от 3.04.95г. N334 этой программе придан статус президентской, а постановлением Правительства РФ от 2 февраля 1996г. N87-4 она утверждена как федеральная целевая программа (6).

Чтобы ответить на вопрос, каким образом Россия могла бы парировать угрозу информационной войны, следует учитывать следующие соображения.

1. Первое слово в оценках вышеуказанных угроз, естественно принадлежит разведке. Необходимо непрерывное отслеживание всего комплекса проблем, касающихся развития ИНФОР и подготовки к информационной войне государств, располагающих наиболее совершенной инфраструктурой. Говоря конкретно, необходима достоверная количественная, качественная и психологическая оценка ИНФОР и способов его применения. Необходим также периодический анализ геостратегической ситуации с прогнозом глобальных и локальных противоречий и конфликтов, содержащих угрозу возникновения информационной войны. Эти оценки и анализ могут служить основой для выработки национальной концепции противодействия угрозе информационной войны.

2. Следовало бы развернуть систематические и целенаправленные теоретические исследования проблем создания собственных защищенных информационных сфер. В этой работе было бы полезно использовать соответствующий опыт США, Японии и других стран, обладающих развитой информационной инфраструктурой.

3. Неотложной задачей можно считать организацию тщательной проверки и доработки импортных информационных систем, функционирующих в государственных (особенно в военных) структурах, с целью поиска и устранения "дыр безопасности" и диверсионных программных закладок.

4. Особо приоритетной задачей должна быть разработка собственного информационного оружия, которое могло бы считаться необходимым дополнением в качестве "информационного обеспечения" ВС России. Однако здесь важно не допустить известных печальных ошибок периода гонки вооружений. А для этого следовало бы тщательно изучить все имеющиеся данные об иностранных видах информационного оружия с тем, чтобы своевременно обнаружить вероятную дезинформацию о характеристиках ИНФОР и способах его применения. Необходимо иметь в виду, что популистских изданий об ИНФОР имеется немало и что значительная часть материалов по ИНФОР, видимо, закрыта (как, например, перед началом второй мировой войны в США, Великобритании и Германии были закрыты все материалы по ядерным исследованиям). Вот почему в этой сфере деятельности было бы целесообразно использовать систему многостороннего мониторинга.

5. Строгое соблюдение правил информационной безопасности должно стать одним из основных требований в экономической, военной и научно-технической политике РФ. Однако эти правила (если, конечно, таковые имеются) необходимо четко сформулировать, систематизировать. А вообще говоря, видимо, необходим "Информационный кодекс", нарушение которого должно считаться тяжким преступлением. Кодекс должен содержать четкое определение: информационная политика государства должна быть протекционистской, направленной на развитие российских информтехнологий, защищающей внутренний рынок от проникновения скрытых элементов ИНФОР. Это приобретает

важное значение в связи с массовыми закупками информационных средств за рубежом и широким использованием их не только в частном секторе, но и в государственных учреждениях. При этом следует иметь в виду, что пользователи импортных информационных систем главное внимание обращают на их исправность и надежное функционирование, а что в этих системах имеется еще, вряд ли их интересует. Здесь просматривается необходимость специального технического контроля приобретаемых информационных систем, контроля по специальной методике, разработку которой следовало бы поручить соответствующим НИИ.

6. Участие России в международных системах телекоммуникаций и обмена информацией должно носить плановый характер и быть монополией государства. Только при этом условии Россия может сохранять "информационную независимость" и принимать в централизованном порядке необходимые контрмеры для противодействия информационному оружию. В этом аспекте следует учитывать, что сеть "Интернет" может служить потенциальному агрессору легальным средством для решения задач, возлагаемых на информационное оружие.

7. Подготовка "информационных кадров". Это, пожалуй, одна из главных проблем "информационной политики" РФ. Для ее решения необходимо создать государственное высшее учебное заведение, а также факультеты в соответствующих вузах для подготовки специалистов естественно-научного и инженерно-технического профиля по защите информационных систем или сетей. В военных академиях и военных училищах следовало бы ввести специальные курсы с целью детального изучения проблем, касающихся информационного оружия и информационной войны.

8. Поскольку Россия в данное время, видимо, относится к числу стран, в которых создание собственной защищенной информационной инфраструктуры запаздывает, а запретить создание ИНФОР вряд ли практически возможно (как это, например, сделано в отношении химического и бактериологического оружия), то представляется весьма важным и неотложным делом международное сотрудничество с целью выработки и принятия правовых документов, обеспечивающих информационную безопасность в условиях современной открытости информационного (кибернетического) пространства и "прозрачности" российских границ. В частности, должны быть определены и юридически закреплены меры международного контроля для предотвращения компьютерных преступлений и установления ответственности за их совершение.

И здесь Россия вполне могла бы выступить инициатором разработки и заключения международной конвенции по ограничению информационного оружия и предотвращению информационных войн.

Главная цель такой конвенции-обеспечение национальной безопасности и независимости государств от "информационной экспансии" стран с развитой информационной инфраструктурой и запасами информационного оружия (1).

Но существует ли вообще эффективная и надежная защита от воздействия

этого своеобразного оружия? Совершенно очевидно, что в настоящее время решение этой проблемы становится высокоприоритетной задачей для любых государств современного мира, в том числе и для России. И прежде всего следует надежно обеспечить защиту информационного оборудования на территории России от возможного проникновения "скрытых элементов" информационного оружия.

Таким образом, главной отличительной чертой атакующего информационного оружия является универсальность и радикальный характер воздействия, скрытность, возможность широкого выбора места и времени его применения, а также очевидная экономичность в сравнении с использованием других современных вооружений.

Необходимо также учитывать, что организация единого международного информационного пространства требует высокой степени унификации информационных и телекоммуникационных технологий. Используя это обстоятельство, такие мощные индустриальные державы, как США и Япония, могут реализовать свое лидирующее положение в области информации для достижения политических, экономических и военных целей. Они получают реальную возможность осуществления глобального информационного контроля над мировым сообществом и навязывания другим странам своих правил и образа жизни.

Уже в настоящее время этими странами осуществляется информационно-культурная и информационно-идеологическая экспансия по мировым телекоммуникационным сетям, в том числе и по "Интернету", а в будущем и через "супермагистраль" (3).

Информационная сфера России является важной составляющей общественной жизни, во многом определяющей перспективы успешного осуществления социально-политических и экономических преобразований российского общества.

Под информационной безопасностью РФ понимается состояние защищенности жизненно важных интересов граждан, общества и государства в информационной сфере.

Информационная безопасность играет ключевую роль в обеспечении жизненно важных интересов РФ. Практика государственного строительства последних лет показала, что стране необходим программный документ, определяющий политику государства в области обеспечения информационной безопасности.

Целью разработки Доктрины информационной безопасности РФ является определение ключевых проблем обеспечения безопасности, консолидация усилий организаций различных форм собственности на реализацию единой политики обеспечения информационной безопасности.

Проект Доктрины информационной безопасности РФ базируется на современных взглядах на проблемы информационной безопасности, основных программных документах, определяющих приоритеты текущей политики, накопленном отечественном и зарубежном опыте решения проблемы обеспечения безопасности в информационной сфере.

Доктрина информационной безопасности РФ состоит из пяти разделов:  
Общие положения.

Угрозы информационной безопасности РФ.

Методы обеспечения информационной безопасности РФ.

Основы государственной политики в области обеспечения информационной безопасности РФ.

Организационная структура и принципы построения системы обеспечения информационной безопасности РФ.

За последние годы в Российской Федерации реализован комплекс практических мер по совершенствованию информационной безопасности.

Приняты Законы РФ "О государственной тайне", "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", "Основы законодательства РФ об Архивном фонде РФ и архивах", ряд других законов, развернута работа по созданию механизмов их реализации, завершена подготовка ряда законопроектов, регламентирующих общественные отношения в информационной сфере.

Осуществлен ряд практических мероприятий по обеспечению информационной безопасности в органах государственной власти, в организациях. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения безопасности способствует создание государственной системы защиты информации, системы лицензирования деятельности организаций в области защиты информации и системы сертификации средств защиты информации.

Вместе с тем анализ современного состояния информационной безопасности России показывает, что ее уровень в настоящее время не в полной мере соответствует потребностям общества и государства (7).

### **Что скрывается за кулисами информационной борьбы?**

Что же такое информационная борьба? Это сбор информации, ее распространение (или замалчивание) в интересах более эффективного противодействия противнику. Образно говоря, это война внутри войны.

Основное оружие информационной борьбы-все виды разведки и средства массовой информации. Сюда можно отнести также и контрпропаганду, начиная от простейших слухов и сплетен, до глубокой психологической обработки "промыванием мозгов" в глобальном масштабе средствами радио и телевидения.

Именно огромные возможности современного радиовещания и телевидения позволяют говорить о победах и поражениях в информационной борьбе, которая ведется в мире последние пятьдесят лет.

Пример-победа коалиционных сил над иракским диктатором Саддамом Хусейном. Информационная война велась в виде разведки, психологической и

радиоэлектронной борьбы. Она сочеталась с последующим применением высокоточного управляемого оружия воздушного, наземного, морского и подводного базирования. Во все страны мира поступали по спутниковым каналам связи круглосуточные программы кабельной сети новостей Си-эн-эн. Не обошлось и без "утечки информации государственной важности". Буквально накануне начала боевых действий начальник штаба ВВС "проговорился" в печати и по телевидению, что боевые действия начнутся с боевой операции.

Было много телесюжетов, которые "свидетельствовали" о слабости США, их нерешительности, страхе перед большими потерями. Все это, безусловно, наблюдал по телевидению и анализировал в Багдаде Саддам Хусейн, полагая, что Америка готовится к войне с очень большими потерями, что американцы в своей значительной части против войны и что вооруженные силы еще не полностью готовы к боевым действиям. Так он в какой-то степени был обманут американскими телевизионщиками.

Операция "Буря в пустыне" началась в ночь с 17 января 1991г. мощным ударом радиоэлектронных помех по всем работающим радиоэлектронным средствам Ирака, в первую очередь по радиолокационным средствам ПВО, объектам связи и управления войсками и оружием.

В рамках сугубо военных операций проходили и мероприятия по линии информационной борьбы. В ходе ведения психологической борьбы наблюдалось "разделение труда". Армейские средства использовались против войск Саддама, а государственные органы доводили "нужную" информацию до гражданского населения.

Ливень бомб на позиции иракских войск сопровождался снежной бурей листовок, которые были частью проводимой кампании психологических операций. Только за первые три недели войны было распространено 15 млн. листовок. Рассчитанные на низкий уровень образования иракских солдат, они (в картинках) призывали к сдаче в плен. Особой популярностью среди иракских солдат пользовались листовки, где говорилось, что каждый сдавшийся в плен получит сразу три пачки "Мальборо" и трехразовое горячее питание. Для людей, проторчавших в окопах более месяца без горячей пищи и курева, такие листовки были путевкой в рай. А для того, чтобы солдат Хусейна шел правильной дорогой в плен, на ее обратной стороне подробно описывалось, куда и как ему следует идти.

Населению, а также солдатам противника было заброшено 15 тыс транзисторных радиоприемников, имеющих фиксированную настройку на частоту проамериканского "Голоса свободного Ирака". Широко велась пропаганда через американские армейские звуковещательные средства.

Основанием для ведения психологических операций в рамках информационной борьбы служили три директивы президента Дж. Буша. Этими документами регламентировалась деятельность разведслужб, занимающихся проблемами арабского мира, психологов, армейских органов психологической борьбы. Сам факт подписания этих документов говорит о многом.

Явное превосходство союзников над Хусейном было только в условиях дальнего боя. В условиях ближнего боя, то есть ближе 300 м, превосходство было уже на стороне иракцев. Здесь эффективность информационной борьбы очень мала, но зато велика эффективность простейших видов стрелкового оружия-автоматов Калашникова и ручных противотанковых гранатометов. И если бы американцы и их союзники вступили в иракские города, то их ожидала бы кровавая бойня. На руках фанатичных ополченцев было более двух миллионов "калашниковых" и десятки тысяч противотанковых гранатометов.

Так что Дж. Буш, как верховный главнокомандующий, представлял тогда, к чему мог привести ввод войск союзников (3).

Некоторые исследователи полагают, что война в Персидском заливе ознаменовала конец эры классических и начало эры электронных, информационных, компьютерных, космических, экологических и других войн, имеющих иную основу.

В армиях США и стран НАТО огромное внимание уделяется информационно-пропагандистскому обеспечению действий войск и сил флота. Во время операций авиации стран НАТО в Боснии при помощи только особым образом подготовленных видеоматериалов, демонстрировавшихся транснациональными и национальными службами новостей, у десятков миллионов зрителей многих стран было сформировано позитивное мнение по отношению к так называемым точечным ударам. Не говоря уже о других, более сложных методах и приемах. Между тем в российской армии информационно-пропагандистское обеспечение оставляет желать лучшего. Достаточно вспомнить о подобном обеспечении операций в Чечне (8).

Разрабатываемая на Западе концепция информационной войны включает:

- подавление элементов инфраструктуры государственного и военного управления (поражение центров командования и управления);
- электромагнитное воздействие на элементы информационных и телекоммуникационных систем (радиоэлектронная борьба),
- получение разведывательной информации путем перехвата и анализа больших объемов информации в открытых каналах связи, перехвата и дешифрования информационных потоков, передаваемых по закрытым каналам связи, а также по побочным излучениям и за счет специально внедренных в помещения и технические средства электронных устройств перехвата информации (радиоэлектронная разведка);
- осуществление несанкционированного доступа к информационным ресурсам путем использования программно-аппаратных средств прорыва системы защиты информационных и телекоммуникационных систем противника с последующим искажением, уничтожением или хищением информации либо нарушением нормального функционирования этих систем (хакерная война);
- распространение по информационным каналам противника или в мировом информационном пространстве дезинформации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения, с целью

формирования общественного мнения, выгодного для воздействующей стороны (психологическая война).

Концепция информационной войны является одной из последних, разработанных в Пентагоне. Оружием информационной войны являются информационные устройства и технологии, которые используются для широкомасштабного, целенаправленного, быстрого и скрытного воздействия на военные и гражданские информационные системы противника с целью разрушения его экономики, подрыва боеготовности и боеспособности. При этом предполагается, что информационная война может вестись как самостоятельно, то есть без применения традиционных средств и способов вооруженной борьбы, так и в сочетании с другими видами боевых действий.

По своему характеру информационная война занимает положение между "холодной" и "горячей" войной. Результатом информационной войны является реальное нарушение функционирования элементов инфраструктуры противника (пунктов управления, ракетных и стартовых позиций, аэродромов, портов, систем связи, складов и т.д.).

По мнению американских специалистов, информационная война стала возможной благодаря "кибернетической революции", результатом которой было массовое внедрение во все сферы жизни различных информационных систем, основанных на применении электронных устройств. Эффективность и возможности информационной войны непрерывно увеличиваются в соответствии с ростом возможностей и распространением микропроцессоров, высокоскоростных систем, получения и обработки данных, сложных датчиков-мощного оружия в руках тех, кто знает, как им распорядиться.

Военные специалисты США считают, что в будущей информационной войне найдут применение различные специфические средства, и прежде всего программные. Это специальные "программные закладки", которые при использовании в системах оружия, поставляемых вероятному противнику, сделают их неэффективными при внешней безотказности. Помимо этого предлагается использовать специальные устройства, которые при взрыве создают мощный электромагнитный импульс, или биологические средства, в частности, особые виды микробов, способные уничтожить электронные схемы и изолирующие материалы в компьютерах.

Информационная война может предшествовать боевым действиям или заменять их, а применяемые в ней методы и техника значительно увеличат боевые возможности обычных сил и вооружений.

Мнение американских военных специалистов о необходимости активных разработок в области информационной войны единодушно. Основной проблемой безопасности своей страны они считают уязвимость от информационной войны. В связи с этим специалисты обращают особое внимание на обеспечение защиты как военных, так и гражданских информационных систем, имеющих особое значение для нормального функционирования государственных структур.

Военно-политическое руководство США считает, что значение информа-

ционной войны неуклонно возрастает по мере развития общества, и намерено принять все возможные меры, чтобы победить в ней (9).

По мнению западных специалистов, ключом к господству на поле боя в будущем станет обеспечение своих войск оперативной и достоверной информацией. Предполагается, что компьютерная технология охватит все категории военнослужащих - от рядового до генерала.

В одной из военных лабораторий США создан образец "амуниции пехотинца XXI в". В комплект входит шлем, оснащенный микрофоном, наушниками, очками ночного видения и дисплеем (на уровне глаз), на который будут передаваться изображение поля боя с высоты птичьего полета и постоянно обновляющиеся данные разведки. Компьютер, вмонтированный в бронежилет, позволит военнослужащему управлять вооружением, идентифицировать цели ("свой-чужой"), определять зараженные участки местности и свое местонахождение.

К 2010 году планируется осуществить полную компьютеризацию на поле сражения, т.е. обеспечить взаимосвязь военнослужащих с системами вооружения посредством электроники. Глобальная компьютеризация вооруженных сил повысит эффективность их действий и увеличит вероятность поражения различными видами информационного оружия, например, компьютерными "вирусами", электронными "логическими бомбами" и т.д.

Споры о новых видах оружия несмертельного действия начались одновременно с дебатами о роли США в мире после окончания "холодной войны". Новое оружие должно было изменить представление о современных военных действиях, а его разработка и применение должны способствовать переходу от войн индустриальной эры с их истреблением противника "огнем и мечом" к войнам века информации, когда нужно парализовать противника, не уничтожая его.

Большинство футурологов считает, что в перспективе расширение сфер влияния и границ империй будет зависеть не от результатов военных действий в привычном их понимании, а от исхода борьбы за контроль над информационной средой.

По мнению зарубежных аналитиков, с внедрением несмертельного оружия и растущим нежеланием правительств подвергать свои вооруженные силы риску (особенно в миротворческих акциях) все более важную роль начинают играть психологические операции. В связи с этим особое внимание обращается на разработку информационного оружия на базе компьютерных технологий, которое используется для психологического воздействия. К их числу относятся технологии, связанные с глобальной сетью INTERNET и воздействующие на подсознание, а также средства создания лазерных голограмических изображений.

Зарубежные специалисты предполагают, что всемирная компьютерная сеть может стать новым глобальным "полем боя" для будущих информационных войн (10).

## ЗАКЛЮЧЕНИЕ

Итак, в мире появился новый вид боевых действий-информационно-психологическое противоборство. Появилось новое "несмертоносное", "информационное", "психологическое" оружие, которое используется как эффективный способ достижения политических, экономических, военных целей еще до применения военной силы. То есть оружие, которое не убивает, не разрушает, но позволяет добиться победы с минимальными потерями.

Значит, верно мнение: кто владеет информацией, тот владеет миром. Вопросы влияния информатизации на политический статус страны в мире, на политическую власть, ее распределение являются центральными в политической жизни.

Исследователи утверждают, что за счет концентрации информации происходит усиление геополитического потенциала технически передовых держав; наблюдается рост возможностей исполнительной власти, власти государственного аппарата.

Геополитическая значимость информационной техники и информационных ресурсов растет в связи с закономерной информацией всех сфер общества, особенно экономики, науки, политики, военного дела.

Информация теперь считается стратегическим национальным ресурсом, одним из основных богатств страны. Под воздействием информации экономика приобретает новые качества-качество гибкости, динаминости, малой материально- и энергоемкости, экологичности и т.д. Возвращаясь назад на 10-15 лет, скажем, что СССР распался во многом потому, что политическое руководство страны поздно поняло всю серьезность этого нового поворота в научно-техническом прогрессе.

Война есть продолжение политики, а армия сильнейшее средство и решающий аргумент в руках политиков. В военном деле наступает новый, постъядерный этап, развертывается новая военно-техническая революция-переход от чреватого гибелью цивилизации оружия массового поражения к высокоточному, избирательному, контрактивному и информационному оружию, которое не угрожает экологической катастрофой, но может быть эффективным средством достижения политических и экономических целей.

## **ЛИТЕРАТУРА**

1. Информационная война. Ближайшее будущее. Инженер, №9, 1995.
2. Ядерную кнопку заменит клавиша Enter. Инженер, № 12, 1997.
3. Информация-оружие. Инженер, №10, 1997.
4. Пентагон на страже информационного пространства Америки. Независимое военное обозрение №30, 1997.
5. Китай готовится к информационным войнам. Независимое военное обозрение №13, 1998.
6. Борьба за информации. Красная Звезда. 15 августа, 1997.
7. Доктрина информационной безопасности. Информационное общество. № 2-3, 1997.
8. Что скрывается за кулисами информационной войны. Ориентир, №2, 1997
9. Информационная война в планах Пентагона. Зарубежное военное обозрение, №2, 1997.
10. Информационное воздействие и компьютерные технологии. Зарубежное военное обозрение, №7, 1997.

## **СОДЕРЖАНИЕ**

Введение.....	..3
Информационная война.....	4
Подготовка к информационной войне в США.....	9
Пентагон на страже информационного пространства Америки.....	13
Традиции противоборства.....	17
КНР и США присматриваются друг к другу.....	18
Защита информационного пространства России.....	19
Что скрывается за кулисами информационной борьбы.....	25
Заключение.....	30
Литература.....	31