# МИФИ

**Военная кафедра**

**Реферат по теме:**

**“Информационная война – что это такое?”**

**Студент: Киреев Анатолий**

**Взвод №43**

**Москва 1999**

### Содержание

Вступление 3

Определение и сфера действия 5

Истоки и статус доктрины 11

Военные игры как средство подготовки к возможным конфликтам 12

Оборонительная составляющая 14

Другие точки зрения 17

Человеческий фактор 20

Другие аспекты 22

Сегодня 23

В поисках рационального зерна 25

Список литературы 26

### Вступление

Время и события побуждают серьезно поразмыслить над поставленным в названии реферата вопросом: безопасности информационных систем угрожают не только и не столько несовершеннолетние хакеры и недовольные сотрудники. Появление этого термина означает, что предстоит столкнуться с менее проработанной, но несомненно более серьезной угрозой со стороны внешних и внутренних враждебных сил. Наиболее полно, в настоящее время, эта проблема изучена в США, этим объясняется использование в реферате, в основном, американских источников.

Опубликованное "Пособие Института компьютерной безопасности по компьютерной преступности и информационной войне: существующие и потенциальные угрозы" вызвало многочисленные отклики экспертов по информационной безопасности из частного сектора, академических кругов, правоохранительных органов и военных ведомств, органов национальной безопасности. Комитет по правительственным делам Сената США провел серию слушаний по компьютерной безопасности. Министерстве юстиции сформирована специальная группа под названием "Группа обеспечения кибербезопасности" (Cyber Security Assurance Group), призванная оказывать содействие в защите компьютеров от нападений в информационном пространстве, реагировать на чрезвычайные ситуации и расследовать любые диверсии кибертеррористов. Выработана программа контроля безопасности киберпространства.

Итак, "информационная война" - новомодное словечко или это понятие пополнит лексикон информационной безопасности? Мартин Либики из Университета национальной обороны высказался так: "Попытки в полной мере осознать все грани понятия информационной войны напоминают усилия слепых, пытающихся понять природу слона: тот, кто ощупывает его ногу, называет ее деревом; тот, кто ощупывает хвост, называет его канатом и так далее. Можно ли так получить верное представление? Возможно, слона-то и нет, а есть только деревья и канаты. Одни готовы подвести под это понятие слишком много, другие трактуют какой-то один аспект информационной войны как понятие в целом...". Это мнение свидетельствует о том, что окончательная формулировка пока не выкристаллизовалась, но процесс идет. Так что же думают по этому поводу штатские? Что говорят и делают военные?

### Определение и сфера действия

Следует отличать информационную войну от компьютерной преступности. Любое компьютерное преступление представляет собой факт нарушения того или иного закона. Оно может быть случайным, а может быть специально спланированным; может быть обособленным, а может быть составной частью обширного плана атаки. Напротив, ведение информационной войны никогда не бывает случайным или обособленным (и может даже не являться нарушением закона), а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий - будь то на реальном поле брани, либо в экономической, политической или социальной сферах.

Театр информационных боевых действий простирается от секретного кабинета до домашнего персонального компьютера и ведется на различных фронтах.

Электронное поле боя представлено постоянно растущим арсеналом электронных вооружений, преимущественно засекреченных. Говоря военным языком, они предназначены для боевых действий в области командования и управления войсками, или "штабной войны". Последние конфликты уже продемонстрировали всю мощь и поражающую силу информационных боевых действий - война в Персидском заливе и вторжение на Гаити в прошлом году. Во время войны в Персидском заливе силы союзников на информационном фронте провели комплекс операций в диапазоне от старомодной тактики разбрасывания пропагандистских листовок до вывода из строя сети военных коммуникаций Ирака с помощью компьютерного вируса.

Атаки инфраструктуры наносят удары по жизненно важным элементам, таким как телекоммуникации или транспортные системы. Подобные действия могут быть предприняты геополитическими или экономическими противниками или террористическими группами. Примером служит вывод из строя междугородной телефонной станции компании AT&T в 1990 году. В наши дни любой банк, любая электростанция, любая транспортная сеть и любая телевизионная студия представляют собой потенциальную мишень для воздействия из киберпространства.

Промышленный шпионаж и другие виды разведки грозят великим множеством тайных операций, осуществляемых корпорациями или государствами в отношении других корпораций или государств; например, сбор информации разведывательного характера о конкурентах, хищение патентованной информации и даже акты саботажа в форме искажения или уничтожения данных. Иллюстрацией этой угрозы служит документально доказанная деятельность французских и японских агентов на протяжении восьмидесятых годов.

Сбор разведывательной информации также выходит на новые рубежи. Лаборатория Линкольна в Массачусетском технологическом институте разрабатывает аппарат для воздушной разведки размером с пачку сигарет. Другая лаборатория работает над химическими веществами, которые можно ввести в провизию неприятельских войск, чтобы позволить датчикам отслеживать их перемещение по дыханию или выделению пота. Помимо этого уже имеются спутниковые системы слежения имеющие разрешающую способность в несколько сантиметров.

Конфиденциальность все более уязвима по мере появления возможности доступа к постоянно растущим объемам информации в постоянно растущем числе абонентских пунктов. Важные персоны таким образом могут стать объектом шантажа или злобной клеветы, и никто не гарантирован от подложного использования личных идентификационных номеров.

Как бы то ни было, термин "информационная война" обязан своим происхождением военным и обозначает жестокую и опасную деятельность, связанную с реальными, кровопролитными и разрушительными боевыми действиями. Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психологические операции и так далее.

Следующее определение вышло из стен кабинета Директора информационных войск Министерства обороны:

**"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 нашей собственной информации и информационных систем”**. Информационная война представляет собой всеобъемлющую, целостную стратегию, призванную отдать должное значимости и ценности информации в вопросах командования, управления и выполнения приказов вооруженными силами и реализации национальной политики. Информационная война нацелена на все возможности и факторы уязвимости, неизбежно возникающие при возрастающей зависимости от информации, а также на использование информации во всевозможных конфликтах. Объектом внимания становятся информационные системы (включая соответствующие линии передач, обрабатывающие центры и человеческие факторы этих систем), а также информационные технологии, используемые в системах вооружений. Информационная война имеет наступательные и оборонительные составляющие, но начинается с целевого проектирования и разработки своей "Архитектуры командования, управления, коммуникаций, компьютеров и разведки", обеспечивающей лицам, принимающим решения, ощутимое информационное превосходство во всевозможных конфликтах.

Многие ведущие стратеги полагают, что противостояние армий, погибающих на полях генеральных сражений, очень скоро займет свое место на свалке истории рядом со шпорами и арбалетами. Высшая форма победы теперь состоит в том, чтобы выигрывать без крови. В то же время довольно трудно представить боевые действия как игру на видеоприставке без страха и боли.

Каждый род войск создал в Пентагоне свою собственную рабочую группу по проблемам информационных боевых действий.

"Force 21" - название проекта полной модернизации вооружений и организационной перестройки, успешная реализация которого сулит появление абсолютно новых сухопутных войск США, в которых солдаты, танковые экипажи, пилоты вертолетов и командиры будут в мгновение ока получать информацию с полей сражений с помощью портативных или настольных компьютеров. Такие сухопутные силы обладали бы способностью наблюдать события в масштабе реального времени, и командование имело бы возможность четко и быстро принимать решения и действовать. Вооруженные силы США намерены фундаментально подготовиться к вступлению в грядущий информационный век.

В соответствии с проектом "Force 21", сенсорные устройства Глобальной Cистемы Позиционирования (GPS) используют спутниковую информацию для определения местонахождения личности. В сухопутных войсках разрабатывают новые системы коммуникаций, радары и имитационные модели с тем, чтобы в любой момент операции буквально каждый от окопа до штаба знал, где он находится, где дислоцировано его подразделение, где расположился противник и какими должны быть наилучшие варианты действий.

Один американский научно-исследовательский коллектив в следующем году представит новый боевой шлем "воина двадцать первого века", оснащенный микрофонами и головными телефонами для связи, прибором ночного видения и датчиками теплового изображения, а также дисплеем перед глазами, который предоставит корректировки дислокации и разведывательные данные. Так видится сегодня идеальная модель. Но чтобы модернизировать арсеналы сухопутных войск, суммы, выделенные на закупки вооружений, должны быть увеличены почти в три раза и составить 21 млрд. долларов.

Вряд ли скоро найдутся такие средства, а кроме того, конкуренцию сухопутным войскам составляют военно-морской флот, военно-воздушные силы, морская пехота.

В настоящее время каждый вид вооруженных сил имеет свой собственный специализированный центр: например, Центр информационных боевых действий Военно-воздушных сил США (AFIWC) расположен на военно-воздушной базе Келли в штате Техас, а Служба наземных информационных боевых действий Армии США (LIWA) находится в Форт Белвуар, штат Вирджиния.

Задачи Центра AFIWC состоят в том, чтобы "создавать средства ведения информационной войны в поддержку операций; планировать кампании, приобретать и испытывать оборудование, защищать военно-воздушные штабы от нападения". С этой целью Центр обучает, экипирует и развертывает группы реагирования, разрабатывает и поддерживает базы данных и прикладные программы, проводит анализ уязвимости электронных систем военно-воздушных сил. Усилиями сотрудников Центра AFIWC создана Распределенная система определения вторжений (DIDS), которая выявляет злоупотребления компьютерными системами, отслеживает бюджеты пользователей, род занятий и место их происхождения; обеспечивает централизованный доступ к информации о состоянии безопасности той или иной системы и распределяет обработку проверяемых данных; фактически, это инструмент администраторов сетей и сотрудников служб компьютерной безопасности.

Таким образом, под угрозой информационной войны понимается намерение определенных сил воспользоваться поразительными возможностями, скрытыми в компьютерах, на необозримом кибер-пространстве, чтобы вести "бесконтактную" войну, в которой количество жертв (в прямом значении слова) сведено до минимума. "**Мы приближаемся к такой ступени развития, когда уже никто не является солдатом, но все являются участниками боевых действий**, - сказал один из руководителей Пентагона. - **Задача теперь состоит не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума**".

Гражданская информационная война может быть развязана террористами, наркотическими картелями, подпольными торговцами оружием массового поражения. Крупномасштабное информационное противостояние между общественными группами или государствами имеет целью изменить расстановку сил в обществе.

Поскольку такая война связана с вопросами информации и коммуникаций, то если смотреть в корень, это есть война за знания - за то, кому известны ответы на вопросы: что, когда, где и почему и насколько надежными считает отдельно взятое общество или армия свои знания о себе и своих противниках.

Вот пример. В марте 1996 года один из американских университетов обнародовал в Internet страницы секретной информации с описанием британских военных объектов в Северной Ирландии. Доступ к этому абонентскому пункту можно получить из любой точки земного шара и узнать подробные данные об армейской аппаратуре в Северной Ирландии, адреса предполагаемой базы службы МИ-5 и двух опорных пунктов Штаба верховного главнокомандования. Адреса директора и координатора разведывательной службы приводятся вместе с картой, демонстрирующей все военные базы и подробности операций британского экспедиционного корпуса.

Позже, правда, абонентский пункт был удален из главного компьютера Университета штата Техас, и при этом сообщалось, что указанная информация была предоставлена партией Шин Фейн. Очевидно, что фактически партия располагает гораздо большими сведениями и, скорее всего, не преминет извлечь из этого максимальную пользу.

### Истоки и статус доктрины

В последней четверти нашего столетия возникло и развивается положение о том, что в своем развитии человечество одолело "первую волну" (сельскохозяйственную), которая началась 10000 лет назад, и "вторую волну" (промышленную), которая началась 300 лет назад, что каждая из этих волн принесла цивилизации революционные изменения; в настоящее время идет "третья волна" (технологическая), которая, как и в первых двух случаях, должна принести свою экономику, свою структуру семьи, свои средства массовой информации, свои политические институты, равно как и свой собственный период болезненного и хаотичного становления и, конечно же, свой способ и характер ведения войны.

Осознание этих процессов привело к возникновению термина информационная война.

Но понятия, используемые для определения и изучения информационной войны и ее последствий, все еще не устоялись и могут измениться в результате иной классификации в будущем. Пожалуй, потребуются новые законодательные акты и не исключено, что придется переписать все международные законы и договоры.

### Военные игры как средство подготовки к возможным конфликтам

Стратеги информационной войны играют в военные игры. Они придумывают сценарии атаки и обороны вероятных целей как в военной системе командования и управления, так и в телекоммуникациях, на транспорте и других жизненно важных объектах национальной инфраструктуры.

Вот некоторые из целей для ведения боевых действий, которые появились в ходе игры "По проводам" (июль/август 1993 года):

* Коммутатор в Кулпеппере, штат Вирджиния. Эта электронная станция обрабатывает все перечисления федеральных средств и операции с ними.
* Трубопровод на Аляске, по которому передается 10% всей нефти для внутреннего потребления США.
* Система электронной коммутации (ESS) управляющая всей телефонией.
* Internet - коммуникационный каркас науки и индустрии.
* Система распределения времени -- все крупные системы зависят от точного времени.
* Всемирная система военного командования и управления (WWMCCS), которая особо уязвима для "мягких" атак.
* “Большой голубой куб" рядом с Моффет-филд в Маунтин Вью, штат Калифорния - Тихоокеанский центр анализа и синтеза информации космической разведки.

Вот общее содержание некоторых сценариев. Для атаки коммутатора достаточно запрограммировать телефонные станции по всей территории Соединенных Штатов на подключение по всем исходящим телефонным линиям к коммутатору. Тем самым создается перегрузка телефонных линий, прекращение всех перечислений на длительный период и возникает необходимость крупномасштабной модификации всех систем, перечисляющих средства через этот коммутатор. Для защиты коммутатора следует перепрограммировать национальную коммутационную сеть так, чтобы она отвергала несанкционированные прямые связи на местном уровне, распределяя бремя отвергнутых вызовов по всей стране.

Для атаки на Internet можно открыть несколько сотен бюджетов на подставных лиц в машинах разнообразных коммерческих поставщиков и заставить эти машины рассылать всю электронную корреспонденцию из сотен списков рассылки по всем остальным спискам адресатов. Это привело бы к автоматической перерегистрации миллионов сообщений в стремительно расширяющемся цикле обратной связи, затрагивающем сотни тысяч компьютеров, - их диски забиты ненужной электронной корреспонденцией, а сеть - массой сообщений, отправленных по ненужным адресам. Для защиты сети необходимо воспользоваться средствами обнаружения злоупотреблений, выявить модели, создающие указанные проблемы, и запретить ньюс-группам передавать материалы без разрешения в явной форме. Еще лучше допускать конференции только с ограниченным числом участников.

### Оборонительная составляющая

Основными догматами оборонительных информационных боевых действий являются защита, обнаружение и реагирование. Защита обеспечивается фундаментальной информационной безопасностью. Обнаружение все еще является нерешенной проблемой. (Как, например, телефонная компания реально может определить, что она подверглась атаке?) Реагирование невозможно без осмотрительности. Прежде чем реагировать, уместно выяснить, не идет ли речь лишь о каком-то недоросле, который повел свою атаку, к примеру, из Германии, проникнув на один из немецких абонентских пунктов?

Во всяком случае, на фронте информационной безопасности ведется обширная работа. В США существуют различные проекты "Национальной информационной инфраструктуры", "Глобальной информационной инфраструктуры".

Рабочую группу (Аннаполис, штат Мэриленд), разрабатывающую предложения по национальной политике в области оборонительных информационных боевых действий, возглавляет заместитель министра обороны. Перед группой поставлена задача создать программу мероприятий, устраняющих угрозы жизненно важным системам командования, управления и коммуникаций. По завершении войны в Персидском заливе армейские стратеги ощутили настоятельную потребность в подобной разработке. Противник на себе смог оценить технические новинки и теперь угрожает повернуть наше оружие против нас. Дело в том, что, по некоторым оценкам, в Internet действуют 150 000 военных компьютеров, и 95% военных линий связи проходят по тем же телефонным линиям, которыми вы и я пользуемся ежедневно. Лишь 30% телекоммуникационных сетей, которые в данный момент предназначены для использования в случае военных действий, относятся к категории засекреченных, а остальные 70% приходятся на МСI, "Спринт", детскую сеть "Беллс", "Белкор" и другие коммерческие предприятия.

На заре компьютерной безопасности основу всех директив федерального правительства и Министерства обороны составляло требование закрыть на замок тот или иной главный компьютер. Но за последние 10 лет конфигурация сетей изменилась: ныне она призвана обеспечить взаимосвязь всего оборудования внутри сети и внешнюю связь с остальным миром (например, CNN в режиме диалога по Internet). При этом ценность информации неизмеримо возрастает. Полагаться на старый подход типа "посидим в компьютерном зале и посторожим центральный компьютер" уже не приходится; необходимо изучать абсолютно все электронные устройства, чтобы, получить представление об их потенциальном влиянии - модемную связь, связь по Internet, факсимильную связь, телефонную связь, кабели и провода. Когда каждый связан с каждым, это означает зависимость каждого от всех.

Реализация нового подхода возлагается на новое поколение. Каждый из студентов учебного класса Университета национальной обороны в Вашингтоне выглядит практически точно так же, как любой учащийся. Но эта группа серьезных юношей и девушек, специально отобранных из всех подразделений вооруженных сил, является авангардом революции в военном деле и обещает переписать заново тактику и стратегию будущих военных конфликтов. Эти студенты, сканирующие Internet на своих портативных компьютерах, представляют первое поколение кибернетических воинов. Их обучение - всего лишь часть подготовительных мероприятий Пентагона к тому дню, когда разразятся сражения между войсками, находящимися на расстоянии тысяч миль друг от друга; их оружие - клавиатура, с помощью которой они разрушают неприятельские коммуникации, манипулируют их средствами информации и крушат их финансовые системы.

Министерство обороны США "рассматривает оборонительные информационные боевые действия как нечто большее, но одновременно и использующее традиционные подходы. Способность противостоять нападению подразумевает применение всех этих подходов, но что более важно, включает в себя интегрированные средства защиты, обнаружения и реагирования. Защита от вторжений и злоупотреблений требует эффективных механизмов идентификации и аутентификации, высоконадежных брандмауэров, равно как и методов проверки и отслеживания".

При этом в Министерстве обороны полагают, что по мере повышения уровня знаний о возможных рисках и факторах уязвимости, исследования и выработка технических и методических решений для защиты, отражения, обнаружения и реагирования на случай агрессии будут в значительной степени отданы на откуп частному сектору. Взаимодействие государственного и частного сектора могло бы служить взаимному обогащению в результате разнообразия подходов в процессе совместной деятельности.

### Другие точки зрения

Однако существуют и другие взгляды на проблему. Высказываются мнения о том, что "информационная война" - это способ остаться на плаву людям, которые ищут, чем бы заняться после окончания холодной воины и так или иначе оправдывать расходные статьи бюджета. Им требуются новые точки приложения сил, вот они и стремятся стать активными участниками проектов в сфере электронной информации, с которыми выступила нынешняя администрация. Более того, акцент на оборонительные информационные боевые действия используется как предлог добиться давно желанного безраздельного господства в других, гражданских сферах компьютерной безопасности и технологического развития.

По мнению некоторых специалистов военные преследуют двоякую цель. Они хотят получить возможность развязать агрессивные информационные боевые действия и в то же время не желают появления мощных средств защиты, особенно таких, которые используются в коммерческих продуктах и которые умерили бы их пыл при ведении такого рода действий. А решения, которые они пытаются навязать коммерческим поставщикам и обществу в целом, сильно смахивают на известный сценарий, когда позиция государства выражена примерно так: "Мы обеспечим вам эффективные средства защиты, но в то же время хотим иметь возможность обходить эти средства или получать к ним доступ весьма удобным для нас способом”.

Маркус Ранум из компании "Information Works" (Балтимор, штат Мэриленд), разработчик брандмауэров, который создал "DEC SEAL", "NIS Gauntlet" и комплект для брандмауэра TIS ("FWTK"), не признает некоторых предпосылок рекламируемой информационной войны:

"Огромная масса материалов, посвященных информационной войне, высосана из пальца. Например, "информационная война", финансируемая террористами. Теоретически, иранские террористы (которые по ряду причин обогнали развитие технологии) собираются сокрушить Уолл Стрит. При этом абсолютно никто не понимает, чем именно угрожают террористы и какого рода средства они используют. Думаю, что если какой-то террорист захочет посеять панику на Уолл Стрит, он не станет это делать с помощью компьютеров, а выведет из строя электросеть. Если террорист намерен снести здание NASDAQ, то он заложит бомбу на торговом этаже, поскольку никто не оставит это событие без внимания: репортеры из CNN постараются усугубить драматизм ситуации. Терроризм - государственный или любительский - связан с самыми сенсационными, громкими и ужасающими разрушениями, чего не скажешь, по мнению большинства людей, о "тихих" компьютерных диверсиях. После сильного взрыва, среди клубов дыма, вряд ли кто заметит: "Ничего страшного, сломался один из трассировщиков". Крупные террористические акты последних лет, к сожалению, подтверждают такое мнение.

Сотрудники Института компьютерной безопасности, которым доверено стоять на страже целостности, конфиденциальности и доступности информационных систем около 500 корпораций, бесчисленного множества государственных органов и ведущих университетов убеждены, что информационная война в конечном счете нацелена на экономику в мировом масштабе. А потому особенно актуальны информационные действия оборонительного характера в современной глобальной экономике.

В марте президент Клинтон подписал распоряжение, которое устанавливает приоритетные направления в сборе информации. Создана рабочая группа, призванная периодически пересматривать как указанные приоритеты, так и сведения, подлежащие сбору в соответствии с ними. Экономический шпионаж оказался где-то посередине краткого списка приоритетных направлений Клинтона, занимая место после угрозы распространения ядерных вооружений, международных террористических организаций и региональных "горячих" точек, но перед здравоохранением и охраной окружающей среды.

К июлю источники из разведывательных органов уже успели доложить об успехах ЦРУ в экономическом шпионаже, включая информацию, позволившую добиться успеха на торговых переговорах с. Японией и другими странами. Если говорить о внутреннем фронте, то несколько историй, связанных с хищением патентованной информации и промышленных секретов, в конечном счете, попали на первые полосы крупнейших газет.

ФБР пришлось перерыть горы мусора, чтобы пресечь деятельность агентурной сети в Силиконовой долине, которая занималась хищением промышленных секретов у одной компании и их сбытом другой. В другом случае, бывший инженер компании "Локхид", работавший над совершенно секретным проектом "Скунс", был арестован при попытке продать секретную информацию в ходе операции, проведенной ФБР с подставным лицом.

### Человеческий фактор

Информация становится исключительно ценным товаром. Корпорациям придется в ближайшем будущем разработать политику оборонительных информационных боевых действий, или у них останется мало шансов выжить.

Общеизвестное практическое средство для оценки и снижения уровня риска содержит одиннадцать пунктов первоочередных оборонительных мероприятий:

* все сотрудники подписывают обязательство о неразглашении сведений в качестве условия приема на работу;
* сотрудникам ни под каким видом не разрешается приносить программные средства из дома или других внешних источников; им также не разрешается выносить компьютерные диски и другие магнитные носители с предприятия;
* существует и действует исходный план информационной безопасности, обеспеченный соответствующим персоналом и ресурсами;
* обучение всех работников мерам безопасности проводится как минимум раз в полгода;
* организация проводит квалифицированный анализ факторов риска и имеет план экстренного реагирования и план ликвидации последствий;
* все пользователи компьютерных систем имеют пароли, составленные методом случайной генерации, которые периодически меняются;
* все случаи нарушения безопасности тщательно расследуются и докладываются высшему руководству;
* проводится проверка предыдущей деятельности всех сотрудников;
* на каждом объекте существует программа контроля действий посетителей;
* существуют специальные методики при приеме на работу граждан других государств;
* безопасность каждого объекта проверяется каждые двенадцать месяцев.

Однако вряд ли карты контроля доступа и закрытая операционная система с несколькими уровнями безопасности способны выполнить свои защитные функции, если конкурент собирается пригласить на работу пятерых ваших ведущих сотрудников, и они намерены уволиться, прихватив с собой все, что имеется в их головах. Вот где истинная проблема. "Информационная война" подразумевает, что гораздо надежнее купить какого-либо человека и иметь непрерывный источник информации внутри, нежели пытаться выуживать секретную информацию в компьютерной системе той или иной компании, или даже "оседлать" ее линии связи и перехватывать информацию в момент передачи. Промышленный (и любой другой) шпионаж имеет множество аспектов - у него есть как электронное, так и человеческое лицо. И человеческий фактор зачастую представляет собой угрозу значительнее той, что может последовать от засылки "компьютерных ниндзя" по Internet в ваши компьютерные сети.

### Другие аспекты

По мере того, как разворачивается эта неизведанная впечатляющая картина компьютерных боевых действий, появляются новые проблемы. Вся наша концепция боевых действий и ведения войн основана на идее национального суверенитета. Отличительная особенность информационных боевых действий состоит в том, что они сметают эти барьеры. А какое право имеет Америка делать ту или иную страну банкротом? И при каких обстоятельствах должны использоваться такие полномочия? Мы только начинаем задавать себе эти вопросы, не говоря уже о том, чтобы найти ответы.

Помимо нравственных дилемм, вырисовываются более приземленные вопросы. По традиции, вооруженные силы разрабатывают и затем используют новые, вооружения и технологии. В то же время планами информационных войн заправляют, в настоящее время, гражданские специалисты. Впервые вооруженные силы оказались вынуждены сначала овладевать каждым новым открытием, а уже потом изыскивать пути их использования. "Мы всегда были тем паровозом, который тащил поезд, - сказал один из экспертов Пентагона по информационным войнам. - Сегодня ситуация такова, что поезд ушел, а мы на своей патрульной дрезине пытаемся его догнать".

В Великобритании, Америке и других государствах Запада все чаще слышны голоса, утверждающие, что развитые страны обязаны не допустить совершенствования новой формы ведения боевых действий, чтобы она впоследствии не стала достоянием деспотических режимов и террористов. Иначе любое государство может стать жертвой нападения, его коммуникации будут уничтожены, финансовая система расстроена, и при этом оно не сможет даже вычислить врага. Поскольку около 95% военных коммуникаций проходят по тем же сетям факсимильной и телефонной связи, которыми пользуются гражданские лица и военные базы питаются электроэнергией от тех же систем, что и городские компьютеры, постольку все страны оказываются под угрозой, причем самые развитые государства одновременно становятся и самыми уязвимыми.

### Сегодня

Одним из первых подразделений армии США, направленных в зону конфликта в бывшей Югославии, стал временно прикомандированный 72-й батальон войск связи. Его задача - организовать систему электронной почты с тем, чтобы солдаты могли поддерживать связь с домом, так как полагаться на письма и телефонные звонки - как способы общения с родными и близкими- не приходится.

Видимо, остальные подразделения со временем обзаведутся аналогичными системами.

Электронная почта представляет собой часть армейской военной сети, но и пользователи таких популярных оперативных услуг, как Соmpuserve и America On Line, также могут связываться с солдатами этого подразделения, если располагают правильным электронным адресом. Отлично, не правда ли? Но кто гарантирован от несанкционированной передачи ложного или провокационного сообщения в условиях информационной войны?

Чтобы общественность имела доступ к оперативной информации по Боснии, открыта страница в Internet - Bosnia Link. Новый боснийский абонентский узел предназначен для того, чтобы, во избежание информационного вакуума, обеспечить своевременной информацией репортеров, находящихся в "мертвой зоне" или в войсках.

Наблюдатели за использованием телекоммуникаций и гражданских свобод заявили, что Bosnia Link является положительным примером использования технологии правительством и свидетельством демократии. Начиная с 5 декабря, за первые 36 часов своей работы пункт Bosnia Link получил 45 500 информационных запросов от пользователей Internet со всего света. Какие страны направляют войска в Боснию, чтобы содействовать осуществлению плана мирного урегулирования на Балканах? Кто командует 60-тысячным контингентом НАТО? И почему министр обороны Уильям Перри думает, что эта рискованная операция служит национальным интересам США? Как обеспечены солдаты на случай холодной погоды?

Фанаты портативных компьютеров просто сияют от счастья, имея возможность бороздить WWW в поисках цветных карт Боснии, протоколов пресс-конференций с высшими командирами и списков танков М1-A1 и вертолетов-штурмовиков "Апач".

В то же время раздаются голоса, что кажущаяся более открытая позиция Пентагона на самом деле сводится к тому, что он обращается напрямую к общественности не только с объективными цифрами продовольствия и боеприпасов, но также и с субъективными политическими оценками и решениями без фильтра средств массовой информации, с аргументацией, сформулированной самим чиновником или его ведомством.

В недавнем прошлом Пентагон всячески препятствовал репортерам во время вторжений на Гренаду в 1983 году и в Панаму в 1989 году и пытался держать в узде представителей прессы во время войны в Персидском заливе в 1991 году. Теперь же Пентагон рассылает электронными средствами различные документы и репортерам и всем желающим. Любой пользователь Internet может получить любую интересующую его информацию.

### +В поисках рационального зерна

Исходя из всего вышеперечисленного я склоняюсь к мнению, что понятие "война" в настоящее время не не совсем подходит для, так как война это сложное общественно-политическое явление. Она представляет собой противоборство общественных систем, классов, наций, государств с применением вооруженного насилия для достижения политических целей. Думается, что пока не следует ожидать определения единого и четкого понятия "информационная война". "Информационное противоборство" или "информационная борьба" - являются вполне законными и выражают борьбу сторон за превосходство в количестве, качестве и скорости добывания, анализа и применения информации. Ясно, что этот вид противоборства также , как и другие его виды имеет две составляющие - оборонительную и наступательную или ударную. Оборонительная - защитить свою информацию от воздействия противника. Ударная - дезорганизовать или разрушить инфрмационную инфраструктуру противника, нарушить процесс оперативного управления его силами и средствами. Видимо для ударной составляющей информационного противоборства можно использовать и понятие "информационная интервенция" или "информационная агрессия". В связи с тем, что сейчас четко обозначено движение в сторону войн нового поколения, роль информационного противоборства резко возростает в следующих направлениях: в борьбе с системами управления; в навязывании противнику своих правил ведения военных действий; в ставке на военно-техническое превосходство. Вершиной информационного противоборства, по видимому, станет создание глобальной боевой информационно - ударной системы страны и вооруженных сил, способной контролировать состояние и функционирование вооруженных сил и группировок противника и снижать эффективность их применения. Сейчас информационное противоборство уже стало важнейшим содержанием войны, но из-за применяемых в нем сил и средств, а также специфических целей и задач прибретает как значительную самостоятельность, так и является неотъемлемым элементом всех остальных форм борьбы. Таким образом, под информационным противоборством следует понимать новую форму борьбы сторон в которой используются специальные способы и средства, воздействующие на информационную среду противника и защищающие собственную в интересах достижения стратегических целей войны.

По коридорам Пентагона гуляет такая шутка: "Информационная война - что это такое?" - "О, это компьютерная безопасность плюс деньги". Можно сказать еще, что информационная война - это компьютерная безопасность плюс взвешенное отношение. И это обнадеживает.

### Список литературы

Реферат подготовлен по публикациям в Интернет. В нем использованы материалы докладов Университета Национальной Обороны, Министерства Обороны США, Сената США, Администрации Президента США и информация из независимых источников.