Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 10 (101)/2001

Новые приоритеты в информационной безопасности США (стр. 2)

Проблемы России в условиях глобальной информатизации общества (стр. 11)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Новые приоритеты в информационной безопасности США

Александр ЛЕВАКОВ
профессор Академии военных наук

Трагические события, которые произошли в США 11 сентября 2001 года и повергли в шок весь мир, вновь напомнили человечеству об обратной стороне технического прогресса. Варварские террористические акты, совершенные группой террористов-смертников в Нью-Йорке и Вашингтоне, стали суровым испытанием не только для правительства и спецслужб, но и для всего американского общества. К своему удивлению мы узнали, что США — это далеко не самая безопасная и благополучная страна в мире, а американцы — это не только прагматики и бизнесмены, но и патриоты своей Родины, за которую они готовы отдать жизнь, как это сделали пассажиры Боинга под Питсбургом. Сейчас, когда на волне гнева и мести, буквально захлестнувшего США, Пентагон и ЦРУ пытаются взять реванш в схватке с невидимкой Бен Ладеном в горах Афганистана, на повестку дня вновь и вновь встает вопрос о безопасности информационных технологий.

Впрочем, почему только информационных: попробуйте назвать хоть одну сферу деятельности человека (связь, транспорт, авиация, космос, энергетика, водоснабжение, финансы, торговля, наука, образование, оборона, охрана общественного порядка, медицина и др.), где сейчас не применяются эти технологии и вы поймете, насколько зависимы мы все стали от битов, чипов, модемов... — одним словом всего того, что превращает нас помимо нашей воли из «homo sapiense» в «homo informaticus». Фактически во многих развитых странах сегодня активно реализуется концепция так называемого «электронного правительства». Можно поспорить о том, что далеко не все страны и народы приемлют новый «цифровой» порядок, что высокие технологии для многих просто недосягаемы и миллионы голодных людей вообще не знают о том, что есть сотовые телефоны, спутники, персональные компьютеры и Интернет, но факт остается фактом — человечество шагнуло в новое тысячелетие, имея в своих руках инструмент столь же созидательный как и разрушительный по своим возможностям одновременно.

Как установило ФБР, террористы-камикадзе готовились к своим ударам с помощью широко доступных программ, имитирующих полет самолета над Нью-Йорком и Вашингтоном, а для передачи инструкций в процессе подготовки и планирования террористической операции по захвату самолетов — электронную почту Интернет. Разрушение комплекса зданий только в Нью-Йорке, помимо человеческих жертв повлекло за собой закрытие биржи, падение курса акций, потерю десятка тысяч каналов передачи данных, перегрузку трафика в Интернет, уничтожение информации в компьютерах сотен фирм и офисов...

Для того, чтобы лучше осознать масштабы распространения информационных технологий в современном обществе, а следовательно и степень его технологической уязвимости обратимся к опыту США — стране, откуда к нам и пришли эти высокие технологии вместе с новыми проблемами. Американцы любят повторять, что они — нация эмигрантов, страна равных возможностей, где уснув бедняком можно проснуться миллионером. Количество желающих приехать на постоянное жительство в одну их самых богатых и развитых стран мира неуклонно возрастает из года в год, несмотря на все строгости американского законодательства, жестко регулирующего въездные квоты. США после распада СССР на протяжении последних десяти лет прочно занимают место государства-лидера со статусом мировой сверхдержавы. На земном шаре нет ни одного уголка, который не попадал бы в сферу американских национальных интересов.

Но вот парадокс — сегодня американцы вполне реально могут стать жертвами «кибернетического» Перл-Харбора, для подготовки и осуществления которого агрессору не понадобятся, как это было в прошлом, ни ракеты, ни самолеты, ни атомная бом-

ба. Буквально в считанные минуты страна может оказаться парализованной, а через несколько часов стать ареной ужасающих по своим последствиям беспорядкам среди населения, где в охваченной паникой еще недавно благополучной демократии стихийно начнут провозглашаться новые государственные образования, до боли знакомые нам по опыту Северного Кавказа. Что это — бред сумасшедшего, сюжет фантастического триллера или очередная журналистская утка? Это — сценарий Пентагона, американского военного ведомства, по коридорам которого вот уже 10 лет витает зловещая тень угрозы информационной войны, нависшей над Америкой после войны в Персидском заливе.

В ночь с 16-го на 17-ое января 1991 года, через сутки после истечения срока ультиматума ООН о выводе иракских войск с территории аннексированного 2 августа 1990 г. Кувейта, американские стратегические бомбардировщики и военные корабли нанесли удар крылатыми ракетами по военным объектам Ирака. Еще до подлета первых 50-ти крылатых ракет до целей группа армейских вертолетов внезапно на малой высоте атаковала и вывела из строя две главных иракских РЛС. Так началась операция многонациональных вооруженных сил по освобождению Кувейта «Буря в пустыне», которой суждено было войти в историю как война 21-го века.

За 43 дня боевых действий Ирак потерял 4000 танков (95%), 2140 орудий (69%), 1856 БТР (65%), 7 вертолетов (4%), 240 самолетов (30%), 143 корабля (87%). Потери коалиции составили соответственно: 4 танка (0,1%), 1 орудие (0,03%), 9 БТР (0,2%), 17 вертолетов (0,9%), 44 самолета (1,7%). Общее количество убитых со стороны 700000 союзных войск составило 148 человек (0,021%), из которых примерно 30% стали жертвами «огня по своим». Потери Ирака, армия которого насчитывала свыше полумиллиона человек, оцениваются в 9000 убитых (2%), 17000 раненых (3%) и 63000 пленных (12%). Свыше 150000 солдат (28%) дезертировали из иракской армии в ходе наземного наступления.

Но не пройдет и года после внушительно одержанной военной победы, еще будут полыхать факелы нефтяных скважин Кувейта, как в Пентагоне забьют тревогу: на смену эйфории придет отрезвление. Хорошо спланированная и блестяще проведенная военная операция с применением новейшего высокоточного оружия, самолетов-невидимок, приборов ночного видения, беспилотных самолетов-разведчиков, спутников и компьютеров могла окончиться полным провалом: военно-техническое превосходство победителя в одночасье превратилось в его ахиллесову пяту.

В секретной директиве Пентагона S-3600.1 появится совершенно новое и непривычное понятие — «информационная операция», которому суждено будет совершить подлинную революцию в военном деле. Как ни парадоксально, но в основу «информационной операции» против Ирака, как это уже официально записано в уставах и наставлениях вооруженных сил США, был положен классический прием ведения войны — дезорганизация управления. Исход поединка «Давида и Голиафа» решил внезапный удар в «голову» противника, потерявшего «зрение», «слух» и «речь» почти одновременно.

За несколько недель до начала ведения боевых действий специально обученные агенты ЦРУ с помощью портативных компьютеров в Багдаде внедрили программные «вирусы-закладки», которые в назначенный день и час отключили телефонные станции и радиолокационные посты, парализовав уже в первые минуты воздушного налета систему ПВО Ирака. Есть сведения, что истребители «Мираж» иракских ВВС по этой же причине не могли использовать свои бортовые РЛС в ходе отражения налета. Это позволило союзной авиации в первые несколько часов уничтожить основные объекты иракской системы ПВО и через 10 дней завоевать превосходство в воздухе.

Оружие возмездия — баллистические ракеты «Скад», которыми Ирак будет обстреливать Израиль и Саудовскую Аравию в ответ на прицельные авиационные налеты американцев, в большинстве случаев окажется малоэффективным против зенитных ракет «Патриот» и спутников системы раннего предупреждения. На угрозы Хуссейна применить химическое оружие президент Буш хладнокровно отдаст приказ о приведении стратегической ядерной триады США в полную боевую готовность. Весь мир, затаив дыхание, будет смотреть на экранах телевизоров прямые репортажи с театра военных действий.

По иронии судьбы «непобедимой» иракской армии в январе-феврале 1991 г. было суждено получить от НАТО урок немецкого блицкрига, за который Красная армия летом 1941 г. заплатила миллионами убитых, раненных и пленных солдат и офицеров. Жесткая централизация системы военного руководства Ирака, большинство объектов которой было сосредоточено в Багдаде, а закрытые правительственные линии связи проложены через автомобильные и железнодорожные мосты, оказала Хуссейну медвежью услугу. Союзники, используя авиационные бомбы с лазерным наведением и крылатые ракеты со спутниковой системой навигации, к началу наземного наступления разрушили практически все коммуникации иракских войск. Попытки отдавать приказы из Багдада с помощью посыльных мотоциклистов только усугубили положение иракской армии, которая за время воздушных налетов уже была фактически деморализована. Миллионы листовок, сброшенных на головы иракских солдат призывали их держаться подальше от своих танков, бронетранспортеров и орудий, как объектов поражения высокоточного оружия, эффективность которого уже не вызывала сомнения.

Что же так напугало генералов в Пентагоне, пребывавших в зените своей славы? Сегодня в США созданы самые оснащенные вооруженные силы в мире: около 3 млн. гражданских специалистов и военнослужащих, включая резервистов имеют в своем распоряжении вооружение, технику и имущество на общую сумму в 1000 млрд. $, на содержание которых выделяется свыше 300 млрд. $ в год.

Для ведения такого большого разбросанного по всему миру «хозяйства», доставляющего немало организационных, технических и чисто человеческих хлопот, американцы содержат внушительный арсенал информационных ресурсов: свыше 2 млн. компьютеров, 100000 локальных сетей и 10000 информационных систем.

Для вооруженных сил США, где на одного военнослужащего приходится один персональный или бортовой компьютер, а количество информационных систем, в которых эти компьютеры интегрированы для решения боевых задач в ходе военных действий, исчисляется десятками тысяч, сценарий 1991 года означал бы полный крах. Обрушенные на головы иракцев 60 тыс. тонн боеприпасов, из которых 10% составили высокоточное оружие, включая 323 крылатые ракеты, не достигли бы своих целей, если бы противник вывел из строя хотя бы одну из этих систем, например, навигации или тылового обеспечения. Если вспомнить, что во время американских бомбежек Югославии устаревшая информация ЦРУ привела к «точному» попаданию крылатой ракеты... в здание посольства КНР — нейтральной страны, обладающей ядерным оружием, то нетрудно представить возможные последствия замены всего нескольких байт в «ядерном чемоданчике» президента США.

Но это еще не все. В отличие от Ирака, где для управления войсками использовалось 60% гражданских линий связи, в США этот показатель достиг 95%, включая использование глобальной сети Интернет и спутников связи Интелсат. Известны случаи, когда недавние выпускники военных академий, корректировали огонь своих артиллерийских батарей, используя электронные карты Пентагона за тысячи миль от своих боевых позиций в пустыне. Для непрерывного, практически в течение каждого часа, уточнения данных воздушной и космической разведки, необходимо было задействовать сотни спутниковых каналов одновременно. Большинство пилотов после вылета на задание перенацеливались уже в ходе полета, поражая цели с ходу, что значительно снизило потери союзной авиации.

Общедоступность и высокая оперативность обновления информации о боевой обстановке, в сочетании с ее наглядностью и высокой достоверностью «единой цифровой картины поля боя», превращают информацию не только в мощное оружие, но и уязвимую цель для противника.

Планирование операций, разведка, навигация, связь, материально-техническое снабжение, инженерное оборудование, транспортировка грузов, медицинское обеспечение, финансирование и расквартирование войск, заказ вооружений и электронная торговля прочно обосновались в паутине компьютерных сетей, в которые то и дело заглядывают через Интернет любознательные хакеры, где им есть что посмотреть в секретных файлах американских военных.

Военный флот выходит в Интернет

Америка — крупнейшая военно-морская держава. Сегодня в боевом строю военного флота США находятся свыше 300 военных кораблей, 4000 самолетов и вертолетов. Общая численность ВМС и морской пехоты составляет примерно 900 тысяч военнослужащих и гражданского персонала, из которых 88 тыс (10%) находятся за пределами США. Годовой бюджет ВМС — это 90 млрд. $ или 30% всего военного бюджета Пентагона. Ежегодно военно-морское ведомство тратит около 1.6 млрд. $ на автоматизацию и информационные технологии.

Американские ВМС в тандеме с морской пехотой начинают грандиозную и беспрецедентную по своей стоимости и масштабу охвата программу создания глобальной информационной сети NMCI (Navy Marine Corps Intranet). По данным военно-морского ведомства США стоимость программы оценивается в 7 млрд. $. В ходе ее выполнения в период 2001-2008 гг. предполагается объединить около 100 разрозненных в настоящее время ведомственных информационных сетей и ликвидировать порядка 200 телекоммуникационных шлюзов, задействованных в системе оперативного планирования и боевого использования кораблей, авиации и подразделений морской пехоты США. Общее количество компьютеров (серверов, настольных рабочих станций, портативных и карманных компьютеров) может достичь 360 тысяч ед., при этом они будут разбросаны по всему земному шару на 300 военных базах (Аляска, Исландия, Пуэрто-Рико, Гуам, Окинава, Гавайи, Куба и др.), включая континентальную часть США.

Сама идея создания подобной сети появилась как результат обобщения опыта совместного боевого использования разнородных (авиационных, морских и сухопутных) смешанных группировок во-

оруженных сил в так называемых конфликтах низкой интенсивности (Косово, Сомали и др.). В итоге военно-морские силы в рамках концепции Пентагона по реформированию и автоматизации ВС «общее видение 2020» выдвинули свою инициативу — «информационные технологии 21-го века», одной из важнейших составляющих которой и является данная программа.

Создаваемая сеть объединит все потоки информации, передаваемые в направлении «корабль-берег» и «берег-корабль», за счет использования универсального мультимедийного интерфейса и технологии Интранет. Пользователи сети будут иметь выход на все важнейшие правительственные, военные и коммерческие информационные системы, что позволит им оперативно решать задачи не только в интересах планирования и проведения военных операций, но и в личных целях (заказ авиабилетов, оплата счетов, медицинская диагностика и др.).

Пехотинец 21-го века

По оценкам Пентагона в текущем десятилетии 50% всех боевых действий будут вестись в условиях городских застроек (населенных пунктах), а к 2025 г. этот показатель может достигнуть 75-80%. Мировой опыт вооруженных конфликтов низкой интенсивности (Ливан, Гренада, Сомали, Косово, Чечня) показывает, что ведение боя в населенных пунктах характеризуется высокими потерями, быстрой сменой обстановки, неустойчивостью связи, плохой видимостью, низкой эффективностью применения тяжелых вооружений (авиации, танков), затрудненным тыловым снабжением и медицинским обеспечением войск.

Вот почему сухопутные войска активно разворачивают работы по созданию собственного армейского тактического Интранета по программе WIN-T, в ходе которой американские солдаты получат не только новую экипировку со шлемом-дисплеем, компьютером, радиостанцией, датчиком космической системы навигации и автоматической винтовкой, позволяющей с помощью специального прицела-перископа стрелять из-за укрытия ночью и в тумане, но и уникальным доступом к информационным системам планирования и ведения боевых действий.

Подсистема личной связи CRS, сопряженная с портативным компьютером и индивидуальным датчиком глобальной навигационной системы GPS, должна максимально облегчить солдату в бою все его действия, связанные с ориентированием на местности, оценкой обстановки, ведением переговоров в звене отделение-взвод, передачей и получением видео изображений, опознаванием целей, ведением химической разведки, обнаружением мин и другими задачами. Вычислительная система состоит из двух компьютеров: ранцевого портативного и универсальной шины USB, которая обеспечивает обмен данными между основными подсистемами.

Для удобства пользования портативный компьютер оснащен индивидуально настраиваемой системой распознавания голоса. Связь солдата с его отделением в бою поддерживается с помощью двух радиостанций: индивидуальной типа Motorola (1755-1850 МГц) и общей, сопрягаемой с системой одноканальной цифровой связи «Sincgars» (30-88 МГц), что позволяет командиру в случае необходимости ставить ему задачи и получать от него донесения. Подсистема связи обеспечивает одновременный разговор трех абонентов и передачу данных (64 Кбит) в режиме засекречивания на расстоянии до 5 км. Для связи вне зоны видимости используется ретрансляция с автоматическим поиском ближайших радиостанций других пехотинцев или воздушных ретрансляторов (самолетов или вертолетов). Общий вес двух радиостанций составляет 656 г., а габариты — 14 см х 8 см х 2,5 см.

В качестве вычислительной платформы используется IBM совместимый портативный мультимедийный компьютер с упрощенной операционной системой Windows-2000, процессором Пентиум-75 Мгц, оперативной памятью 32 Мбайт, жестким диском объемом 340 Мбайт и сменной флэшпамятью 85 Мбайт, сетевой картой Ethernet. Для подключения периферийного оборудования в компьютере имеются шины PCI и ISA, с двумя разъемами RS-232. Общий вес портативного компьютера составляет около 1200 г, а габариты без внешних соединителей — 4 см х 18 см х 27 см. Диапазон рабочих температур от -15 до 49 град Цельсия. Предусмотрено несколько типовых вариантов установки вычислительной системы в зависимости от выполняемых боевых задач: для командира, солдата, инженера, разведчика, корректировщика огня. В командирском варианте предусмотрено подключения клавиатуры с трекболом и дисплеем VGA.

Общая стоимость программы «пехотинец» оценивается в 2 млрд. $, полномасштабная реализация которой предполагает поставку в войска в течение 2001-2010 гг. 34 тысяч комплектов. По оценкам Счетной палаты Конгресса США стоимость одного комплекта снаряжения оказалось завышенной от первоначальной более чем в 2,5 раза. В январе — феврале 2001 г. в шт. Калифорния были проведены первые полевые учения в ротном звене с использованием нового комплекта снаряжения пехотинца. В ходе учений за счет использования нового снаряжения условные потери противника возросли с 55% до 100%, а собственные потери снизились с 28% до 17%. По отзывам солдат снаряжение их вполне устраивает. Все электронные компоненты безотказно работали даже в воде. Каждый боец точно знал расположение своих товарищей и всегда мог выйти на связь.

Электронная торговля

Еще в мае 1998 г. в рамках широкомасштабной и долгосрочной инициативы по реформированию вооруженных сил Пентагон открыл новую программу по созданию единой системы электронной торговли EMALL, в рамках которой предполагается упорядочить процесс закупки вооружений и предметов материально-технического снабжения войск через Интернет. Для реализации этой программы в Агентстве материально-технического снабжения (тыла) ВС США DLA было создано управление электронной коммерции JECPO. Система электронной торговли создается по принципу Интернет-портала, который связывает сайты видов вооруженных сил и коммерческих фирм-производителей в интересах создания эффективной и безопасной торговли на основе рыночного механизма через прямую продажу-покупку, что обеспечит пользователям свободный доступ к предметам военных поставок посредством электронных каталогов и электронных биржевых операций.

За счет использования системы электронной торговли Пентагон предполагает сократить от 30 до 40 промежуточных этапов закупки вооружений, сведя их фактически до 10 он-лайн операций.

Например, в классической бумажной системе при закупке на сумму в 500$ только на административные расходы тратится от 150$ до 200$, в то время как в электронной системе эти расходы составят всего 2$. При этом сама процедура бумажного оформления заказа может занимать от 1 до 3 месяцев бюрократических согласований в различных инстанциях.

К основным преимуществам создаваемой системы электронной торговли EMALL можно отнести следующие: объединение системы электронной торговли с системами тылового снабжения и финансирования войск, все предметы снабжения будут постоянно находиться под контролем по мере их заказа, оплаты и поставок, устранение дублирования в заказах, централизованная регистрация покупателей и производителей, поиск по всем правительственным источникам информации, коммерческим каталогам и электронным торговым биржам, автоматический сбор статистики и формирование отчетов, эффективный маркетинг и реклама, стандартизация заказов вооружений, налаживание контактов и взаимопонимания между видами вооруженных сил в интересах снижения стоимости программ перевооружения и их реализации.

Однако, у электронной торговли есть и свои минусы, о которых следует помнить. Это, прежде всего, безопасность транзакций при проведении покупок и продаж через Интернет, где хаккеры чувствуют себя как рыба в воде.

В 1999 г. было отмечено всего около 22 тысяч попыток проникновения и снятия информации с систем Пентагона; за первые 11 месяцев 2000 г. количество таких попыток возросло до 26 500.

В целях обеспечения безопасности доступа к информационным ресурсам и секретным объектам Пентагон проводит полномасштабную замену личных номеров военного и гражданского персонала с использованием технологии пластиковых электронных карт — «smart-cards». Каждая такая карта стоимостью 6$ будет иметь микросхему с аппаратной реализацией криптографического алгоритма, индивидуальный магнитный и штрих код владельца. В период с 2000 по 2005 гг. ВМС как головная организация этой программы получит 145 млн. $ для закупки электронных карт, компьютеров, программного обеспечения и электронных замков для установки на 800 военных объектах по всему миру.

В 2000 г. в системе электронной торговли Пентагона было зафиксировано свыше 5 миллионов наименований товаров и услуг, которые были задействованы по операциям купли-продажи в общей сложности на сумму 80 млн. $. По предварительным оценкам в 2001 г. каталоги баз данных электронной торговли МО США должны расширится до 12 млн. наименований, а объем торговых сделок по военным программам должен достигнуть 143 млн. $. В настоящее время в этой системе зарегистрировано около 175 тыс фирм-производителей, заинтересованных в работе по военным контрактам. Для сравнения: в 2000 г. в общей сложности было сделано покупок через Интернент на сумму 33 млрд. $, в которых участвовали 20000 чел. При этом общие расходы из федерального бюджета на информационные технологии за этот же период составили 37.6 млрд. $.

Заказ вооружений

По оценкам Пентагона к 2005 г. свыше 120 тысяч (50%) госслужащих, занятых в программах приобретения (заказов, закупок и поставок) военной техники и имущества для вооруженных сил США, достигнут пенсионного возраста и могут быть уволены. Под угрозу будут поставлены сотни долгосрочных военных программ, от которых зависит не только национальная безопасность, но и экономика, а также благосостояние самой богатой нации в мире. Эта тревожная тенденция вынуждает американцев активно внедрять информационные технологии в военно-промышленном бизнесе.

Параллельно с развитием системы электронной торговли Пентагон активно внедряет передовые информационные технологии непосредственно в систему приобретения вооружений по военным контрактам, которых сегодня насчитывается до 332500 на общую сумму 852 млрд. $. За пять лет

было оборудовано свыше 20000 удаленных терминалов автоматизированной системы военных контрактов SPS. К 2003 г. система должна охватить 43000 пользователей в 1100 районах земного шара. По данным за 2000 г. Пентагон осуществил закупку на 32 млрд. $ товаров и услуг с помощью системы SPS. Когда система будет полностью развернута и интегрирована в сеть Интернет, американские военные расчитывают ежегодно экономить до 1.4 млрд. $ на закупках по военным контрактам.

Космическая фотосъемка

Не секрет, что основные функции современных космических аппаратов (спутников) связаны в основном с навигацией, метеорологией, связью и разведкой. Последняя является в настоящее время одним из приоритетных направлений в обеспечении информационного превосходства практически во всех сферах жизнедеятельности современного общества: военной, политической, научно-технической и экономической.

В ближайшие несколько лет предполагается перейти полностью на систему электронной торговли продуктами космической видовой разведки через Интернет.

Министерство обороны и разведывательное сообщество США в настоящее время начинают осуществлять широкомасштабные долгосрочные программы, направленные на полную замену их спутниковых арсеналов в ближайшие десять лет, стоимость которых оценивается в 60 млрд. долларов. Одновременно ставиться задача по увеличению окупаемости капиталовложений за счет реализации коммерческих проектов в этой области. После долгих колебаний Конгресс США санкционировал возможность коммерческого доступа к изображениям, получаемым со спутников IKONOS с разрешением в 1 м. Такая точность фотосъемки использовалась американскими военными во время войны в Персидском заливе для определения позиций иракских баллистических ракет. По некоторым оценкам Национальное агентство космической фотосъемки и картографии (NIMA) планирует получить от продажи своей продукции до 1 млрд. $ в год.

Для этого планируется создать распределенную базу данных с послойным отображением участков земной поверхности в цифровом формате, доступ к которой будет осуществляться на платной основе избирательно: каждый пользователь сможет увидеть только то, что ему можно будет увидеть без ущерба национальной безопасности США и их союзникам. Информация будет накапливаться не только за счет национальных, но и иностранных орбитальных ресурсов, что позволит иметь наиболее точное и полное представление об интересующих покупателя участках в различных спектрах (видимом, инфракрасном, ультрафиолетовом), ракурсах (черно-белом, цветном, двухмерном, трехмерном) и масштабах обзора (по углу, высоте и ширине полосы съемки). Эта же информация наряду с данными агентурной и радиоэлектронной разведки будет постоянно отслеживаться в базах данных разведывательного сообщества в интересах национальной безопасности.

Разведка

В США разведкой занимаются 14 спецслужб, входящих в так называемое разведывательное сообщество: ЦРУ, Разведуправление Министерства обороны (РУМО), Агентство национальной безопасности (АНБ), органы космической разведки Пентагона, разведуправления видов вооруженных сил, бюро разведки и исследований госдепартамента, занимающиеся разведывательной деятельностью подразделения министерств юстиции и финансов, а также Федеральное бюро расследований (ФБР).

Всего на нужды разведывательного сообщества из бюджета выделяется около 28 — 30 млрд. $. Большая часть этих средств идет на технические системы сбора, обработки и распределения информации.

Информационное превосходство при проведении информационных операций стало основной задачей разведки в 21-ом веке. Из опубликованных в открытой печати материалов следует, что многие вопросы реорганизации разведки касаются в основном информационных технологий.

Анализ боевых действий в Персидском заливе, в ходе которых широко использовалось высокоточное оружие, поставил на повестку дня вопрос об эффективности использования информации, добываемой разведывательным сообществом. Были проведены комплексные исследования по проблеме реформирования и реорганизации разведки, в которых участвовали свыше шести правительственных и частных научно-исследовательских организаций.

Разведывательное сообщество стало сильно зависеть от технических систем, используемых для сбора, обработки и распределения информации. В свою очередь новые технологии оказывают влияние на работу персонала и качество самих систем.

В силу того, что каждое шпионское ведомство США по соображениям безопасности создавало свои собственные системы сбора и распределения информации (АНБ — КРИТИКОМ, РУМО — ДЖЕЙВИКС, ДОДИИС, АМХС) с течением времени назрела острая необходимость в их объединении, и уже в начале 90-х годов была поставлена задача создать в ИНТЕРНЕТ невидимый для большинства пользователей специальный закрытый или как его еще называют секретный ИНТЕРНЕТ.

Хотя в этой секретной сети, получившей название ИНТЕЛИНК, также используется традиционный протокол TCP/IP, непосредственный доступ к секретной информации осуществляется через специальный протокол HTTPS при наличии специального броузера с набором криптографических алгоритмов, поставляемого только для зарегистрированных пользователей ИНТЕЛИНК.

Сеть ИНТЕЛИНК имеет четыре уровня доступа к разведывательной информации по степени секретности: первый уровень представляет особо важная информация для принятия политических решений, которую готовит и распределяет только ЦРУ через специальную сеть ПОЛИСИНЕТ для президента и Совета безопасности; второй — информация, имеющая гриф совершенно секретно, к которой имеют доступ около 50 тыс. пользователей, среди которых в свое время была и Моника Левински, когда она работала в Пентагоне; третий — секретная информация, связанная с планированием военных операций, к которой имеют доступ 265 тыс. пользователей сети СИПРНЕТ; четвертый — несекретная информация из открытых источников (печать, ИНТЕРНЕТ, телевидение, радио), которая составляет свыше 95% всей добываемой разведкой информации.

Как считают американские специалисты пользователи разведывательной информации ожидают, что они смогут получать информацию непосредственно по своему запросу, предпочитая иметь прямые контакты с источником информации.

В случае, если такой контакт невозможен, пользователь должен знать как его информация собирается для того, чтобы оценить ее достоверность.

В настоящее время уже ведутся работы по созданию соответствующей «виртуальной аналитической среды» в рамках разведывательного сообщества, которая соединит в одно целое тех, кто собирает, распределяет, анализирует и потребляет информацию в целях повышения производительности и отдачи каждого аналитика. В рамках «виртуального аналитического сообщества», все участники которого будут интегрированы в единую информационную систему предполагается повысить требования к стандартизации информационных технологий, включая создание единого органа закупок и механизма регулирования бюджета для модернизации систем в течение всего жизненного цикла.

Борьба со шпионажем и терроризмом

Арест высокопоставленного офицера ФБР Роберта Хансена, обвиняемого в сотрудничестве с КГБ/СВР с 1986 г., вызвал самый настоящий шок в разведывательном сообществе США, где еще не успели забыть скандального разоблачения офицера ЦРУ Олдрича Эймса в 1994 г. В деле Хансена, пожалуй впервые в мировой практике шпионажа, можно говорить о прецеденте: «крота вычислил» компьютер. Роберта Хансена без всякого преувеличения можно назвать шпионом 21-го века, который не просто использовал современные информационные технологии, но делал это виртуозно, как настоящий профессионал.

Из представленного ФБР обвинительного заключения следует, что в своей шпионской деятельности Хансен, практически избегал прямых контактов с сотрудниками российской разведки, используя для оперативной связи флэш-карты, дискеты, карманный органайзер Palm Pilot, беспроводный удаленный доступ в Интернет и криптографические программы. Как установили следователи, Хансен постоянно набирал в графе поиска специальной базы данных ФБР не только собственное имя, но и такие ключевые слова, как «Россия», «КГБ», «шпионский тайник», а также свои кодовые обозначения для связи, чтобы установить, не попал ли он под подозрение. Все запросы, которые периодически делал Хансен, компьютер неумолимо записывал в специальный журнал, по которому его в конце концов и «расшифровали» сотрудники ФБР.

В настоящее время ФБР совместно с АНБ ведут работы по созданию системы контроля за электронной почтой в Интернет.

На программу технического перевооружения АНБ «GroundBreaker» Конгресс выделил свыше 5 млрд. $ и еще около 1 млрд. $ дополнительно на переоснащение многоцелевой атомной подводной лодки класса «Sea wolf» для прослушивания подводных кабелей связи с помощью специальной аппаратуры. Названная в честь президента США новая субмарина SSN-23 должна была быть спущена в воду в декабре этого года, но по настоянию АНБ было принято решение повести ее переоборудование, а спуск лодки отложить до июня 2004 года. По сведениям, просочившимся в печать, после ввода в строй новой субмарины АНБ рассчитывает прослушивать не только обычные электрические кабели связи, что оно делало и раньше, но и ... волоконно-оптические! Как это удастся сделать американцам — пока не ясно: для бесконтактного перехвата экранированного светового луча еще не придуман способ. Между тем, подводная лодка-шпион будет нести на своем борту специальный контейнер-камеру, из которой может быть осуществлен беспрепятственный доступ к любым подводным объектам.

Рожденный в кабинетах американского военного ведомства таинственный призрак-невидимка информационной войны за десять лет своего виртуального существования уже успел породить не мало проблем для тех, кто его создал. Сегодня без всякого преувеличения можно утверждать, что главная из них — защита информации. По оценкам ЦРУ не ме-

нее 100 стран располагают в той или иной мере возможностями ведения информационной войны, при этом доля компьютерных вирусов в Интернете, разрушающих информацию и ее носители выросла до 30%. Однако, завеса глубокой тайны и строгой секретности, первоначально опущенная Пентагоном над собственными планами информационных операций, создала явную диспропорцию между желаемым и достигнутым. Для страны, все сферы жизнедеятельности которой столь прочно связаны с информационными технологиями, грань между государственными и коммерческими, военными и гражданскими системами более чем условна.

Ежегодно США расходуют на информационные технологии только из федерального бюджета порядка 38 млрд. $, из которых около 20 млрд. $ (более 50%) составляют расходы военного ведомства. И это без учета десятков млрд. $, затрачиваемых на бортовые системы управления спутников, ракет, самолетов, танков и кораблей. Сегодня Пентагон это не только один из крупнейших владельцев, арендаторов и пользователей информационных и телекоммуникационных ресурсов, ведущих заказчиков программного обеспечения, компьютерного оборудования и средств цифровой связи, но и, по сути дела, законодатель государственной политики и промышленных стандартов в области информационной безопасности. Только в 2000 г. на защиту национальных информационных ресурсов в США было выделено 1,5 млрд. $, в то время как Пентагон истратил на защиту военных информационных систем 1,1 млрд. $.

В определенной степени это сказывается и на самих понятиях, связанных с защитой информации, которые постепенно трансформируясь из чисто военных терминов приобретают характер общегосударственных и промышленных стандартов. Производители оборудования и разработчики программных продуктов, заинтересованные в крупных государственных и военных заказах, начинают прислушиваться к тому, что говорят в коридорах Пентагона об информационной безопасности.

Осознав на собственном опыте бессмысленность защиты информационных ресурсов без участия всех заинтересованных сторон, каковыми в США являются фактически не только все государственные структуры, промышленность, частный капитал, но и рядовые граждане, военное ведомство в буквальном смысле пошло в народ, активно пропагандируя свое видение общенациональной проблемы №1. Одним из примеров такого новаторского подхода является программа DIAP (Defense Information Assurance Program), в рамках которой с участием таких ведущих фирм как Lucent Technologies, IBM, Microsoft, Intel, Cisco, Entrust, HP, Sun, GTE, Bay Networks, Axent, Network Associates, Motorola закладывается фундамент информационной безопасности не только военной инфраструктуры, но и всего американского общества в целом на ближайшие 10 лет.

Когда в декабре 1996 г. в одной из секретных директив американские военные ввели в обращение новый термин — «гарантия информации» (IA — information assurance), на это мало кто обратил внимание, учитывая первоначально ограниченный круг лиц, допущенных к документу. Однако, лингвистическая причуда Пентагона имела далеко идущие последствия, с которыми сегодня вынуждено считаться все большее число пользователей и производителей высоких технологий.

В соответствии с секретной директивой Пентагона S-3600.1 гарантия информации определяется как «информационная операция или операции, связанные с защитой информации и информационных систем за счет обеспечения их готовности (доступности), целостности, аутентичности, конфиденциальности и непротиворечивости.

Данные операции включают в себя восстановление информационных систем за счет объединения возможностей защиты, обнаружения и реагирования. При этом информация не будет раскрыта лицам, процессам или устройствам, не имеющим к ней прав доступа, будет обеспечена полная достоверность факта передачи, наличия самого сообщения и его отправителя, а также проверка прав на получение отдельных категорий информации, данные остаются в исходном виде и не могут быть случайно или преднамеренно изменены или уничтожены, будет обеспечен своевременный и надежный (по требованию) доступ к данным и информационным службам установленных пользователей, а отправитель данных получит уведомление факта доставки, также как получатель — подтверждение личности отправителя, и таким образом никто не сможет отрицать своего участия в обработке данных.»

Тем самым классическое понятие информационной безопасности (INFOSEC — information security) как состояние информационных ресурсов было расширено и дополнено гарантированием их надлежащего использования даже в том случае, если эти ресурсы будут подвергнуты деструктивному воздействию как извне, так и изнутри.

В политике информационной безопасности четко обозначился сдвиг в сторону активных организационно-технических мероприятий защиты информационных ресурсов.

Похоже, что американцы взяли за основу пропаганды знаний в области информационной безопасности советскую систему гражданской обороны 60-х, 70-х годов, когда население учили не только тому как надевать индивидуальные средства защиты и укрываться в бомбоубежищах, но и как вести радиационный, химический и бактериологический контроль и

восстанавливать объекты народного хозяйства после применения оружия массового поражения.

Заметим, что это не единственное нововведение Пентагона в лексиконе информационных технологий, которое стало достоянием общественности не смотря на гриф секретности первоисточника. К числу таковых можно отнести следующие: «информационное противоборство», «информационное превосходство», «информационные операции (общие и специальные)», «информационная среда», «атака на компьютерные сети», «вторжение в информационные системы» и др. С некоторых пор американское военное ведомство считает полезным публиковать отдельные несекретные фрагменты из своих засекреченных официальных нормативных документов (директив, инструкций, меморандумов, уставов и наставлений), повышая информированность общества о потенциальных угрозах национальной безопасности. Военные терпеливо и настойчиво приучают все слои населения к своей терминологии, постепенно стирая грань между государством и обществом, обороной и производством, разведкой и предпринимательством, учебой и досугом.

Как результат, американское общество начинает пожинать плоды информационной революции в виде единых универсальных стандартов, применимых как в гражданском, так и в военном секторе. В качестве примера можно привести стандарт электронной подписи (PKI — public key infrastructure) X.509, разработанный Агентством национальной безопасности для применения не только в военных, но и гражданских информационных сетях и системах. В соответствии с принятым стандартом в США к 2003 г. будут выдаваться пять классов сертификата PKI, гарантирующих информационную безопасность на основе криптографических алгоритмов с открытым ключом в зависимости от степени секретности информации. Каждый сертификат будет включать такие сведения как разновидность класса, порядковый номер, криптографический алгоритм инстанции выдавшей сертификат, наименование инстанции, срок действия (до 10 лет), ключ (до 1024 бит), цифровую подпись и др. К концу 2001 г. Пентагон должен полностью перевести свою электронную почту на стандарт PKI.

Профессиональная подготовка персонала в соответствии с новыми требованиями в области информационной безопасности является ключевым направлением реализации программы DIAP, в рамках которой на учебный процесс выделяется в общей сложности около 80 млн. $ на период до 2005 г.. При этом предполагается открыть специализированные курсы дистанционного обучения (свыше 20) в так называемом «виртуальном университете информационной безопасности» на базе сайтов в Интернете, в которых будут обучаться основам «стратегии глубокой эшелонированной защиты информационных ресурсов» администраторы (2 недели) и специалисты (3-5 дней) практически из всех федеральных ведомств, включая ЦРУ, ФБР, НАСА, Минфина, Минюста, Минэнерго и др.

Ожидается, что за 5 лет будет подготовлено в общей сложности не менее 100 тыс. дипломированных специалистов в области информационной безопасности, готовых к любым неожиданностям в киберпространстве.

В каждом штате на период чрезвычайных условий (землетрясений, ураганов, катастроф, террористических актов) создаются так называемые резервные центры обработки информации, в которых периодически собирается, накапливается и обновляется наиболее важная информация, необходимая для организации управления всех жизненно-важных служб (полиции, скорой помощи, пожарной охраны и др.) в случае выхода из строя основных центров обработки информации и телекоммуникационных систем. Как правило, такие центры оснащаются атомными источниками энергоснабжения (дизель-генераторами), способными поддержать нормальный режим функционирования резервных информационных центров в течение нескольких суток до восстановления стационарной системы энергоснабжения. В повседневных условиях работу таких центров обеспечивает ограниченный по численности технический персонал, имеющий все необходимые навыки для организации работы центра в чрезвычайных условиях.

Краткий обзор только некоторых наиболее важных и дорогостоящих программ развития информационных технологий в США на примере Пентагона показывает, что проблема информационной безопасности отдельно взятого ведомства по своему масштабу уже давно является общенациональной и для своего решения требует пересмотра устоявшихся подходов, принятия единых стандартов, как в промышленности, так и в бизнесе, создания национальной системы подготовки специалистов соответствующего профиля, широкого информирования населения об угрозах и мерах по их предотвращению.

Проблемы России в условиях глобальной информатизации общества

Вторая половина прошлого столетия ознаменована глобальным феноменом информационного взрыва. Развитие различных электронных технологий обеспечило миллионам людей возможность быстрого доступа к громадным информационным ресурсам, рассредоточенным по всей планете, возможность обмена информацией друг с другом и возможность одновременной работы с информацией, представленной в различных формах (текст, графика, видеоизображение, звук и т.д.).

Все это позволяет сделать вывод о том, что человечество (по крайней мере, передовые развитые страны) стремительно движется к такой стадии своего развития, которую принято называть информационным обществом.

Глобальные информационные системы и сети, в том числе и Интернет, являются важнейшим фактором ускорения мирового прогресса, технологической основой международного информационного обмена. Более того, на них ложится колоссальная экономическая нагрузка, которая возрастает на наших глазах буквально в геометрической прогрессии. В этих условиях информационные ресурсы представляют собой огромную материальную ценность, а несанкционированный доступ к этим ресурсам, если они недостаточно защищены, может привести к катастрофам или, в условиях конкуренции корпораций, фирм и целых государств, может радикально изменить ситуацию в пользу получившего такой доступ.

Развитие информационных технологий во всем мире и, естественно, в нашей стране проходит в условиях действия двух противоречивых, но взаимосвязанных факторов.

Первый — это нарастание попыток несанкционированного доступа к информации в целях ее получения, подделки, копирования либо уничтожения, иного использования в ущерб законному владельцу. При этом интеллектуальная и техническая оснащенность злоумышленников непрерывно возрастает и практически никогда не отстает от возможностей создателей и владельцев информационных ресурсов, подвергающихся таким атакам.

Второй фактор, действующий на развитие информационных технологий — это меры и усилия, принимаемые владельцами информационных ресурсов по созданию и внедрению надежных мер их защиты.

Несмотря на имеющиеся экономические, финансовые, а где-то и политические трудности, Россия не должна стоять в стороне от процесса движения к информационному обществу, а, наоборот, должна активно в нем участвовать.

Для того, чтобы сформировать представление о возможностях участия России в современной информационной экономике, необходимо определить ее место в процессе мирового информационно-технологического развития.

Если объективно оценивать путь, пройденный нашей страной в этом направлении, а также ее современное состояние, можно сказать, что созданы достаточно перспективные материально-технические условия и интеллектуально кадровые предпосылки для развития российского общества. Во всем мире очень высоко оцениваются российские научные исследования, а интеллектуально-творческий потенциал фундаментальной науки сопоставим только с потенциалом США. Технологические достижения ряда наукоемких отраслей России нередко служат основой международного сотрудничества страны на стратегически важных направлениях мирового прогресса. Большое количество квалифицированных российских специалистов приглашается зарубежными компаниями для участия в масштабных проектах. Известны многочисленные факты патентования результатов российских разработок иностранными компаниями.

Интеллектуальные ресурсы России могут и должны стать главным фактором технологической модернизации страны, должны обеспечить ее достойное участие в процессах глобализации мировой экономики.

В последнее время ведется активное обсуждение вопросов развития отечественного производства в информационно-коммуникационной сфере. Связано это с его большой стратегической важностью для страны, а также с наличием национально-государственных соображений информационной безопасности.

При решении проблем развития отечественного производства в сфере информационных технологий следует адекватно оценивать ситуацию и правильно определять основные направления ее развития. Ставка на технологические достижения и недооценка роли человеческого капитала вряд ли может служить надежной платформой для формирования и развития отечественного производства информационно-коммуникационной продукции.

Именно поэтому возникает необходимость организовать отечественное производство таким образом, чтобы создать единую корпоративную среду для успешного взаимодействия управленческих решений и информационных ресурсов, а также организации оперативного обмена информацией. Прин-

ципиально важное значение имеет наработка опыта интеллектуального применения импортируемой техники, вместо использования столь часто встречающихся технологий «на коленях».

Немаловажное значение имеет постепенное расширение спектра неэкономических целей, усиление информационного и социального взаимодействия компаний с другими институтами общества.

Человеческий фактор начинает занимать одно из важнейших мест, становится основой благополучного развития современных компаний. Сказанное выше справедливо и по отношению к России в целом, что выражается в проблеме «утечки умов» за рубеж.

Необходимо признать, что информатизация России, насыщение страны новыми информационными технологиями и повсеместное их использование не обеспечено в достаточной степени законодательной базой.

Современное состояние обеспечения информационной безопасности характеризуется недостаточной согласованностью используемых правовых механизмов, недостаточной эффективностью, а подчас и противоречивостью правовых норм. Ряд аспектов информационной безопасности не получил адекватного отражения в законодательстве России.

Следует учитывать также тот факт, что информационно-технологическая и структурная отсталость России в области вовлечения ценных знаний и информационных ресурсов в хозяйственный оборот, осложняет взаимоотношения созидательно-творческого слоя российского общества с государством. Российские органы государственного управления и крупные национальные компании пока не готовы рационально взаимодействовать с субъектами интеллектуальной экономики и эффективно применять импортируемые информационные технологии.

Причина отставания России проявляется еще и в неспособности государственного руководства и лидирующих политических и социальных сил оперативно и адекватно реагировать на все изменения, происходящие в индустриальном мире, непонимании сущности информационной экономики и ее производительных сил, с отставанием в проведении реорганизации управления на всех уровнях власти.

Решение этих вопросов возможно только в случае преодоления сопротивления влиятельных сил, использующих в своих интересах технологическую отсталость России и очень низкую цену интеллектуальной продукции отечественных научно-технических кадров. К сожалению, до сих пор в России материальные ресурсы имеют преобладающее значение над интеллектуальными — имеется в виду ценность интеллектуального продукта как самостоятельного объекта хозяйственного оборота. Важным препятствием остается тяга чиновничества к запретительным процедурам.

Особо следует отметить и низкий уровень информационной безопасности ресурсов. Как следует из статистики, в 2000 году в России в 4 раза выросло число преступлений в сфере компьютерной информации.

В 2000 году по фактам преступлений в сфере компьютерной информации в России было возбуждено 436 уголовных дел, что в четыре раза больше, чем в 1999 году, сообщил в интервью ИТАР-ТАСС первый заместитель начальника Управления по борьбе с преступлениями в сфере высоких технологий МВД РФ Виктор Кудинов.

По данным МВД, в прошлом году в целом число выявленных преступлений в сфере высоких технологий возросло в 2,3 раза — по ним было возбуждено 1900 уголовных дел, а в 1999 году — 852 уголовных дела.

По оценке экспертов, за последние три года число ежегодно регистрируемых преступлений в этой сфере выросло в 20 раз. Только в первом квартале 2000 года было зафиксировано около 200 попыток компьютерного взлома, в том числе баз и банков данных различных государственных организаций и правоохранительных органов. Вместе с тем, по оценке начальника Национального бюро Интерпола в РФ Владимира Гордиенко, пока компьютерная преступность для России не стала такой острой проблемой, как для западных стран.

Реальная угроза национальным интересам России связана сегодня и с опасностью утраты ею своей субъективности в мировом техническом процессе и переход в ранг одной из «отстающих» стран.

Критичным фактором информатизации и распространения пространственного влияния участников глобального информационного пространства является время. Его бессмысленная растрата чревата угрозой полной потери конкурентоспособности российских компаний и национальной экономики по всем направлениям.

России необходимо сконцентрировать усилия на активизации использования своего интеллектуального и культурного потенциала для того, чтобы занять достойное место в общемировом информационном пространстве.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Антонов А.Н. *(silver@jet.msk.su)*
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su
http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555