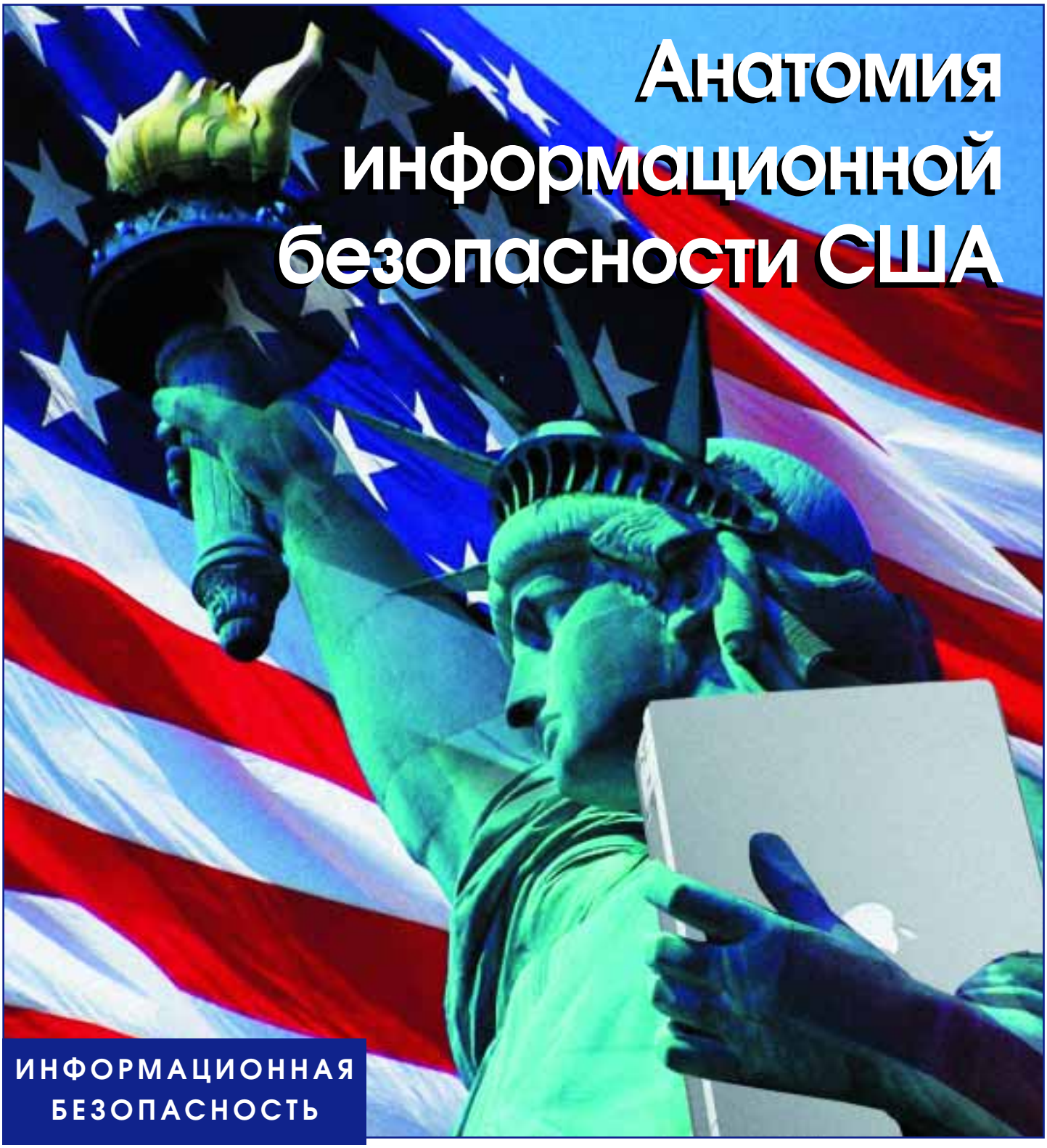
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 6 (109)/2002



Анатомия информационной безопасности США

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

АНАТОМИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ США

кандидат технических наук
Александр Леваков

СОДЕРЖАНИЕ

Об авторе: окончил факультет АСУ и ЭВМ Военной академии им. Петра Великого, кандидат технических наук, профессор, длительное время работал в Центральном институте научно-технической информации, специалист в области компьютерного моделирования, публиковался в Красной звезде, Независимой газете, Известиях и др. изданиях. Его обучающие программы в области криптографии пользуются популярностью в англоязычном Интернете у поклонников языка Visual Basic (www.freevbcode.com, www.vbexplore.com и др.).

Лучше гор могут быть только горы,
На которых никто не бывал

В.Высоцкий

Информационная безопасность сегодня, как самостоятельное направление современных технологий, без тени преувеличения переживает свое второе рождение. Особенность нынешнего этапа развития не только информационных, но и практически всех технологий характеризуется необычайно высокой степенью их интеграции во всех сферах человеческой деятельности и обусловленной этим обстоятельством взаимозависимостью и потенциальной уязвимостью, техногенной опасностью. Потоки информации, связанные с производством, закупкой и продажей товаров, предоставлением и оказанием услуг, банковскими и финансовыми операциями, нормативно-правовой и законодательной деятельностью, постоянно нарастают. По некоторым оценкам суммарная стоимость ежедневных финансовых транзакций в Интернете к концу этого года достигнет отметки $2,8 млрд.[1] На наших глазах глобализация становится определяющим фактором существования и выживания современной цивилизации. Мир подошел к той черте, когда границы между государствами перестали быть непреодолимыми барьерами не только для бизнеса и торговли, науки и образования, отдыха и развлечений, но и для терроризма, преступности и наркомании. События 11 сентября 2001 г., их военно-политические, экономические, общественно-социальные и научно-технические последствия, свидетелями которых являемся все мы, подтверждают это.

В этой связи опыт США, страны с одной из наиболее развитой в мире информационной и телекоммуникационной инфраструктурой представляется весьма интересным и поучительным с точки зрения анализа тенденций в государственной, бюджетной, инвестиционной, научно-технической и кадровой политике решения комплекса проблем, связанных с обеспечением информационной безопасности национальной инфраструктуры.

Организационно-штатные мероприятия в правительстве США после 11 сентября

8 октября 2001 г., через месяц после трагических событий, связанных с террористическими актами в США, президент Буш подписал указ №13228 о создании Управления внутренней безопасности УВБ (Office of Homeland Security) и Совета по вопросам внутренней безопасности при президенте (Homeland Security Council) во главе с губернатором Томом Риджем. В правительстве стало одним чиновником больше, а в разведывательном сообществе появился прообраз новой спецслужбы со специфическими задачами - гражданской обороной населения, инфраструктуры и киберпространства.

Буквально следом по горячим следам вышел еще один указ президента за №13231, специально посвященный вопросам информационной безопасности страны — «Защита критической инфраструктуры в информационный век». В соответствии с этим указом был создан Комитет при президенте по вопросам защиты критической инфраструктуры во главе с председателем Ричардом Кларком, выполняющим одновременно функции специального советника президента по вопросам безопасности кибернетического пространства.

Основная функция комитета заключается в координации всех федеральных программ в области информационной безопасности независимо от их ведомственной принадлежности. При этом Бюджетное управление при президенте (Office of Management and Budget) осуществляет жесткий контроль за эффективностью использования ассигнований, выделяемых Конгрессом на программы в области развития информационных технологий (ИТ) и обеспечения информационной безопасности (ИБ) всех министерств и ведомств США.

Заметим, что для экспертов эти кадровые перестановки, впрочем как и появление нового управления, не стали сенсацией и откровением, поскольку многое было предвосхищено еще задолго до событий 11 сентября[2]. Есть все основания полагать, что это не последние изменения в составе правительства США, где всерьез рассматривают возможность объединения таможенной и миграционной служб вместе с патрульной полицией и береговой охраной в одну спецслужбу по охране границ, прозрачность которых сегодня беспокоит амери-

[1] Towards a National Strategy. Government Computer News, 29 March 2002 г.
[2] Гражданская оборона информационных ресурсов. Известия №95 (25933) от 31.05.2001 г.
[3] Border agency overhaul proves tricky for Bush team. Government Executive Magazine, 29 March 2002 г.

канцев не меньше, чем баллистические ракеты КНДР и Ирака[3].

В целом вся эта организационная триада призвана обеспечить постоянный надзор со стороны исполнительной ветви власти за ходом реализации так называемой концепции «электронного правительства» (e-government), призванной не только сократить нарастающий бумажный поток документов, широко информировать граждан о деятельности правительства, сделав их, насколько это возможно, непосредственными участниками этого процесса, но и обеспечить бесперебойную и эффективную работу всех государственных структур, в том числе и в условиях чрезвычайного положения. Последнее обстоятельство выводит вопросы информационной безопасности на первое место среди приоритетных направлений совершенствования всей системы национальной безопасности США.

Как известно, в январе 2000 г. в соответствии с подписанным президентом Клинтоном так назы-

[4] В США принят план защиты информационных систем. Jet Info, №8 (87), 2000 г.

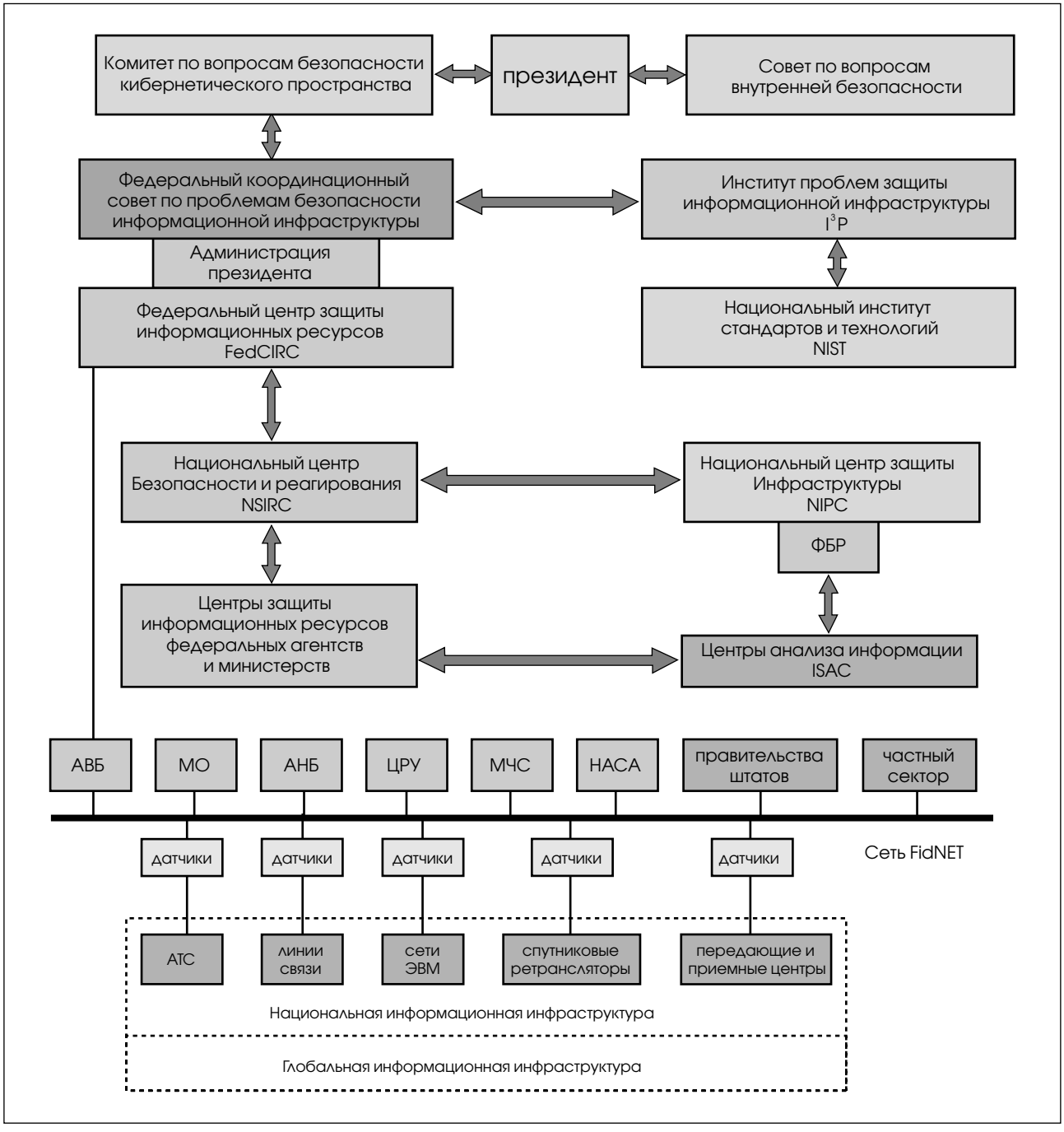


Рис. 1. Структура управления безопасностью национальных информационных ресурсов США

ваемым «Национальным планом защиты информационных систем»[4] на 2000-2003 гг. были созданы Совет по безопасности национальной инфраструктуры (NIAC) и специальные центры компьютерной и информационной безопасности: в Пентагоне — Объединенный центр защиты сетей (JTF-CND), в ФБР — Национальный центр защиты инфраструктуры (NIPC), а также Национальный и Федеральный центры реагирования на компьютерные происшествия (NSIRC, FedCIRC), которые с помощью специальной федеральной сети обнаружения вторжения (FIDNet) должны оповещать правительственные, промышленные, коммерческие и общественные организации об угрозе информационного нападения на США (рис 1).

Не случайно один из воздушных ударов террористов 11 сентября 2001 г. был нанесен именно по зданию Пентагона, в результате которого в течение нескольких часов была нарушена работа так называемого Объединенного антитеррористического центра всех силовых министерств и ведомств США.

Вот почему президент Буш в соответствие с установленным Законом о национальной безопасности регламентом ввел чрезвычайное положение в стране и, заняв свое место как верховный главнокомандующий вооруженными силами на борту поднятого в воздух самолета ВВС №1, лично руководил действиями силовых министерств и ведомств по подготовке к отражению возможных последующих ударов террористов, развертыванием резервной системы государственного и военного управления в стране и приведением в полную боевую готовность стратегической ядерной триады.

В то время как президент Буш-младший находился в воздухе, его ближайший заместитель — вице-президент Дик Чейни (бывший министр обороны во время правления Буша-старшего) занял свое автоматизированное рабочее место по боевой готовности №1 в подземном шестиэтажном комплексе федерального правительства в Форт-Ритци, оснащенном автономной системой жизнеобеспечения, системами связи и всем необходимым для

длительного управления вооруженными силами и страной на случай ядерной войны.

В эти трагические часы военно-политическое руководство США впервые после нападения Японии на Перл-Харбор в 1941 г. и Карибского кризиса 1962 г. сдавало самый настоящий экзамен на действия в условиях военного положения в стране, подвергшейся прямой вооруженной агрессии, и, надо отдать ему должное, выдержало это испытание до конца. Интересно, что все американские газеты в эти дни были полны гневных и обличительных тирад по поводу «растерянности президента», «улетевшего на самолете в неизвестном направлении» и «трусливо петлявшего как заяц», а все симпатии журналистов были на стороне мэра Нью-Йорка Джулиани, руководившего спасательными работами.

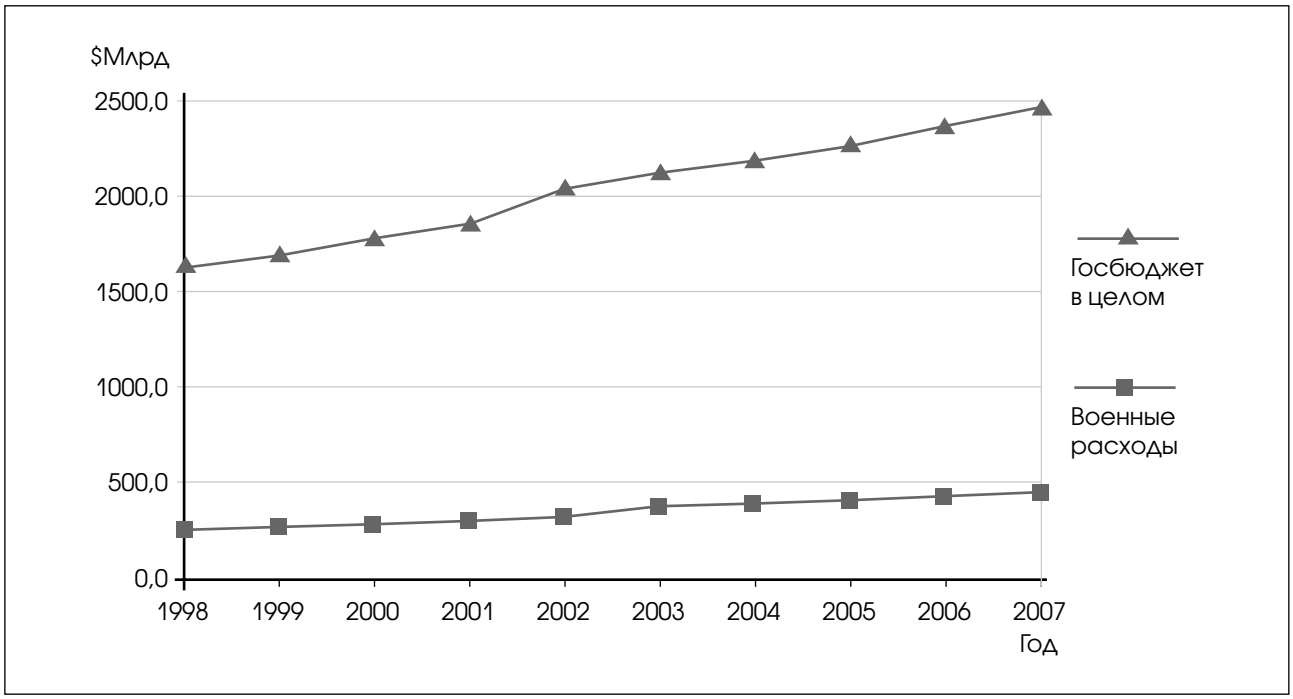


Рис. 2. Динамика роста государственного бюджета и военных расходов США

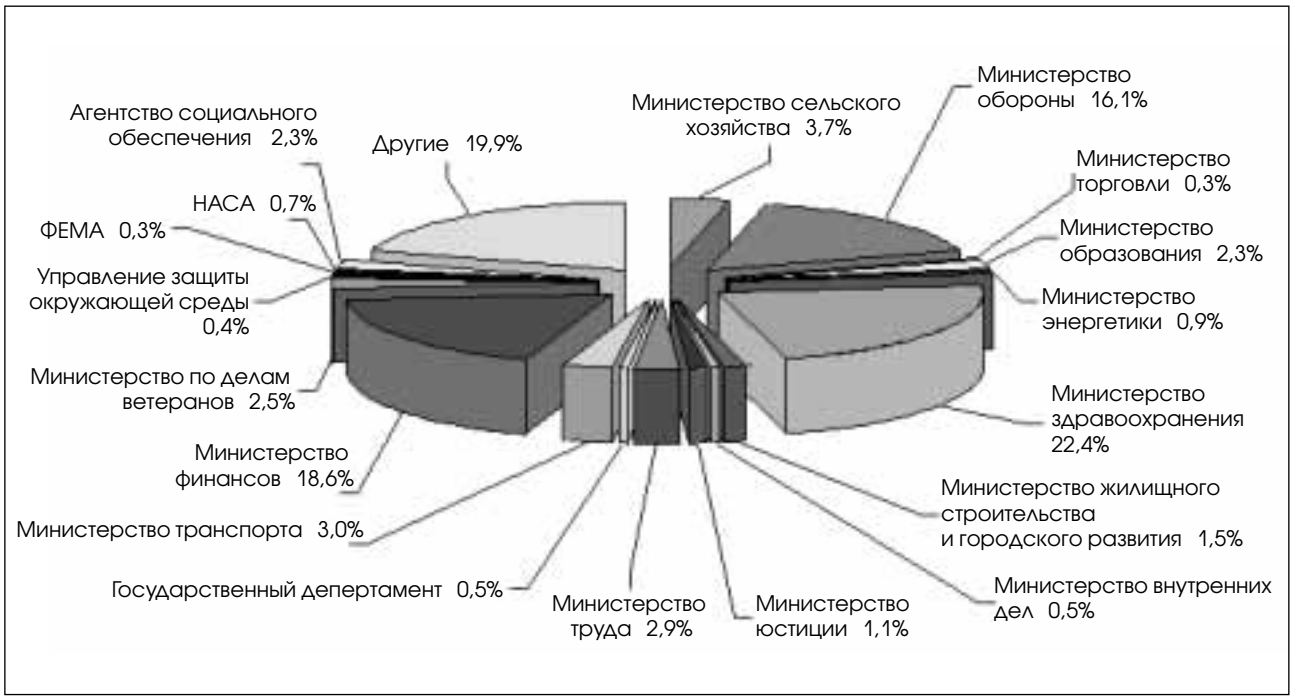


Рис. 3. Распределение бюджетных ассигнований в сумме $2052 млрд. в 2002 финансовом году среди министерств и ведомств США

Бюджет президента Буша – программа безопасности США

Несмотря на трагедию национального масштаба американцы с оптимизмом смотрят в будущее, и, надо признать, у них для этого есть все основания: ФБР по горячим следам обезвредило уцелевших террористов, ЦРУ вскрыло места расположения баз боевиков «Аль-Каида», Пентагон одержал очередную военную победу и получил новые военные базы в Средней Азии, в Афганистане свергнут режим талибов, Зимние Олимпийские игры в Солт-Лейк Сити прошли по сценарию Белого дома, мировые цены на нефть с небольшими колебаниями продолжают снижаться, президент жестко отстаивает интересы национальной металлургической индустрии и производителей продукции птицеводства... Казалось бы, чего еще желать.

А между тем весь этот яркий калейдоскоп событий — ни что иное как очередная пропагандистская компания, имеющая своей целью убедить рядовых налогоплательщиков в том, что они живут в самой сильной, богатой и преуспевающей стране мира. И нет ничего удивительного в том, что правительство США, имея в своих руках такие внушительные козыри, наращивает обороты этой компании и строит планы на будущее, в котором американцы должны быть застрахованы от воздушных таранов, ракетных ударов, вспышек сибирской язвы и проделок хакеров в Интернете.

6 февраля с.г. президент Буш обратился к Конгрессу США с новым законопроектом о бюджете страны на период 2003-2007 гг[5] . В предложенном администрацией и единодушно поддержанном законодателями формально пятилетнем, а фактически (по макро показателям) десятилетнем плане государственных расходов четко просматривается тенденция на увеличение бюджетных ассигнований в области национальной безопасности. К 2007 г. военные расходы США превысят совокупные военные расходы всех остальных стран мира почти в 1,5 раза и составят свыше $450 млрд. В целом за этот период предполагается израсходовать только на военные программы свыше $2050 млрд, т.е. сумму, сопоставимую с бюджетом всех государственных расходов США на текущий ф.г., (рис. 2).

Общая структура госбюджета на 2002 ф.г., дающая представление о приоритетах в расходовании бюджетных средств, приведена на рис. 3.

Среди важнейших направлений бюджетного финансирования помимо военной области администрация четко обозначила: образование, здравоохранение, заботу о ветеранах, безопасность и ... информационные технологии, как ключ решения всех проблем. Только на развитие информационных технологий в ближайшие пять лет предполагается выделить свыше $290 млрд., т.е. почти в 2 раза больше, чем за предыдущие пять лет или примерно весь бюджет Пентагона за 2001 г.

Приоритеты финансирования информационных технологий

На 2003 ф.г. администрация представила запрос на развитие информационных технологий в сумме $52 млрд., что составляет увеличение ассигнований на 15,6% по сравнению с текущим 2002 ф.г. ($45 млрд.)[6]. Известно, что еще в самом начале своего пребывания на посту главы государства нынешний хозяин Белого дома подверг острой критике финансирование так называемого «Национального плана защиты информационных систем в 2000 — 2003 гг.», принятого администрацией Клинтона[7]. По инициативе президента Буша была сформирована специальная комиссия, которой было поручено провести не только проверку выполнения плана, но и пересмотреть сам подход к решению проблемы обеспечения безопасности информационной инфраструктуры в целом. События 11 сентября 2001 г. дали новый толчок этому важнейшему направлению обеспечения национальной безопасности США.

Новый бюджетный план администрации включает $18 млрд. на финансирование 900 стратегических проектов и $11,5 млрд. — других 2000 про-

[5] Budget of the US Government, FY 2002. Office of Management and Budget.
[6] Performance Information for Major IT Investments, February 4 2002, President's Budget for 2003, cross-reference Chapter 22 of the Analytical Perspectives Section, of the 2003 Budget. Page 1 of 89.
[7] Defending America's Cyberspace. National Plan for Information Systems Protection, Version 1.0 An Invitation to a Dialogue, The White House 2000.

ектов, связанных с информационными технологиями. Одним из приоритетных направлений реализации этих проектов является борьба с терроризмом. В частности, предполагается выделить дополнительно свыше $2 млрд. на создание общенациональной информационной системы контроля за иностранцами: по данным Госдепа в США сегодня находится свыше 3 млн. человек с просроченными визами.

На ближайшие пять лет только на проведение НИОКР в области информационной безопасности (ИБ) выделено $880 млн. Начиная с 2003 г. Национальная академия наук США получит на исследования в области безопасности компьютерных сетей $233 млн. и $144 млн. — на создание и развитие специальных исследовательских центров при ведущих американских университетах, а также коммерческих и правительственных лабораториях. Этим же законопроектом Национальному институту стандартов выделено $275 млн. на поддержку совместных с частными компаниями исследований, направленных на совершенствование систем защиты информационных систем и компьютерных сетей.

При этом следует иметь в виду, что эти ассигнования отражают только одно направление НИОКР в общей программе финансирования научных исследований, связанных с защитой критической инфраструктуры, которая была разработана на десятилетний период совместной рабочей

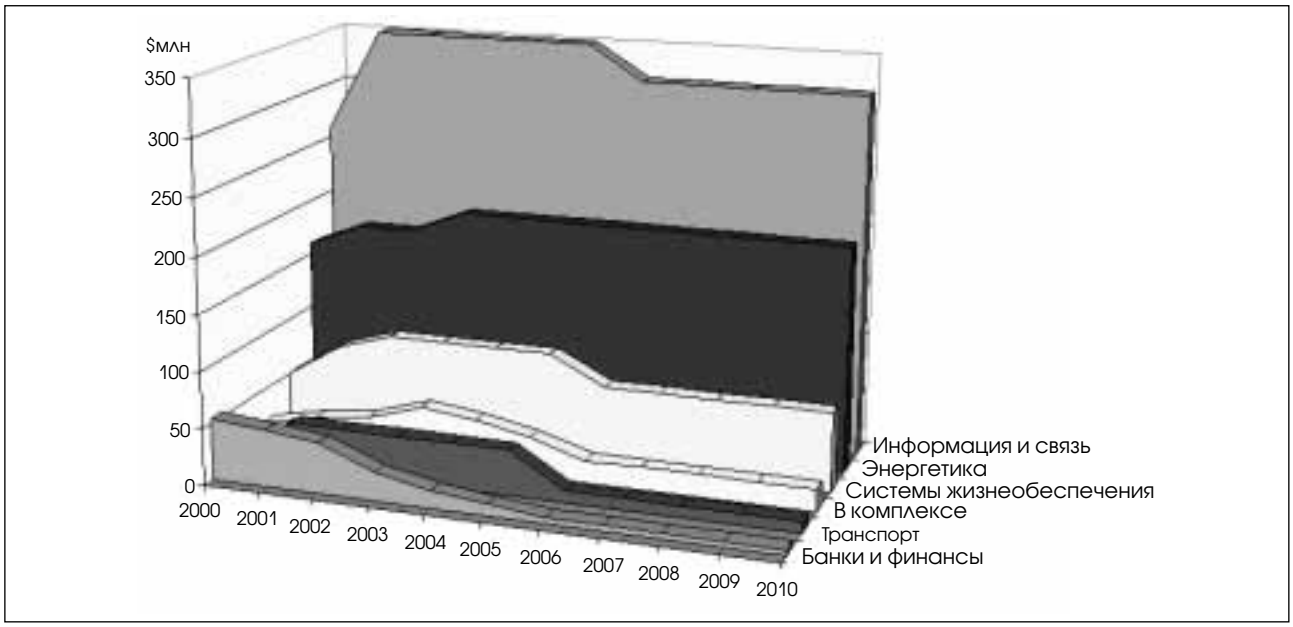


Рис. 4. План финансирования НИОКР по защите основных секторов национальной инфраструктуры США

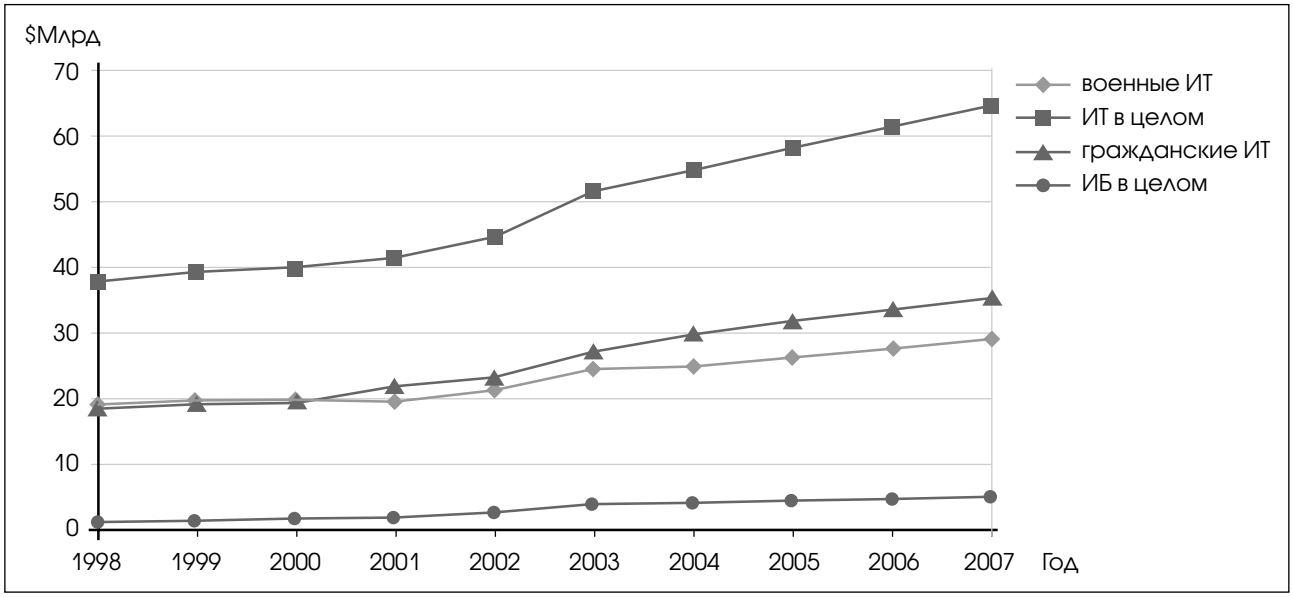


Рис. 5. Динамика бюджетных расходов США на информационные технологии и информационную безопасность

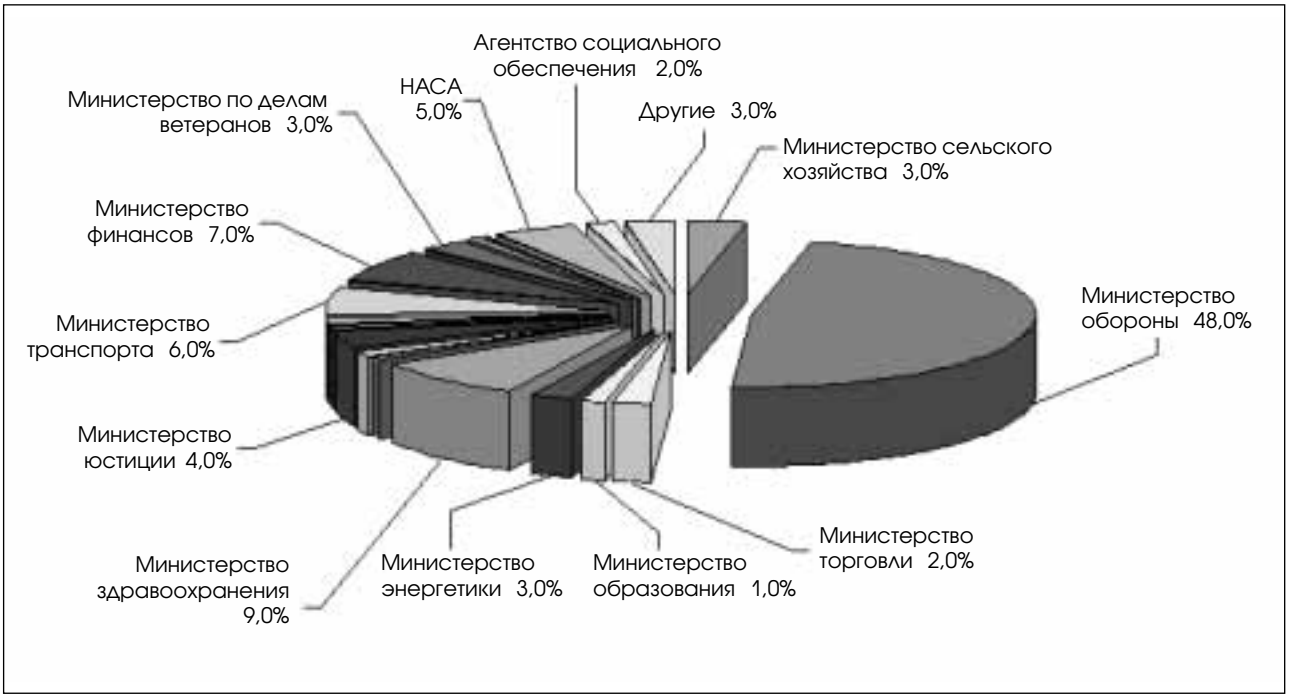


Рис. 6. Распределение бюджетных ассигнований США на информационные технологии в сумме $45 млрд. в 2002 финансовом году

группой министерств и ведомств еще в 2000 г.[8] Динамика и структура общего плана финансирования НИОКР по защите основных секторов национальной инфраструктуры представлены на диаграмме (рис. 4). Анализ этих затрат (свыше $7,4 млрд.) говорит сам за себя: 49% всех ассигнований ($3,6 млрд.) выделено на информационные и телекоммуникационные системы, 29% ($2,1 млрд.) — на энергетику, 12% ($0,86 млрд.) — на системы жизнеобеспечения, по 3% — на банки и транспорт (всего $0,49 млрд.), и еще 4% ($0,315 млрд.) — на комплексные (межотраслевые) исследования.

Кроме НИОКР предусмотрены уже в текущем году конкретные проекты, связанные с информационными технологиями в интересах безопасности: $380 млн. выделено на объединенную информационную систему учета въезжающих и выезжающих за пределы страны, свыше $200 млн. — на создание национальной информационной сети неотложной медицинской помощи, $90 млн. получит Пентагон на создание информационной сети раннего предупреждения населения и беспроводной сети связи для чрезвычайных условий, $50 млн. — ФБР, $20 млн. — на создание объединенного информационного управления при Минторге для координации инвестиционных проектов в области ИБ — одним словом деньги говорят сами за себя.

Прогноз динамики бюджетных ассигнований

Необходимо отметить, что запланированный уровень финансирования НИОКР в области информационной безопасности отражает в целом уровень финансирования федеральных программ, связанных с развитием информационных технологий на предстоящие пять лет. Динамика бюджетных ассигнований, выделенных на развитие ИТ и собственно ИБ, полученная на основе линейной экстраполяции искомых значений на период 2003-2007 гг. при допущении постоянных средних темпов роста с учетом ограничений принятого законопроекта отражает устойчивую тенденцию в этом секторе экономики (рис. 5).

По планам администрации среднегодовой темп роста финансирования ИТ в период 2003 — 2007 гг. составит 6% и к 2007 г. расходы на ИТ в абсолютном исчислении составят $65 млрд. в год, что в 1,65 раза больше аналогичного показателя за 1999 г ($39,5 млрд.)[9]. При этом сложившаяся за последнее время пропорция распределения ассигнований между военными и гражданскими программами развития ИТ будет изменяться в сторону приоритетного развития гражданских систем

[8] Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures (Main). Transition Office of the President's Commission on Critical Infrastructure Protection (PCCIP) and the Critical Infrastructure Assurance Office (CIAO).
[9] GEIA Predicts Significant Growth in the Information Assurance Market, January 11, 2002.

и к 2007 г. составит 45% и 55% соответственно, против аналогичного показателя в 1999 г. — 60% и 40%.

Структура бюджетных ассигнований по министерствам

Распределение бюджетных ассигнований на финансирование развития ИТ в США в 2002 г. в процентном отношении от общей суммы в $45 млрд. (в абсолютных показателях) представлено на рис. 6.

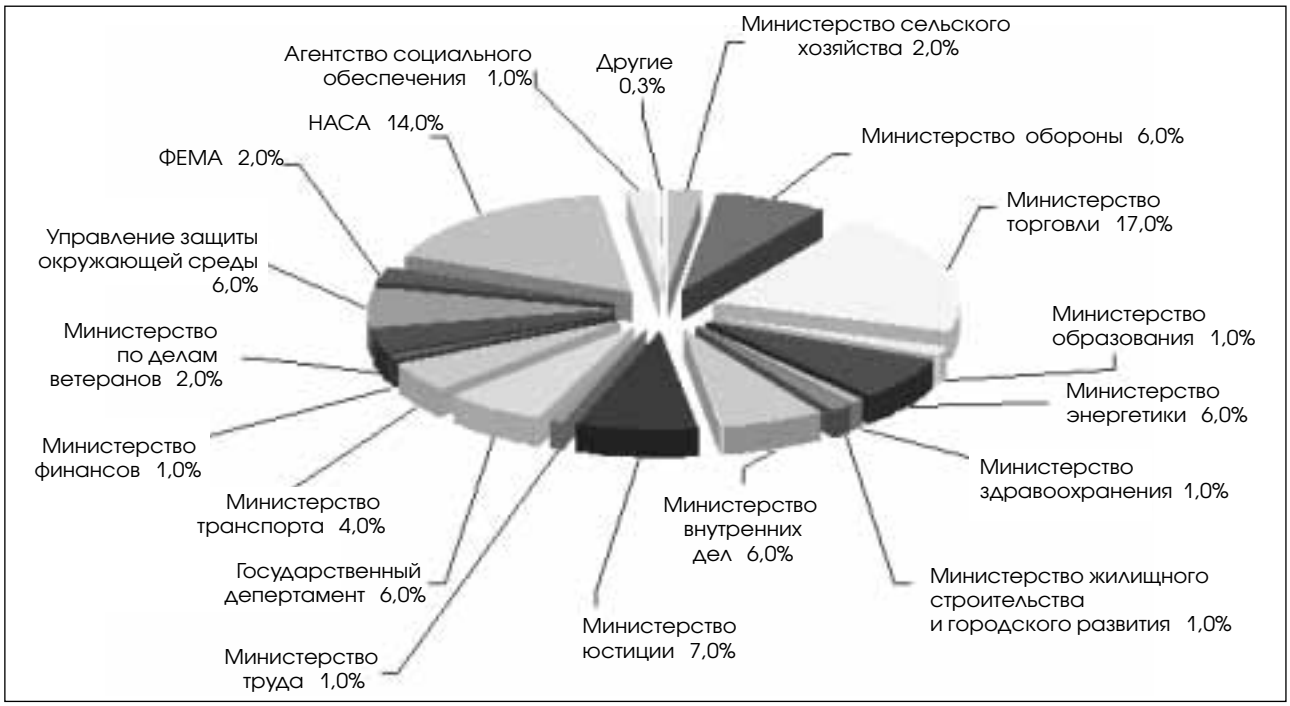


Рис. 7. Доля финансирования информационных технологий в бюджетах министерств и ведомств США в 2002 финансовом году

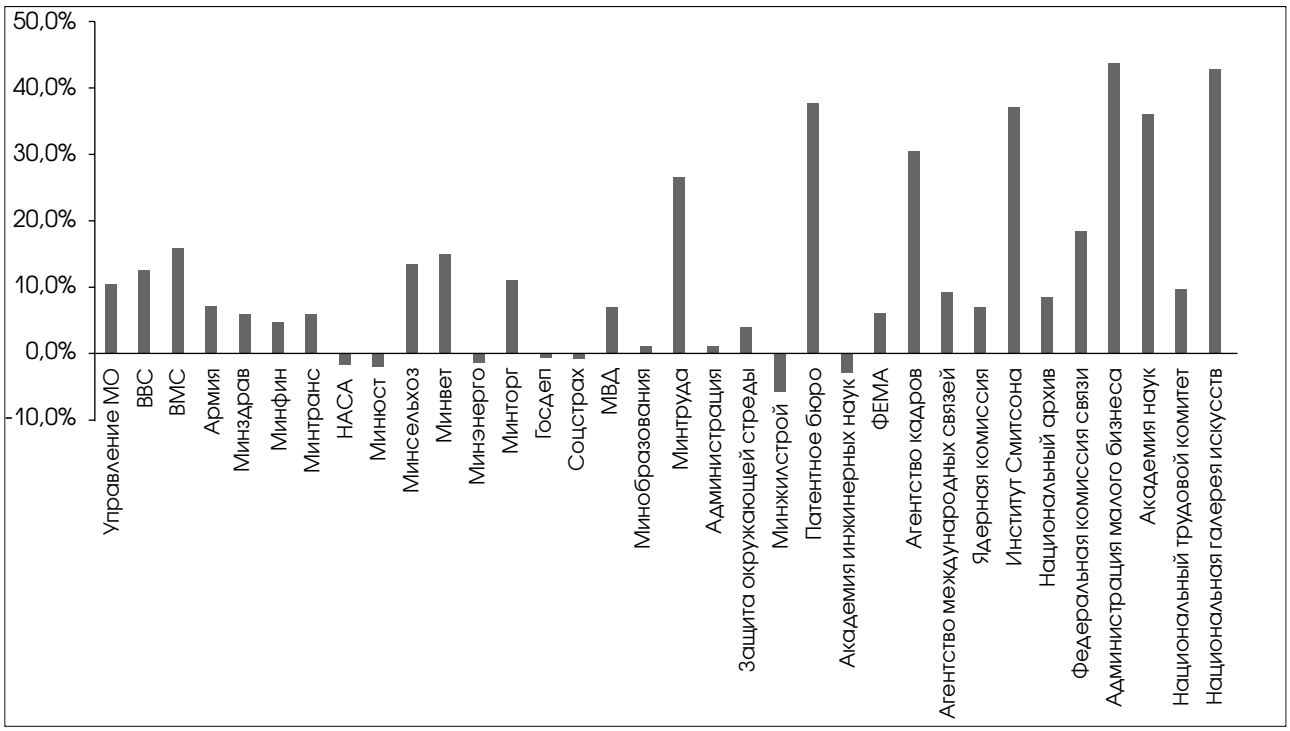


Рис. 8. Изменение структуры бюджетных ассигнований на информационные технологии по министерствам и ведомствам США с 2002 по 2003 финансовые годы

После Пентагона (48% — $21,5 млрд.) — лидера в абсолютных затратах, ведущее положение среди гражданских министерств и ведомств по уровню финансирования ИТ занимают: Министерство здравоохранения (9% — $3,9 млрд.), Министерство финансов (7% — $3,1 млрд.), Министерство транспорта (6% — $2,7 млрд.) и Национальное агентство по аэронавтике и исследованию космического пространства НАСА (5% — $2,1 млрд.). При этом аутсайдерами являются такие ведомства как Министерство торговли (2% — $0,95 млрд.), Агентство социального обеспечения (1,5% — $0,7 млрд.) и Министерство образования (1,5% — $0,65 млрд.) (рис. 6).

В тоже время, если рассмотреть удельный вес финансирования ИТ в бюджете каждого ведомства в отдельности, то не трудно заметить совершенно иную картину характера распределения ассигнований (рис. 7). Например, лидерами по удельному весу расходов на ИТ являются Министерство торговли (17%) и НАСА (14%), в то время как Пентагон (6%) находится на одном уровне по этому показателю с Минэнерго (6%), Госдепом (6%), Управлением защиты окружающей среды (6%), МВД (6%), уступая Минюсту (7%). При этом аутсайдерами по удельному весу затрат являются Минфин (1%) и Минздрав (1%).

Увеличение удельного веса финансирования гражданских программ развития ИТ (рис. 8) свидетельствует об изменении акцентов в государственной политике США в этой области за последние 3-4 года, когда происходило формирование концепции развития национальной информационной инфраструктуры и разработка плана ее защиты. Осознание военными бесперспективности решения этой задачи исключительно собственными силами побудило Пентагон подключить к ее решению фактически все общество, включая государственные, научные, образовательные, коммерческие и общественные организации. При этом Пентагон не снимал и не собирается снимать с себя функции координатора НИОКР и законодателя национальных стандартов в области ИБ, гибко реагируя одновременно на изменения в конъюнктуре рынка данного вида высокотехнологичной продукции.

«Электронное правительство» для «информационного общества»

Большая часть расходов из госбюджета, выделяемых на правительственные программы в области ИТ невоенного назначения в настоящее время идет на развитие ресурсов Интернета, где создано свыше 35 млн. страниц и 22 тыс. сайтов. Результаты проведенного исследования среди 27 правительственных министерств и ведомств США[10], дающие представление об информационном наполнении этих сайтов, отображены на рис. 9. На диаграмме видно, что наиболее полно в правительственном домене Интернета в настоящее время представлены такие разделы как экономика, общественная безопасность, ликвидация аварий и катастроф, управление ресурсами, оплата счетов, обращения и жалобы, кадровые вакансии, финансы, закупки, путешествия, снабжение, администрирование.

В рамках концепции электронного правительства предполагается перевести в режим online около 6600 процедур, связанных с прохождением бумажных документов и унифицировать свыше 1000 форм электронных документов в более чем 250 федеральных учреждениях, что наряду с другими 23 программами в этой области должно дать экономию бюджетных средств в сумме свыше $1 млрд. Основными стратегическими направлениями реализации данной концепции являются следующие: правительство-граждане, правительство-бизнес, правительство-правительство, внутри учреждения.

Среди программ можно выделить, как наиболее значимые, «инициативу электронной аутентичности», призванную обеспечить необходимый уровень идентификации пользователя, достоверности и целостности информации и «проект архитектуры электронного правительства», направленный на создание так называемой межведомственной корпоративной информационной инфраструктуры на основе Интранет-технологий и единого стандарта представления информации в формате XML.

Согласно опубликованному отчету компании Intellor Group, Inc. об исследовании проблем, связанных с использованием стандарта XML (Extensible Markup Language) в правительстве и промышленности США, по отзывам свыше 230 респондентов большинство организаций (до 80%) рассматривают данный стандарт как универсальный формат обмена информацией, позволяющий

[10] Implementing the President's Management Agenda for E-Government, February 27, 2002.

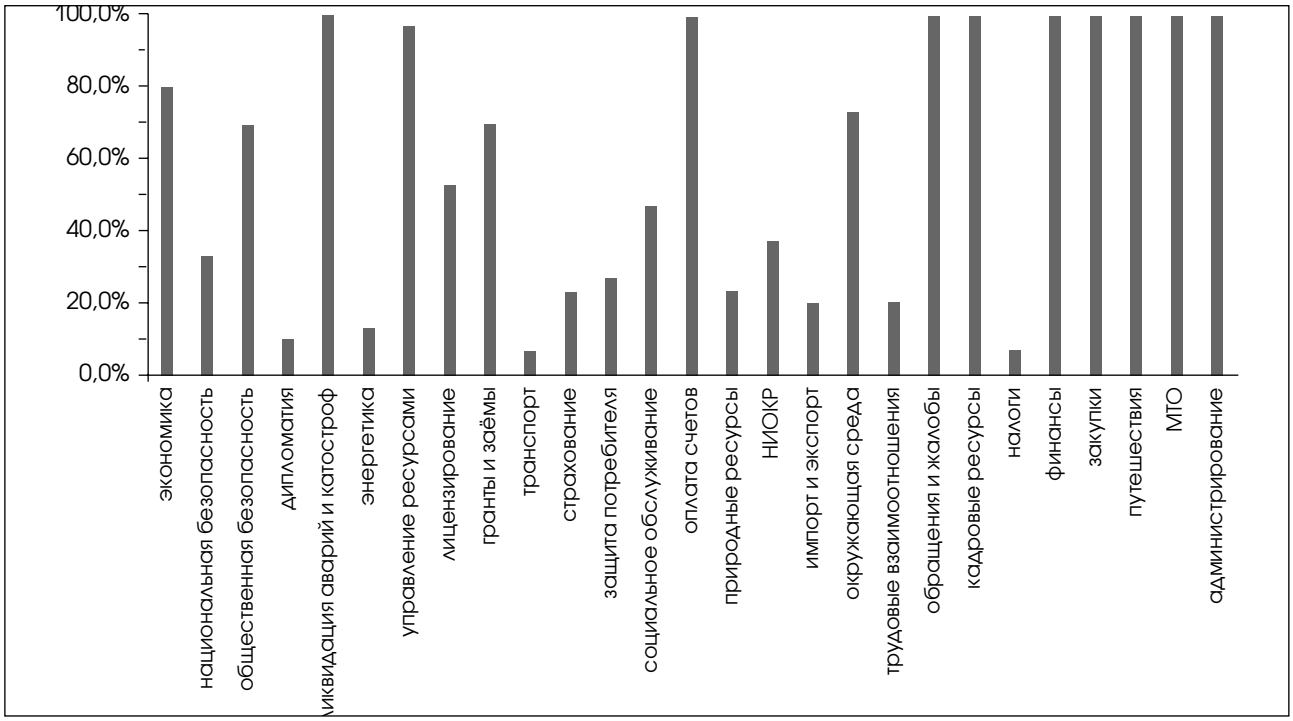


Рис. 9. Структура информационных ресурсов правительства США в Интернете

разрабатывать приложения независимо от аппаратной и системной программной платформ[11]. К числу основных достоинств этого уже широко завоевавшего популярность и авторитет стандарта специалисты относят: универсальность для решения задач класса «бизнес-бизнес», прозрачность технологии доступа к данным, высокий потенциал для разработки интегрированных приложений, значительную экономию времени при преобразовании данных. Вместе с тем, использование XML и сопровождение баз данных в этом формате предполагают высокую квалификацию специалистов, владеющих достаточно обширным в настоящее время спектром технической документации, решение вопросов безопасности транзакций, что накладывает большую ответственность на руководителей при принятии решения о переходе на новую модель данных.

В основе общей концепции электронного правительства положены три руководящих принципа: ориентация ресурсов и услуг на рядовых граждан, а не чиновников, высокая отдача проектов по результатам использования, рыночная система внедрения технологий и инвестирования проектов. Ожидается, что реализация данной концепции позволит в будущем сократить время обслуживания граждан при их обращениях в правительственные инстанции до нескольких часов и даже минут, например, для получения справочной информации, вместо нескольких дней или недель в настоящий момент.

Тем самым работа правительства станет более оперативной и продуктивной, многие бюрократические процедуры будут максимально упрощены, сократятся бюджетные расходы, а граждане станут непосредственными участниками формирования общего информационного поля при принятии решений, затрагивающих их конституционные права и свободы, экономические интересы и личную безопасность. Как говорил вождь мировой пролетарской революции Ульянов-Ленин «каждая домохозяйка сможет участвовать в управлении государством».

[11] Electronic Government. Challenges to Effective Adoption of the Extensible Markup Language. Report to the Chairman, Committee on Governmental Affairs, U.S. Senate GAO-02-327, April 2002.

Информационные технологии для «бесконтактных» войн

Не пожалели американские законодатели денег и на финансирование военных программ, обозначив в качестве главных своих противников политические режимы, поддерживающие терроризм, распространение ракетных технологий и оружия массового уничтожения. Распределение бюджетных средств Пентагона на финансирование ИТ по видам вооруженных сил (ВС) в 2001 г. представлено на рис. 10. Не трудно заметить, что львиную долю ассигнований на развитие ИТ получают военно-воздушные силы (ВВС) — 24%, сухопутные войска (Армия) — 20% и военно-морские силы (ВМС) — 17%, а также управление информационных систем МО — 16%, как ведущая организация, отвечающая за развитие ИТ военного назначения. На долю всех остальных управлений и служб, задействованных в материально-техническом, финансовом, медицинском, картографическом, навигационном и транспортном обеспечении войск приходится в общей сложности 23%, т.е. примерно весь бюджет ИТ ВВС.

Иными словами распределение бюджета Пентагона на развитие ИТ отражает как в капле воды современную американскую военную доктрину, т.е. взгляды на ведение войн, которые США за последние 10 лет научились вести с минимальными потерями на чужой территории так называемым «бесконтактным» способом, используя авиацию, высокоточное оружие, спутниковые системы связи, навигационное оборудование, беспилотные самолеты-разведчики и компьютерные сети. В свою очередь, новые технологии меняют и сам облик вооруженных сил, которые становятся более компактными, мобильными, оснащенными и боеспособными, позволяя быстро развертывать в любой точке земного шара группировки войск «целевого назначения» для решения практически любых задач — от оказания гуманитарной помощи до проведения специальных операций.

Весьма показательной в этом плане является наметившаяся после войны в Югославии в 1999 г. и получившая свое дальнейшее развитие в ходе антитеррористической операции в Афганистане тенденция на максимальное сжатие цикла управления (обнаружение-распознавание-наведение-поражение)[12] при нанесении воздушных ударов с помощью

[12] Network Centric Warfare Conference: Wednesday 19th & Thursday 20th September 2001, Waldorf Meridien Hotel, London.

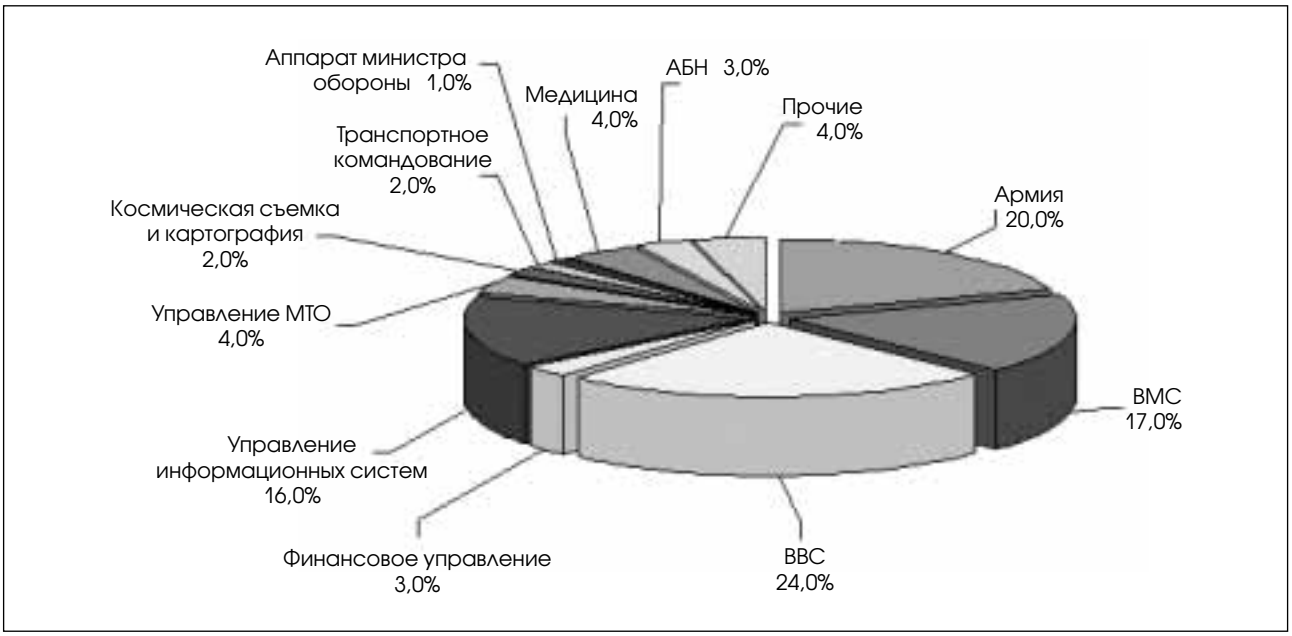


Рис. 10. Распределение бюджета информационных технологий МО США в сумме $20 млрд. в 2001 финансовом году

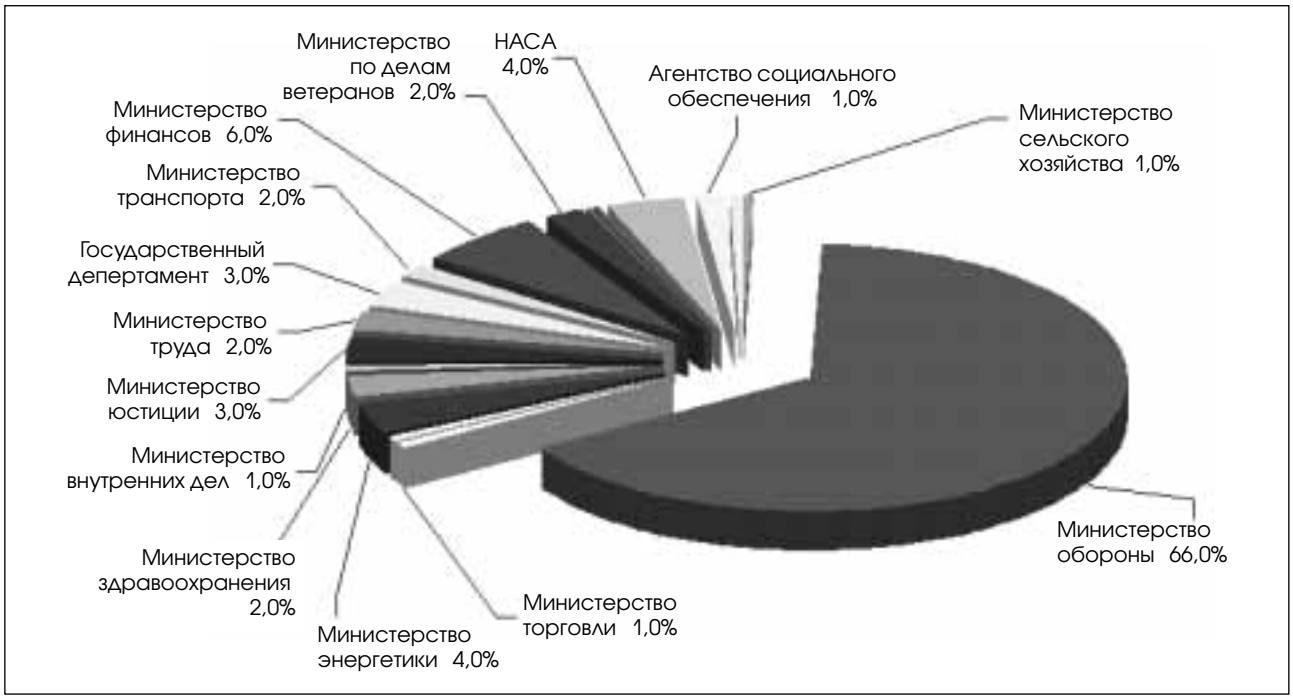


Рис. 11. Распределение бюджетных ассигнований США на информационную безопасность в сумме $2,7 млрд. в 2002 финансовом году

беспилотных самолетов-разведчиков типа Predator (хищник), оборудованных цифровыми видеокамерами, системами распознавания наземных целей, спутниковыми широкополосными системами цифровой связи и самонаводящимися ракетами.

По сообщениям в печати во время одной из таких разведывательных операций 11 февраля с.г. был уничтожен в горах вооруженный отряд террористов, в котором по информации ЦРУ мог находиться Усама Бен Ладен. При этом решение по нанесению удара на поражение принималось практически в течение нескольких минут после обнаружения цели и уточнения информации из других источников, включая космические системы. Ранее при наведении самолетов на цель требовалось значительно больше времени, а фактор внезапности зачастую терял свое значение.

Стоимость одного такого беспилотного аппарата сопоставима со стоимостью истребителя и составляет величину порядка $50 млн. Всего на программу закупки для вооруженных сил беспилотных летательных аппаратов Пентагону выделено около $1 млрд., а на обеспечение их боевого применения с использованием современной информационной инфраструктуры, систем космической навигации, управления, связи и разведки — $5,5 млрд.[13].

Бюджет информационной безопасности

При таких масштабах использования ИТ в структурах федерального правительства и в военных целях[14] не удивительно, что ассигнования на программы, связанные непосредственно с ИБ в соответствии с принятым законопроектом должны возрасти практически в 1,6 раза с $2,7 млрд. в 2002 г. до $4,2 млрд. в 2003 г.[15] Всего же за предстоящие пять лет прогнозируемая сумма расходов на ИБ с учетом вышеописанных допущений может составить сумму порядка $22 млрд. или весь бюджет ИТ Пентагона за 2002 г.

Структура бюджетных ассигнований на ИБ по министерствам и ведомствам на 2002 ф.г. представлена на рис. 11. На диаграмме видно, что львиную долю ассигнований в этой области получает Пентагон 66%, в то время как остальные ведомства, за исключением НАСА (4%), Минэнерго (4%) и Минфин (6%) получают от 1 до 3 % ассигнований, что говорит о действующей системе приоритетов, которая в предстоящие 5 лет постепенно будет меняться.

Интересно, что удельный вес затрат на ИБ в ведомственных бюджетах ассигнований на ИТ имеет совершенно иной характер распределения

[13] DOD gets good marks overall, Federal Computer Week, 4 February, 2002.
[14] Новые приоритеты в информационной безопасности США. Jet Info №10, ноябрь, 2001 г.
[15] FY 2001 Report to Congress on Federal Government Information Security Reform. OMB, 2002.

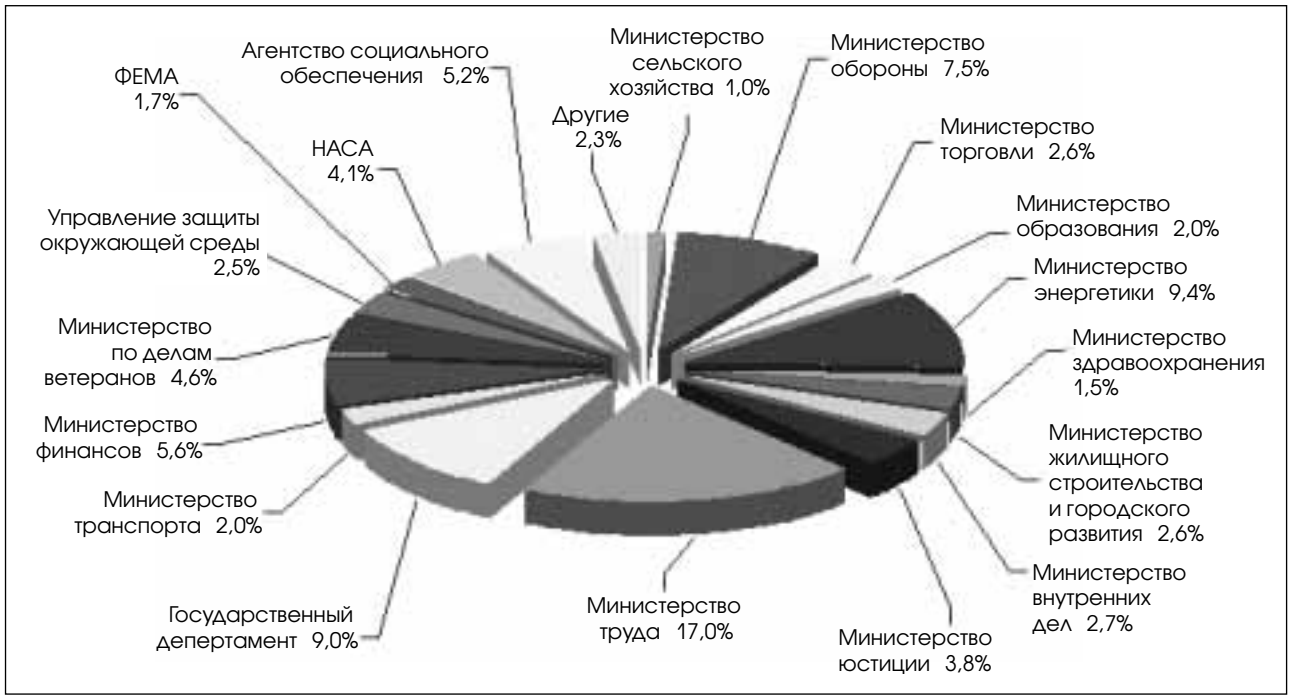


Рис. 12. Удельный вес затрат на информационную безопасность в бюджетах информационных технологий федеральных ведомств США

(рис. 12). Так лидером по этому показателю является Минтруда (17%), а аутсайдером — Минсельхоз (1%), в то время как Пентагон занимает промежуточное положение (7,5%) наряду с другими ведомствами, уступая Минэнерго (9,4%) и Госдепартаменту (9%) и опережая Минфин (5,6%) и Агентство социального обеспечения (5,2%).

Столь резкое увеличение финансирования данной области объясняется во многом неудовлетворительным состоянием защищенности информационных ресурсов, вскрытым Бюджетным управлением при президенте, Счетной палатой Конгресса США и созданным после событий 11 сентября 2001 г. при президенте специальным Комитетом по вопросам защиты критической инфраструктуры во главе с Ричардом Кларком. По данным комиссий из 24 основных федеральных министерств и ведомств в 22 не в полной мере выполняются, а в отдельных случаях нарушаются основные требования, связанные с обязательным выполнением принятых нормативных положений в области ИБ[16].

В соответствии с Законом о безопасности правительственных информационных систем в конце 2001 г. Бюджетное управление при президенте подготовило для Конгресса США годовой доклад о состоянии информационной безопасности в федеральных ведомствах США.

Проанализировав свыше 50 отчетов федеральных ведомств, Бюджетное управление выявило 6 общих для всех недостатков в области ИБ: эпизодическое, от случая к случаю внимание со стороны руководства к данной проблеме, отсутствие стройной, сбалансированной системы критериев эффективности, слабая система профессиональной подготовки и обучения, неэффективная инвестиционная политика, слабый контроль за ИБ на стадии заключения контрактов на поставку ИТ, отсутствие на местах систем обнаружения вторжения и недостаточный обмен информацией[17].

Большая часть федеральных министерств и ведомств (60%) тратит от 2% до 6% бюджета ИТ непосредственно на ИБ. И только пять из 24 организаций тратят от 7% до 17%, а еще пять — от 1% до 2%.

[16] Computer security. Improvements Needed to Reduce Risk to Critical Federal Operations and Assets. GAO. November 9, 2001.
[17] Information sharing. Practices That Can Benefit Critical Infrastructure Protection. GAO. October 2001.

Кадры решают все, но только там, где знания – сила

Какой бы не была совершенной техника и сколько бы на нее не тратили денег пользоваться ей все равно будет человек, потому что он и есть та мера всех вещей, которые создают его дерзновенный разум и неуемная фантазия. Говоря словами отца кибернетики Норберта Винера «оставьте человеку человеческое, а машине — машинное». В конце концов американцы, какими бы богатыми и сильными они не представлялись нам — тоже люди, такие же как и мы. А как известно человеку свойственно ошибаться и впадать в грех, потому что хочет он счастья не завтра, а сегодня. Вот только век его, увы, не долог и денег ему не хватает.

В специальном отчете Комитета Национальной академии общественной администрации, подготовленном в августе 2001 г. для Совета главных информационных администраторов и Административного управления Верховного суда, указываются основные проблемы, связанные с подготовкой персонала в области ИТ: нехватка квалифицированного персонала будет ощущаться в ближайшие 20 лет, в предстоящие 10 лет примерно половина трудовых ресурсов в ИТ достигнут пенсионного возраста, средняя заработная плата специалистов старшего и среднего звеньев в государственном секторе ИТ на 15,7% ниже заработной платы в частном секторе, государственная система подбора кадров на должности специалистов в области ИТ неэффективна, медлительна и непродуктивна по своей организации, слабая система мотивации для профессионального роста специалистов в области ИТ в государственном секторе, система кадрового менеджмента в государственном секторе, в отличие от частного сектора, не стимулирует, а по сути уравнивает в оплате специалистов в области ИТ, отсутствует система непрерывного профессионального роста и обучения, система профессиональной и тарифной классификации устарела и отражает модель промышленности 40-х годов[18].

В целом по результатам проведенного исследования в предстоящие 7 лет США столкнутся с необходимостью увеличить количество специалистов в области ИТ на 20%, при этом к 2006 году 50% специалистов достигнут пенсионного возраста и, как следствие, в среднем на каждые два рабочих места будет приходиться один кандидат, что наряду с неэффективной системой кадрового менеджмента, стремительным развитием рынка ИТ, острой нехваткой квалифицированных кадров, слабой мотивацией и неадекватным материальным стимулированием оплаты труда, отсутствием инвестиций в

[18] A Report by a Panel of the National Academy of Public Administration for the Chief Information Officers Council and the Administrative Office of the U.S. Courts, August 2001, The Transforming Power of Information Technology: Making the Federal Government an Employer of Choice for IT Employees.

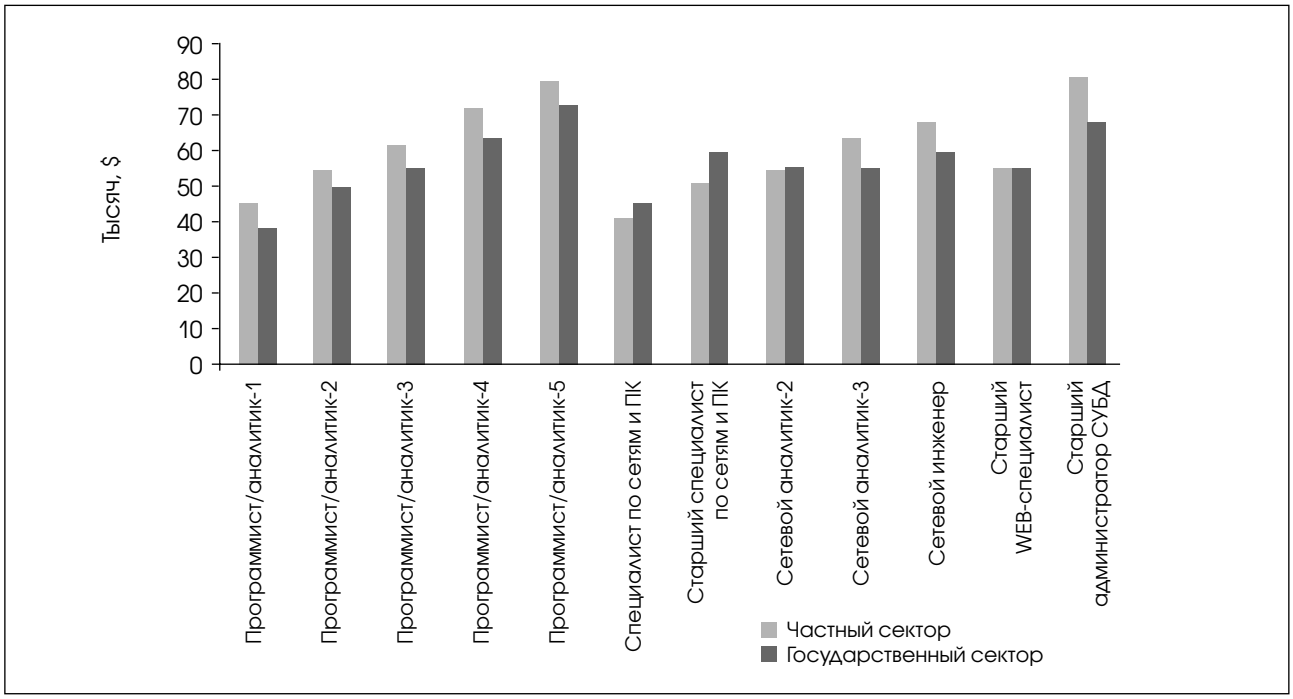


Рис. 13. Средняя заработная плата в год американских специалистов в области информационных технологий

непрерывное обучение, устаревшей системой профессиональной квалификации, разрывом в оплате труда между государственным и частным сектором может привести к неэффективному использованию бюджетных средств, выделяемых на ИТ и ИБ.

По данным Министерства торговли к 2005 году будет создано около 820000 новых рабочих мест в секторе ИТ, а с учетом текучести кадров (до 16% в год по стране) общая потребность составит 1047000 специалистов в области ИТ. Согласно другой не менее авторитетной организации — Американской ассоциации информационных технологий — в 2001 году общее количество специалистов, занятых в этом секторе экономики США, оценивалось в 10,4 млн. человек, а потребность в этих специалистах составляла — 900000 человек, при этом 425000 (47%) заявок остались не удовлетворенными.

Количество специалистов, получивших степень бакалавра по ИТ в 1986 году составляло 42195, а в 1994 — только 24200, т.е. в 1,74 меньше, что подтверждает характерную на этот период времени тенденцию пополнения квалифицированных кадров за счет «утечки мозгов» из бывшего СССР и других стран[19]. Тем самым американским университетам и колледжам потребуются долгосрочные, рассчитанные на 10-20 лет программы подготовки собственных национальных кадров в области ИТ[20].

Это тем более осложняет кадровую ситуацию, поскольку для большинства правительственных организаций характерно в основном безразличное отношение к профессиональному росту специалистов этого высокотехнологичного и одновременно быстро развивающегося сектора рынка труда, где знания устаревают столь же стремительно как и сами технологии. Так по данным Минфина США, где занято свыше 15% всех специалистов в области ИТ, в 1998 г. это ведомство потратило на обучение всего 1,5% от общего фонда заработной платы, в то время как в частном секторе эти затраты составили соответственно — 4,5%, т.е. в 3 раза больше!

Система профессиональной и должностной квалификации специалистов в ИТ, которая на сегодня используется в правительственных учреждениях США, по мнению самих специалистов представляет собой типичный анахронизм конца 40-годов. Несмотря на то, что на протяжении последних 20 лет она уже трижды претерпевала изменения, ее суть осталась прежней: квалифицированные специалисты, проявившие себя в работе выдвигаются на вышестоящие, как правило, руководящие должности, где действует золотое правило бюрократии всех времен и народов — чем больше подчиненных, тем больше тарифная сетка и выше оклад. В итоге большинство хороших профессионалов становится заурядными руководителями с устаревшими уже через 3-4 года знаниями, а организация несет потери в эффективности и организации труда, хотя формально эти специалисты остаются в ней. Иными словами порочной является сама практика стимулировать не постоянный профессиональный рост специалиста, используя его знания и опыт в конкретных проектах, а продвигать его вверх по служебной лестнице, невзирая на то, есть ли у него вообще способности и желание руководить людьми.

В известной степени на низкую эффективность использования специалистов оказывает влияние и сама система тарифов, где по действующему законодательству в правительственных организациях ограничен разброс (30%) в минимальной и максимальной ставке по тарифному разряду (всего 15). Более прогрессивная система оплаты, принятая в частном секторе, допускает 100% разрыв и создает потенциально значительный отрыв в стимулировании труда специалистов с учетом их квалификации, выполненного объема работы и спроса на рынке труда. По разным оценкам разрыв в оплате труда специалистов в бюджетных и коммерческих организациях в США на рынке ИТ колеблется от 17 до 32% в пользу последних (рис. 13).

Не меньшую тревогу вызывает и сама динамика изменения возрастного ценза трудовых ресурсов в этом высокотехнологичном секторе экономики США. За четыре года с 1996 по 2000 гг. количество специалистов, занятых в государственном секторе ИТ, увеличилось всего на 1,32 % с 58,797 до 59,577 соответственно. При этом сами кадры непрерывно стареют: до 70% от общего количества работников достигли возрастной отметки 41 год, а 29% — 51 год и более (рис. 14).

Интересно, что для бюджетных организаций США в настоящее время характерна низкая текучесть специалистов в области ИТ. По официальным данным за 2000 г. средняя текучесть кадров в бюджетных организациях составляла 2,4%: в возрасте от 31 до 40 лет — 4%, от 41 до 50 — 1,6%, от 51 до 60 — 0,9%, а от 60 и старше — 0,5%, в то время как в возрастном интервале от 21 до 30 лет этот показатель сопоставим с коммерческим сектором — свыше 10%. Вполне естественно, что для людей зрелого возраста более привлекательной становится надежная государственная система социального обеспечения, а не высокая зарплата. Подобная стабильность не стимулирует обмен высокопрофессиональными специалистами, руководителями проектов и администраторами систем даже внутри правительственных учреждений, не говоря уже о

[19] Mid-Career Hiring Trends Report. The Partnership for Public Service — February 22, 2002.
[20] Using Information Technology To Transform The Way We Learn. Report to the President. February 2001.

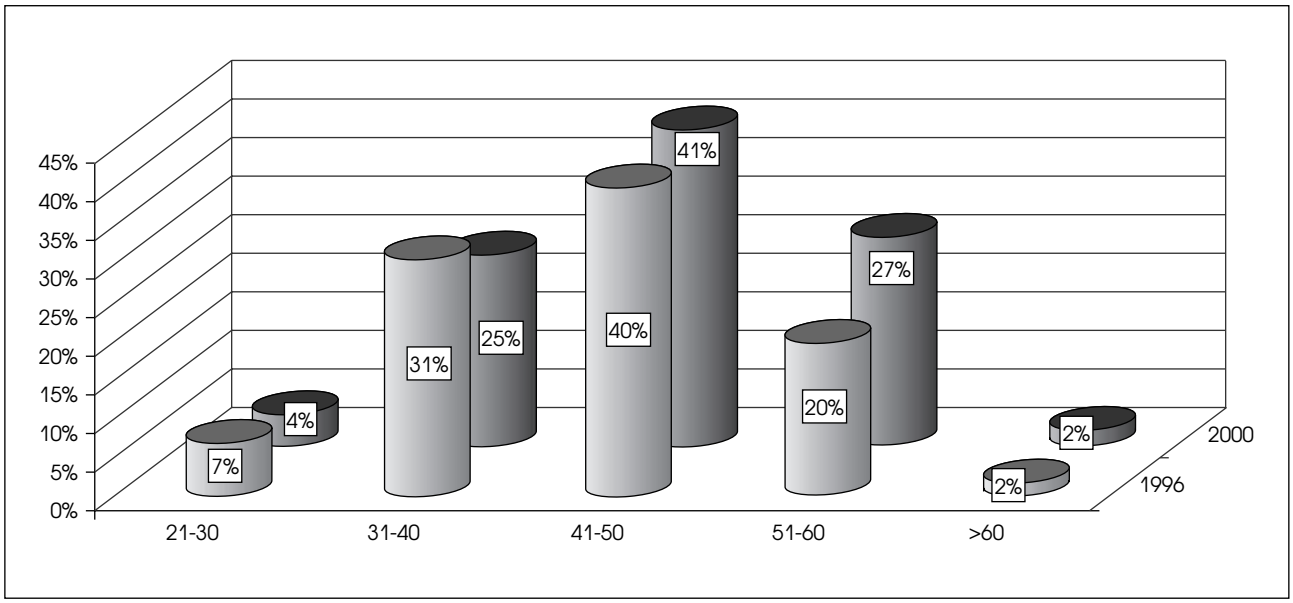


Рис. 14. Распределение специалистов в области информационных технологий по возрастным группам в государственном секторе экономики США в 1996 и 2000 гг.

межведомственной ротации кадров, что широко практикуется в частном секторе.

Учитывая данную демографическую тенденцию, можно ожидать, что к концу 2004 г. в США доля бюджетных «голубых воротничков» в сфере высоких технологий, достигших пенсионного возраста, составит порядка 50%. В целом прогнозируемая потребность для федеральных ведомств в этих специалистах в ближайшие 10 лет по оценкам экспертов составит величину порядка 46 тысяч, включая новые рабочие места.

На основе полученных результатов анализа практики кадрового менеджмента, уровня подготовки, системы обучения, тарифов оплаты и профессиональной квалификации комиссией были даны следующие рекомендации:

- переход на рыночную систему дифференцированной денежной компенсации оплаты по эффективности работы и используемой квалификации;
- использование гибкой системы оценки личного вклада специалиста в конкретный проект с учетом его профессиональной подготовки, снижение времени на подбор и трудоустройство необходимых специалистов с учетом конъюнктуры рынка, отслеживание баланса между личным вкладом, внутренней и внешней конкуренцией специалистов;
- приоритетное стимулирование в оплате руководителей верхнего звена и специалистов высшей квалификации, долгосрочная система подбора кадров на основе рыночной конъюнктуры, выполняемых задач и требуемой квалификации, стимулирование руководителей на гибкое поощрение оплаты труда, выдвижение, профессиональный рост специалистов;
- создание системы непрерывного обучения и профессионального роста с использованием наставников, инструкторов, тестов, удаленных систем обучения и Интернет-классов;
- широкое внедрение ясной и прозрачной системы оценки эффективности труда специалистов по индивидуальному вкладу, стратегическое планирование кадрового менеджмента, профессионального роста и материального стимулирования специалистов.

Для Пентагона проблема подготовки кадров в области высоких технологий имеет особое значение, связанное со спецификой их использования в интересах решения всего спектра задач деятельности ВС. В этом плане следует отдать должное американцам, использующим своих специалистов по назначению на все 100%, активно проводя в кадровом менеджменте линию на широкое привлечение гражданских специалистов.

Распределение специалистов в области ИТ и ИБ по видам ВС представлено на рис. 15. Анализ диаграммы показывает, что абсолютным лидером по количеству специалистов являются сухопутные войска (Армия) (42%), а аутсайдером — морская пехота (13%), в то время как ВВС (21%) и ВМС (24%) занимают промежуточное положение. В целом, это распределение отражает скорее численность личного состава видов ВС, а не приоритеты Пентагона. Однако, если рассмотреть укомплектованность видов ВС кадрами с точки зрения удельного веса специалистов в области ИБ в общей массе специалистов по ИТ, то мы увидим иную картину, где абсо-

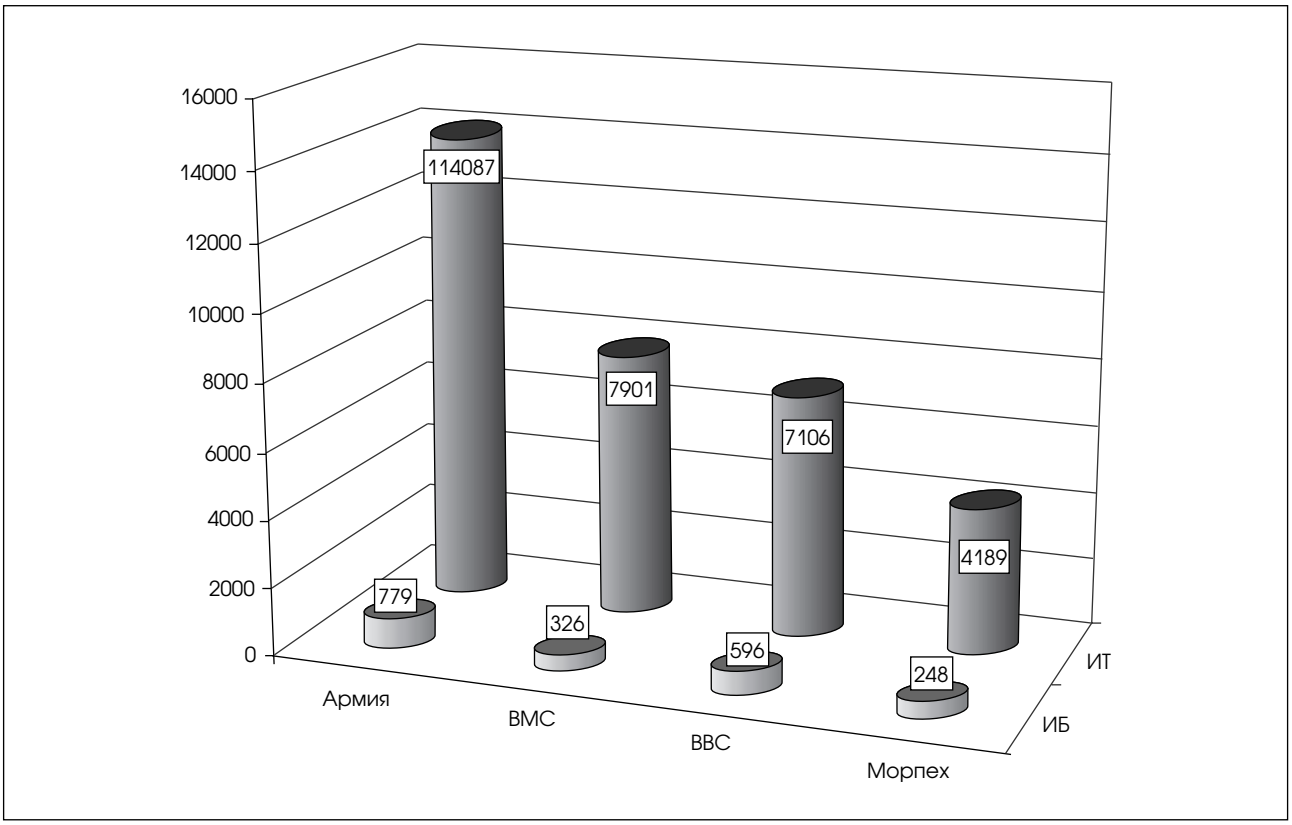


Рис. 15. Распределение специалистов в области информационных технологий по видам вооруженных сил США

лютным лидером выступают летчики (8,4%), аутсайдером, как ни странно, являются моряки (4,1%), а пехотинцы (сухопутные и морские) находятся примерно в равном положении (5,5% и 5,9%)[21].

Эти цифры подтверждают, что ВВС в настоящее время во многом определяют техническую политику Пентагона в области ИБ, решая критически важные задачи в области использования космических ресурсов в интересах национальной безопасности. Заметим, что ВМС уже извлекли определенные уроки из этой статистики и в настоящее время активно готовятся к созданию в июне т.г. первого в американской военной практике «сетевого командования» (Naval Network Warfare Command — NETWARCOM) для решения задач как по защите собственных, так и подавлению информационных сетей противника[22].

Наперекор стихии и террористам

Природные катаклизмы и техногенные катастрофы, обрушившиеся на планету на переломе двух тысячелетий, унесли сотни тысяч человеческих жизней, сметая и разрушая на своем пути плоды титанических усилий цивилизации в борьбе за выживание. Землетрясения, оползни, наводнения, ураганы, тайфуны, магнитные бури — вот далеко не полный послужной список природных бедствий, которым человечество подвергается несмотря на все достижения науки и чудеса техники. Природа коварно мстит homo sapiens за его самонадеянность, напоминая о себе без предупреждения. Но человек отчаянно пытается отвоевать в этой жестокой борьбе со стихией возможность если не обмануть, то по крайней мере предупредить негативные последствия будущих бедствий.

Сейчас, когда человечество вступает в новую эру информационных технологий, проблема защиты коммуникаций становится ключевой для обеспечения эффективного функционирования всех госу-

[21] Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense. Office of the Secretary of Defense August 27, 1999.
[22] Navy sets up a network command. GCN 29 March 2002.

дарственных и общественных институтов практически в любой стране мира, но особенно в США.

Представьте себе, что в вашем доме кто-то из соседей решил сделать ремонт, что само по себе вас никоем образом не должно волновать: в конце концов свои деньги и время тратит кто-то другой, а не вы. Однако, как только у вас перестает идти вода из крана или отключается свет, вы уже начинаете волноваться. Хорошо, если от такого «ремонта» страдают соседи по лестничной клетке или подъезду, а если весь дом. Бывают случаи, когда некотрые организации прояляют такую прыть в своих геологических изысканиях, что приходится останавливать движение поездов в метро, как это было в районе станции Новокузнецкая, где машинист буквально в последний момент успел затормозить, увидев прямо перед собой одиноко торчащий бур «первопроходцев».Тоже самое, но в других масштабах сейчас может произойти с крайне зависимой от информационных технологий и телекоммуникаций инфраструктурой США.

Например, интенсивное развитие трубопроводной, транспортной, энергетической и телекоммуникационной сетей Нью-Йорка за последние 20 лет привело к образованию так называемых критических узлов городской инфраструктуры, один из которых — комплекс зданий Международного торгового центра — стал объектом террористических актов 11 сентября 2001 г.

Обрушение комплекса зданий в результате двух воздушных ударов помимо невосполнимой утраты тысяч человеческих жизней уже в первые часы катастрофы повлекло за собой вывод из строя нескольких подземных станций метро, разрушение путепроводов, отключение энергетической системы, уничтожение информации в компьютерах сотен фирм и офисов, потерю десятка тысяч волоконно-оптических каналов передачи данных, перегрузку трафика Интернета, падение курса акций и закрытие биржи на несколько дней.

Согласно оценкам независимой исследовательской корпорации Computer Economics, сумма ущерба, нанесенного информационной инфраструктуре США в результате террористических актов в Нью-Йорке и Вашингтоне с учетом финансовых потерь и затрат на восстановление, составила величину порядка $15,8 млрд., при этом свыше 25000 специалистов из телекоммуникационных компаний всего мира в течение нескольких недель были заняты восстановлением утраченных и перераспределением сохранившихся информационных и телекоммуникационных ресурсов, и порядка 100000 человек, занятых в сфере банковских и финансовых онлайн операций, были вынуждены сменить место работы по техническим причинам[23].

По мнению экспертов общий замысел крупномасштабной террористической операции, если бы она проводилась в полном объеме, предусматривал в качестве конечной цели дезорганизацию всей государственной системы управления США на фоне финансового кризиса, опустошения прилавков и продовольственных запасов, общественных беспорядков и вооруженных столкновений на расовой и религиозной почве.

Несмотря на то, что еще в начале 90-х годов было принято решение о создании специальных резервных информационных центров в каждом штате на период чрезвычайных условий (аварий, катастроф, стихийных бедствий, террористических актов) власти Нью-Йорка оказались не готовы к такому

[23] Overview of Attack Trends. CERT® Coordination Center. Carnegie Mellon University, 2002.

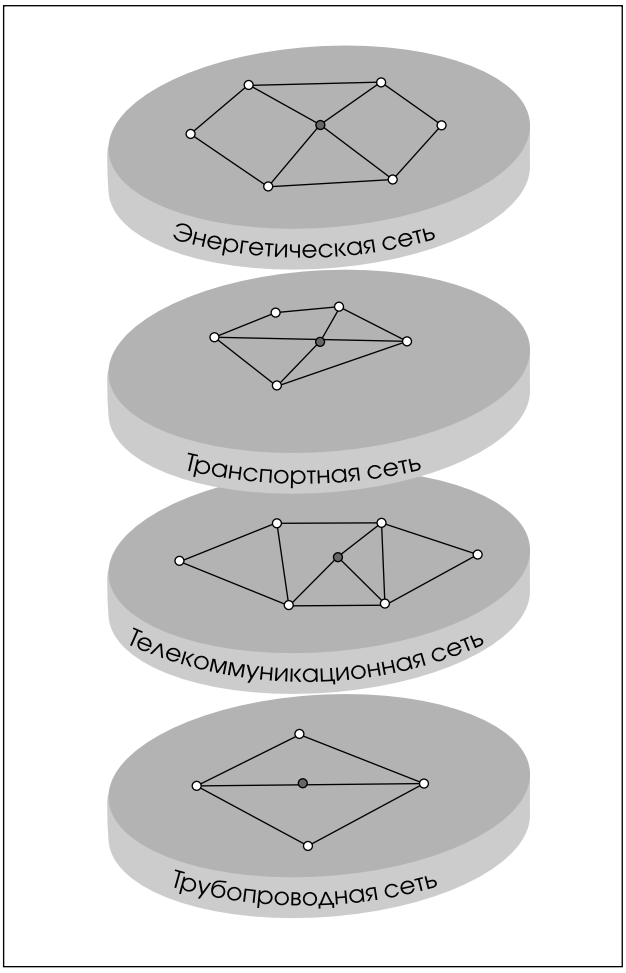


Рис. 16. Многоуровневая топологическая модель коммуникационных сетей

развитию событий, что повлекло за собой потерю информации в сфере социального обеспечения, при этом десятки тысяч малообеспеченных, инвалидов и престарелых оказались в первые недели без пособий. Власти вынуждены были пойти на беспрецедентные меры, обратившись за помощью к добровольцам по сбору, обработке и накоплению утраченной информации. В настоящее время в Конгрессе находится законопроект о создании «национальной сетевой гвардии» (National Emergency Technology Guard)[24], в задачи которой и будет входить оказание помощи правительству в восстановлении информационных ресурсов в кризисных ситуациях.

Вот почему еще задолго до 11 сентября ученые и специалисты начали бить тревогу по поводу непредсказуемости последствий кризисных ситуаций, связанных с масштабными техногенными катастрофами на объектах инфраструктуры. Суть этой проблемы состоит в том, что сегодня в США практически нет точного и подробного национального плана (схемы) не только информационных, но и других видов коммуникаций, неразрывно связанных между собой, которые становятся важнейшим критерием оценки состояния бизнеса, государства, общества. Между тем значимость развития коммуникаций для дальнейшего прогресса цивилизации можно представить в сравнении с повышением обмена веществ, определяющим эволюцию живых организмов.

Пространственно-временная модель корреляции (взаимосвязи) физических и информационных процессов жизнедеятельности всех важнейших компонентов инфраструктуры государства (транспорт, энергетика, связь, финансы...) предполагает знание топологии и определение на ее основе критически важных узлов пересечения элементов сетей.

Наиболее сложным моментом в этой концепции является определение границ системы как совокупности пересекающихся во времени и пространстве сетевых топологических структур. При этом изначально функционально несвязанные элементы этих структур на каком-то этапе своего развития становятся косвенно зависимыми и при определенных обстоятельствах образуют причинно-следственные цепочки потенциальных техногенных катастроф (рис. 16).

В настоящее время в США проводится в жизнь государственная программа аудита (учета) всех видов коммуникаций с целью построения многоуровневой топологической модели и определения на ее основе критически важных объектов инфраструктуры, их взаимосвязи с точки зрения прогнозирования характера и степени потенциальных угроз для безопасности общества и государства в целом.

Сетецентрическая парадигма информационной безопасности

Вот почему жестким и бескомпромиссным императивом дня становится пересмотр, уточнение и расширение существующих классических критериев оценки и стратегии обеспечения информационной безопасности, основы которых были заложены еще в середине 80-х годов прошлого столетия.

[24] NET Guard would be a volunteer expert force. Government Computers News, January 21, 2002.

Классическая модель ИБ основывалась на автономности и локальности ресурсов информационной системы, а ее постановка заключалась, образно говоря, в трех НЕ:

- не допустить,
- не пропустить,
- не упустить.

Соответственно и сама концепция защиты информационных ресурсов строилась по этим же принципам, когда главными задачами обеспечения ИБ являлись:

- ограничение круга пользователей,
- создание системы доступа по паролям и разграничение информации по категориям.

Верхним пределом локальности системы являлись границы государства, а автономности — контур управления или рамки ведомства (организации). Иными словами, в эпоху информационного феодализма все ресурсы имели своих сюзеренов и вассалов в лице администраторов и пользователей, а путь к ним преграждали глубокие крепостные рвы и высокие, непробиваемые стены учреждений, где были закрыты и опечатаны все двери, установлены свои правила в виде многочисленных инструкций и наставлений.

При этом техническая грамотность, культура пользователей и этика их поведения в основном соответствовали существовавшей на тот момент модели информационной безопасности. Интересно, что первый в мировой практике законодательный акт о правовой ответственности за умышленное проникновение, порчу и использование в преступных целях информационных ресурсов — закон о компьютерных преступлениях был принят в США еще в 1987 г. — практически на заре эры лэптоп и до появления Интернета, как всемирной информационной паутины.

Однако после начала массового распространения доступных в цене персональных компьютеров с сетевыми операционными системами уже в середине 90-х годов ситуация с информационной безопасностью начала ухудшаться. Лавинообразный рост числа локальных сетей и пользователей Интернета, среди которых появилось немало авантюристов, хулиганов и преступников, стимулировал поиск новых методов борьбы со взломщиками (хакерами) информационных ресурсов. В связи с активным внедрением доступа к распределенным базам данных на технологии клиент-сервер появляются операционные системы с многоуровневой за-

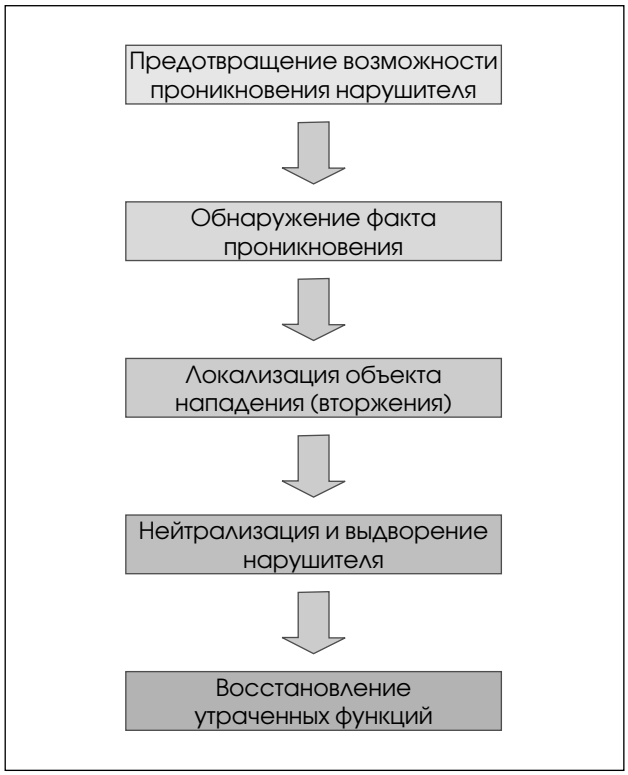


Рис. 17. Концепция эшелонированной системы защиты информационных ресурсов

щитой от несанкционированного доступа, начинают широко использоваться методы криптографии для шифрования транзакций, внедряются интеллектуальные аппаратные средства блокирования подключения устройств (смарткарты).

В 1995 году в открытой печати появляются первые газетные и журнальные публикации, в которых проблема информационной безопасности приобретает своего близнеца и антипода — концепцию информационного противоборства и информационной войны[25,26]. Впрочем, строго говоря, эта концепция в теоретическом плане не является американским изобретением, поскольку многие ее элементы и приемы были позаимствованы прагматичными янки у ... немецких генералов, которые опробовали свои идеи в первых сражениях летней кампании 1941 г. против Красной Армии, впоследствии развеявшей миф о непобедимости германского Вермахта[27].

В США инициатором широкомасштабной и беспрецедентной по своей гласности компании утечки сведений из секретных директивных документов[28], посвященных вопросам ведения информационной войны, становится Пентагон — крестный отец Арпанет, резервной сети связи для веде-

[25] What is information warfare, National Defense University, August 1995.
[26] Пентагон готовится к информационной войне, «Красная звезда», 17 октября 1995г.
[27] Блицкриг как предтеча информационной войны, www.agentura.ru, 2001.
[28] Information warfare TS 3600.1, DOD, 21 December 1992.

ния ядерной войны и бабушки современного Интернета.

Достоянием общественности становятся сенсационные факты использования американскими военными в ходе войны в Персидском заливе в 1991 г. новых технологий, связанных с противодействием информационным системам противника, но при этом раскрывается величайшая со времен атомного проекта «Манхэтэн» тайна — самые оснащенные вооруженные силы в мире могут проиграть войну еще не начав ее: слишком велика зависимость американских военных от информационных технологий, крайне уязвимых для хакеров. Тем самым Пентагон признает реальность угрозы национального масштаба и дает импульс к раскручиванию нового витка гонки технологий безопасности информационных систем.

Историкам еще предстоит пролить свет на темные страницы этой фантастической по своему замыслу и воплощению интриги, в которой было сломано немало копий политиками, военными, учеными и специалистами в поисках истины, защищено множество диссертаций, написаны десятки книг и сотни статей, проиграны и выиграны судебные иски, возвышены капризом изменчивой фортуны и безжалостно низвергнуты слепым провидением человеческие судьбы.

Скандальные истории о крупных мошенничествах в банковской и финансовой сфере, судебные процессы над Кевином Митником и его последователями в кибернетических преступлениях, миллиардные убытки от «электронного» воровства и компьютерных вирусов только подливают масла в огонь. Апофеозом этой компании становится подписание в 1998 г. президентом Клинтоном директивы PDD-63 и принятие в начале 2000 г. «Национального плана защиты информационных систем», в которых информационная безопасность напрямую связывается с безопасностью инфраструктуры страны и благополучием всей нации. В самой богатой и преуспевающей стране мира подлинным лозунгом дня становится девиз «хочешь жить в мире с компьютером — готовься к информационной войне в Интернете». Но война в Америку приходит совершенно с другой стороны — с невидимого фронта борьбы с терроризмом, что только усиливает аспект безопасности инфраструктуры в целом и информационной безопасности в частности.

Новая, сетецентрическая (network-centric)[29] парадигма информационной безопасности, как концептуальная схема (модель) постановки и решения проблемы, вытекает прежде всего из повышенных требований к живучести информационных систем, характеризующихся высокой степенью распределения ресурсов (обслуживанием, логикой, программным и аппаратным обеспечением, телекоммуникациями) и практически полным отсутствием централизованного управления[30].

Получившая в настоящее время в США концептуальная модель эшелонированной многослойной системы информационной безопасности, национального стандарта ISO/IEC 15408[31], разработанного в коридорах Пентагона и АНБ, включает в себя набор компонентов, реализующих функции мониторинга, защиты и адаптации информационных ресурсов, которые в совокупности позволяют поэтапно предотвратить проникновение, обнаружить факт нарушения, локализовать объект воздействия, нейтрализовать и выдворить нарушителя, восстановить утраченные функции системы (рис. 17).

В основе данной модели ИБ лежит широкое использование пассивных (фильтров, экранов) и активных (датчиков обнаружения вторжения, распознавания аномального поведения, адаптивных алгоритмов восстановления) технических средств защиты[32].

Американский опыт использования технологии IDS (Intrusion Detection Systems) в различных секторах экономики и народного хозяйства говорит о том, что не смотря на очевидные преимущества этого направления ИБ (автономность, гибкость, адресность, оперативность и др.) его распространение связано с целым рядом проблем, как объективного, так и субъективного происхождения, среди которых можно выделить в качестве превалирующих ведомственные интересы и организационно-технические аспекты эксплуатации.

Преследование ведомственных интересов даже в таком общенациональном деле как защита информационных ресурсов побуждает одних к активности, а других к пассивности в политике ИБ, что лишний раз подтверждает необходимость централизованного государственного контроля за своевременностью внедрения новых технологий (рис. 18).

На диаграмме видно, что аэрокосмическая промышленность, связь и вооруженные силы явля-

[29] Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations, MILCOM-2001.
[30] Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'2000), Hilton Head Island, South Carolina, January 25-27, 2000.
[31] Defining IT Security Requirements for Federal Systems and Networks Employing Common Criteria Protection Profiles in Key Technology Areas NIST-NSA Technical Working Group.
[32] State of the Practice of Intrusion Detection Technologies CMU/SEI-99-TR-028 ESC-99-028 January 2000 Networked Systems Survivability Program.

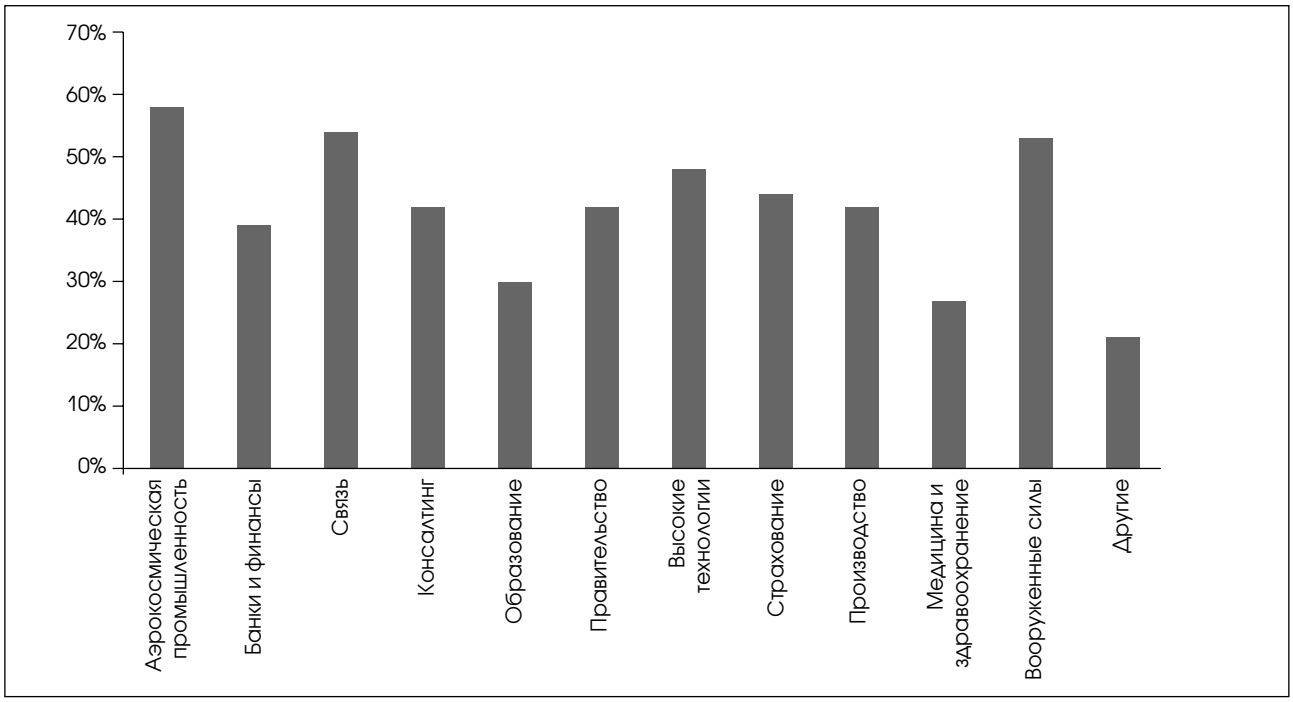


Рис. 18. Использование датчиков обнаружения в информационных системах и сетях в различных секторах экономики и народного хозяйства США

ются наиболее передовыми отраслями народного хозяйства США, где технология IDS нашла свое достаточно широкое распространение, в то время как образование и здравоохранение отстают в данном направлении от других отраслей, что в настоящее время тревожит американцев.

По данным экспертного опроса, проводившегося в США еще до 11 сентября, внедрение технологий на основе датчиков обнаружения вторжения характеризуется большой степенью инерции в мышлении как персонала, так и руководства, что проявляется в стремлении под любыми предлогами уйти от нововведений такого рода.

Характерно, что в большинстве случаев (рис. 19) основными причинами являются не сами технологии, их качество, высокая стоимость, бюджетные ограничения и сложность исполнения (объективные факторы), а отсутствие централизованного руководства, неясность в степени ответственности, отсутствие внутренней политики, обученного персонала, слабые навыки и безразличие администрации к данной проблеме (субъективные факторы). Тем самым, на примере только одной технологии IDS мы видим, что ИБ по сути является не проблемой технологий, а проблемой менеджмента.

В целом обеспечение информационной безопасности сегодня включает в себя такие понятия как **целостность** (integrity) информации, **конфиденциальность** (confidentiality) и **защищенность** от несанкционированного доступа (authentication, non-repudiation) и обеспечение **надежности** (availability) функционирования системы[33]. Зарубежный и отечественный опыт показывает, что эта задача наиболее эффективно решается с помощью методов криптографии в сочетании с использованием проверенного и лицензированного программного обеспечения, а также надежными интеллектуальными носителями ключевой информации (материала ключа).

Например, обеспечение целостности информации и аутентичности (личности) пользователя в настоящее время наиболее эффективно реализуется за счет использования электронной подписи на основе несимметричных криптографических алгоритмов с двумя ключами (личным и общим) в сочетании с системой удостоверяющих центров. В США этот концептуальный подход к защите информационных ресурсов получил название «информационной гарантии» (information assurance), который существенно расширил рамки классического понятия информационной безопасности (INFOSEC).

Фактически концепция информационной гарантии в США рассматривается как оборонительная информационная операция, в ходе которой даже при случайном или преднамеренном искажении информации, несанкционированном проникновении или умышленном вторжении в контур управления, потери части ресурсов и перегрузки трафика комплекс организационно-технических мер защиты должен обеспечить выполнение наиболее важных задач. Иными словами, не только от-

[33] Information Assurance in Networked Enterprises: Definition, Requirements, and Experimental Results CERIAS, TR 2001-34 School of Industrial Engineering, No. 01-05 Purdue University January 2001.

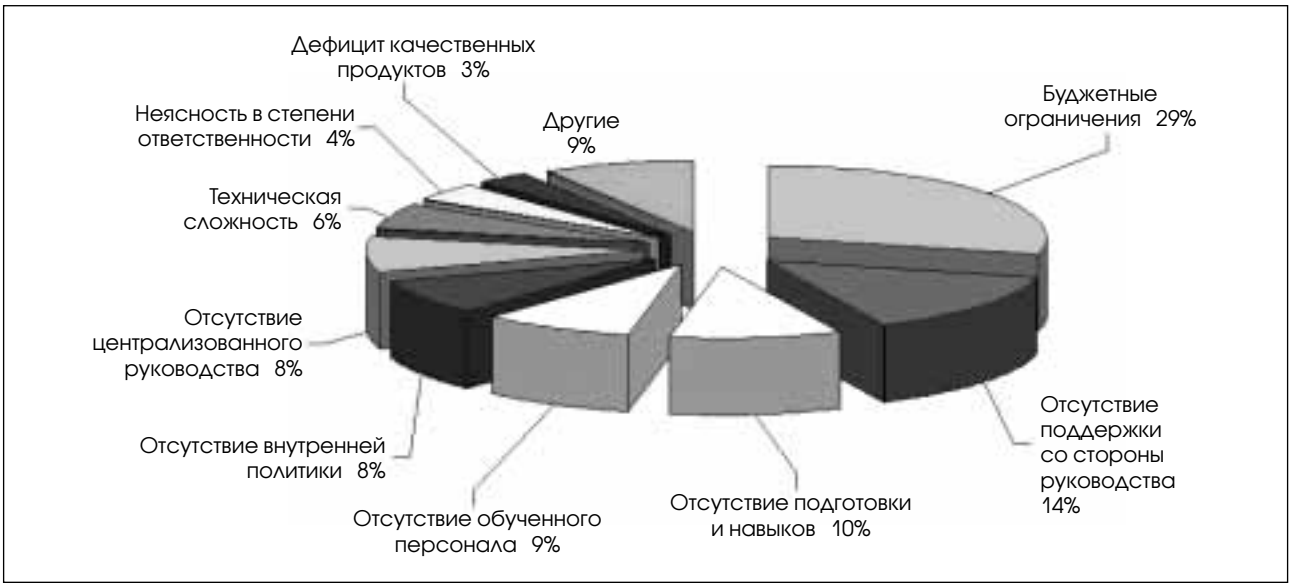


Рис. 19. Причины, затрудняющие внедрение технологии датчиков обнаружения вторжения

казы и сбои оборудования, искажение и утечка информации, но и саботаж персонала, шпионаж, действия хакеров, диверсии и террористические акты на объектах информационной инфраструктуры рассматриваются уже не как гипотетические угрозы, а как системотехнические факторы внешней среды со всеми вытекающими последствиями.

Понятно, что для полноценной работы и сохранения минимального набора критически важных функций система должна обладать вполне определенным запасом устойчивости к внешним дестабилизирующим воздействиям среды. При этом нарушение целостности системы на фоне снижения активности ее элементов влечет за собой дезорганизацию управления, одновременное снижение активности элементов и их живучести — потерю гибкости, а снижение живучести и нарушение целостности системы — потерю важнейших функций[34]. Тем самым синергетика гомеостаза (состояния устойчивого равновесия) информационной системы определяется балансом энтропии (мерой неопределенности) внешней среды и запасом живучести ее элементов (рис. 20).

В свою очередь, понятие живучести (survivability) системы[35] подразумевает ее способность своевременно выполнять свои функции в условиях действия дестабилизирующих факторов (физическое разрушение, частичная потеря ресурсов, отказы и сбои элементов, несанкционированное вмешательство в контур управления). При этом техническая надежность, проявляющаяся как способность системы работать на заданном отрезке вре-

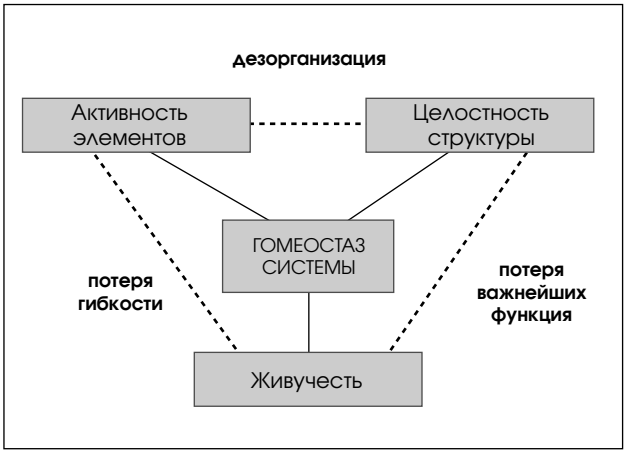


Рис. 20. Концептуальная модель гомеостаза информационной системы

мени в штатной ситуации без отказов, определяет минимальный порог устойчивости системы, за которым без наличия системы восстановления утраченных элементов и функций может наступить катастрофа. Следовательно, живучесть информационных систем имеет определяющее значение для информационной безопасности в целом[36].

В свою очередь, эффективность такой концепции защиты государственных и коммерческих информационных систем определяет безопасность инфраструктуры государства в целом, а живучесть этих систем — мобилизационную готовность вооруженных сил, промышленности, экономики, народного хозяйства и общества в целом как к ведению войны, так и к ликвидации последствий террористических актов, стихийных бедствий и техногенных катастроф.

[34] Modeling the Revolution in Military Affairs, Autumn/Winter 1998-99 / JFQ.
[35] Survivable Network Systems: An Emerging Discipline CMU/SEI-97-TR-013 ESC-TR-97-013 Software Engineering Institute Carnegie Mellon University Pittsburgh, May 1999.
[36] On the definition of survivability. Department of Computer Science University of Virginia, June 2001.

Таким образом, концепция информационной безопасности 21-го века вытекает прежде всего из повышенных требований к живучести информационных систем, выходящих за рамки предприятий, ведомств и границ государств, характеризующихся высокой степенью распределения ресурсов и практически полным отсутствием централизованного управления.

Системы безопасности будущего должны не только и не столько ограничивать допуск пользователей к программам и данным, сколько определять и делегировать их полномочия в корпоративном решении задач, выявлять аномальное использование ресурсов, прогнозировать аварийные ситуации и устранять их последствия, гибко адаптируя структуру в условиях отказов, частичной потери или длительного блокирования ресурсов[37].

Человеческий фактор

Исходя из этой модели ИБ, система должна распознавать пользователей не только по логинам и паролям, индивидуальным биометрическим показателям, но и по их поведению (характерным запросам информации, последовательности доступа к данным, трафику, временным нормативам транзакций). На определенных этапах работы, связанных с доступом к особо важной информации и критическим функциям системы, возможен контрольный тест, при этом данные теста могут быть сверены с результатами предыдущих тестов и занесены в базу данных. Накопление статистики дает возможность определять аномальные отклонения в модели поведения пользователя и реагировать соответствующим образом на них, выдавая предупреждения, вводя ограничения, отключая или выдворяя за грубые нарушения регламента.

Однако для этого необходимо иметь своеобразный формализованный социально-психологический портрет личности пользователя, в котором должны быть отражены такие его индивидуальные качества как: интересы и мотивы, склонности и способности, характер и темперамент, идеалы, ценностные ориентации, волевые, эмоциональные и интеллектуальные особенности, профессиональная квалификация, жизненный опыт[38].

Заметим, что идея создания формализованного описания портрета личности человека не нова и при всей своей очевидной прагматичности может вызвать скептическое отношение не только у профессиональных психологов, но и протест у любого человека, осознающего свою индивидуальность, которая не всегда вписывается в стереотипы поведения: одно дело сопоставлять вес, рост, цвет глаз, отпечатки пальцев, группу крови и код ДНК, другое дело — характеры, способности и наклонности, которые проявляются далеко не всегда у всех одинаково в различных ситуациях.

Кроме того, подобный подход к профессиональному подбору кадров может привести к дискриминации: по оценкам специалистов около 40% людей относятся к интровертам, т.е. замкнутым по характеру, сосредоточенным на себе или, как говорят психологи, «углубленным в свой внутренний мир» личностям — потенциальным с точки зрения информационной безопасности «нарушителям» и «злоумышленникам», чье поведение характеризуется непредсказуемостью и неадекватностью.

Как ни странно, но именно среди интровертов можно найти немало одаренных, талантливых людей (композиторов, художников, писателей, ученых), чье творчество обогатило культуру и приумножило знания человечества. Не секрет, что многие руководители предпочитают иметь в своем окружении заурядных и послушных во всем работников, сверкая на их фоне подобно звездам на небосклоне в безлунную ночь.

Как видим проблема в большей степени заключается не в психологическом типе человеческой личности, а в конкретных социально-бытовых и культурно-исторических условиях, в которых эта личность пытается найти свое место в обществе, утвердить себя и раскрыть свой духовный и интеллектуальный потенциал.

Безусловно, тщательный профессиональный отбор с точки зрения изучения психологических особенностей личности специалиста, от настроения и поведения которого в экстремальной ситуации могут зависеть тысячи человеческих жизней, работа сложнейших технологически связанных между собой и потенциально опасных систем и их сетей (в самом широком понимании) является необходимым, но не достаточным условием обеспечения информационной безопасности.

[37] A Case Study in Survivable Network System Analysis CMU/SEI-98-TR-014 ESC-TR-98-014 September 1998.
[38] Research on mitigating the insider threat to information systems. RAND. Conference Proceedings, August 2000.

Информационная матрица 21-го века

Сегодня мир находится на распутье, в начале новой эры компьютерных технологий, связанных с «сетецентрической» обработкой данных. Манипуляция и обмен сложными данными происходят в масштабах все более крупных и сложных неоднородных сетей, спонтанно расширяющихся в неконтролируемом пространстве Интернета, пользователями которого сегодня в мире являются свыше 500 млн. человек. Аудит информационных ресурсов[39] и обеспечение живучести сетей становятся самыми актуальными направлениями безопасности инфраструктуры современной цивилизации. Требования, предъявляемые к функциональным возможностям, производительности и безопасности следующего поколения информационных технологий, подразумевают выход формы представления и способа обработки данных за пределы ставших уже классическими клиент-серверных и реляционных моделей.

В настоящее время за рубежом все большее развитие получает принцип организации информационных, телекоммуникационных, вычислительных и кадровых ресурсов по типу «матрицы», когда обеспечивается гибкое, безопасное и централизованное распределение ресурсов в интересах так называемых «виртуальных организаций», создаваемых под решение возникающих задач в сложной динамичной обстановке[40].

Так Пентагон, в соответствии с единой концепцией развития ВС США до 2020 г., создает Глобальную информационную матрицу (Global Information Grid), с помощью которой, уже начиная с 2005 г., будет осуществляться в реальном времени управление мобильными и компактными смешанными формированиями в любой точке земного шара[41]. При этом высокая маневренность и огневая мощь подразделений будут органично сочетаться с эффективным, гибким, безопасным и оперативным распределением информационного ресурса. Иными словами любая боевая платформа — танк, самолет, спутник или корабль — в зависимости от условий обстановки и решаемых задач в «матрице» сможет выступать и как средство поражения, и как источник разведывательной информации, и как канал связи, и как элемент системы планирования и принятия решения. Конечной целью данного проекта является интегрирование в «матрицу» в качестве огневой, разведывательной, информационной и командной «ячейки» отдельного военнослужащего вне зависимости от принадлежности к формированию, роду войск или виду вооруженных сил.

Опыт проведения антитеррористических операций в Афганистане и на Северном Кавказе показывает, что организация связи и информационного взаимодействия даже среди элитных подразделений спецназа различной ведомственной принадлежности зачастую вызывает проблему, для решения которой в боевых условиях приходится расплачиваться жизнями людей.

Еще одним примером «матричного» подхода к организации распределения информационных ресурсов является проект АНБ «Пахарь» (GroundBreaker), с помощью которого за $5 млрд. из кармана налогоплательщиков шпионское ведомство США предполагает радикальным образом решить назревшую проблему дефицита вычислительных ресурсов для обработки перехваченной системой «Эшелон» в эфире и телекоммуникационных сетях информации. Пытаясь представить реорганизацию своего ведомства внешне как сокращение штата и формальный перевод квалифицированных сотрудников в промышленность и бизнес, руководство АНБ лукаво умалчивает о той роли, которую они будут выполнять в «матрице» глобальной электронной разведки. Между тем на этот шаг «Большого брата» во многом натолкнули эксперименты энтузиастов, использовавших для раскрытия блочного шифра DES ресурсы Интернета, когда на перебор всех комбинаций ключа потребовалось всего несколько часов, а не заявленных ранее сотен лет непрерывной работы новейшего суперкомпьютера.

Для оперативного анализа и принятия решений в кризисных ситуациях в рамках разведывательного сообщества США разрабатывается «виртуальная аналитическая среда» по проекту «Генуя», с помощью которой предполагается на основе неструктурированной и неоднородной информации (текст, графика, изображение, видео, звук) из различных источников (агентурных, радиотехнических, оптических, электронных и др.) получать новые знания о ситуации, проводить сравнения с аналогичными ситуациями в прошлом, отбирать скрытые факты и делать на их основе логические заключения, обеспечивать совместную работу всех заинтересованных участников независимо от их местонахождения. При этом основной упор в данном проекте делается на углубленном и неформальном анализе предкризисной ситуации в инте-

[39] Implementation of DOD information security policy for processing accomplished at defense enterprise computing centers Report No. D-2001-183, September 19, 2001.
[40] The Anatomy of the Grid. Enabling Scalable Virtual Organizations. Ian Foster, Carl Kesselman, Steven Tuecke.
[41] Global Information Grid support to CINC requirements (DSC Study FY00-05, FY01-05).

ресах принятия упреждающих стратегических решений военно-политическим руководством страны, что должно обеспечить так называемое «превосходство в принятии решений» как основы для проведения широкомасштабной информационной операции в интересах национальной безопасности.

Именно эти информационные системы (Интелинк, Джейвис, Критиком и др.) в настоящее время и вызывают настоящую головную боль у американских политиков и военных, которые добиваются от директора ЦРУ и его коллег по сообществу (ФБР, АНБ, РУМО, Госдеп и др.), где каждое ведомство «готовит обед из собственных продуктов на отдельной плите», только одного — своевременной, полной и достоверной информации об угрозах США.

Иными словами сегодня эффективность разведки определяется не количеством компьютеров, баз данных, спутников и агентов, а степенью метаболизма (обмена) во всем этом бескрайнем океане информации. В этом плане для рыцарей плаща и кинжала лучшего примера для подражания, чем биржи не найти: по информации, поступающей в режиме реального времени, брокеры устанавливают реальные курсы валют и котировки акций, которые и служат достоверным индикатором состояния финансовой системы и экономики страны.

Предполагается, что «матричный» подход к организации распределения информационных ресурсов в рамках «виртуальных организаций» будет реализован на основе универсальной эталонной модели взаимодействия открытых сетей (ЭМВОС), в которой информационная сеть рассматривается как совокупность функций, которые делятся на группы, называемые уровнями. Разделение на уровни (прикладной, представительный, сеансовый, транспортный, сетевой, канальный, физический) позволяет вносить изменения в средства реализации одного уровня без перестройки средств других уровней, что значительно упрощает и удешевляет модернизацию средств по мере развития техники. При этом будут разработаны стандартные протоколы и распределенные операционные системы для более высоких уровней организации обмена информацией и обработки данных, надстроенных в виде интеллектуальной оболочки над ЭМВОС.

Одним из перспективных направлений в этой области является технология так называемых «тонких клиентов», в которой рабочие станции пользователей в отличие от современных будут иметь минимальный набор аппаратно-программных средств, а все необходимые программы и данные будут загружаться непосредственно из мощных сетевых серверов каждый раз для решения конкретных задач, а после их выполнения удаляться. Тем самым Интернет постепенно будет трансформироваться в сеть исполняемых приложений[42].

В настоящее время в разработке проблемы «матрицы» заняты ведущие научно-исследовательские центры (Митре, Карнеги и др.) и университеты США (шт. Мэрилэнд, Калифорния, Нью-Джерси и др.), финансируемые в рамках проектов N66001-96-C-8523 министерством обороны и W-31-109-Eng-38 — министерством энергетики, а также космическим агентством НАСА, кровно заинтересованными в результатах проводимых исследований для повышения эффективности и безопасности использования информационных ресурсов.

Статистика и структура компьютерных правонарушений

Пентагон уже официально признал низкую эффективность широко разрекламированной концепции создания так называемой эшелонированной системы информационной безопасности, трезво оценивая масштабы не только внешних вторжений, но и внутренних инцидентов, связанных с нарушением персоналом регламента использования информационных ресурсов.

По данным центра оперативного реагирования CERT, отслеживающего все инциденты, связанные с несанкционированным вторжением в информационные ресурсы США, количество таких инцидентов в 2001 г. по сравнению с 2000 г. увеличилось более чем в 2 раза с 21756 до 52658. Всего, начиная с 1988 г., после принятия Конгрессом США специального закона о компьютерных преступлениях было зафиксировано 100369 таких правонарушений, большинство которых остается нераскрытыми (рис. 21).

Только по официальным данным американские компании понесли убытки от действия двух компьютерных вирусов «Красный червь» и NIMDA летом 2001 г. свыше $4 млрд. В целом, по различным

[42] Network-Centric Computing. Preparing the Enterprise for the Next Millennium. Computer Technology Research Corp. http://www.itworks.be/reports/.

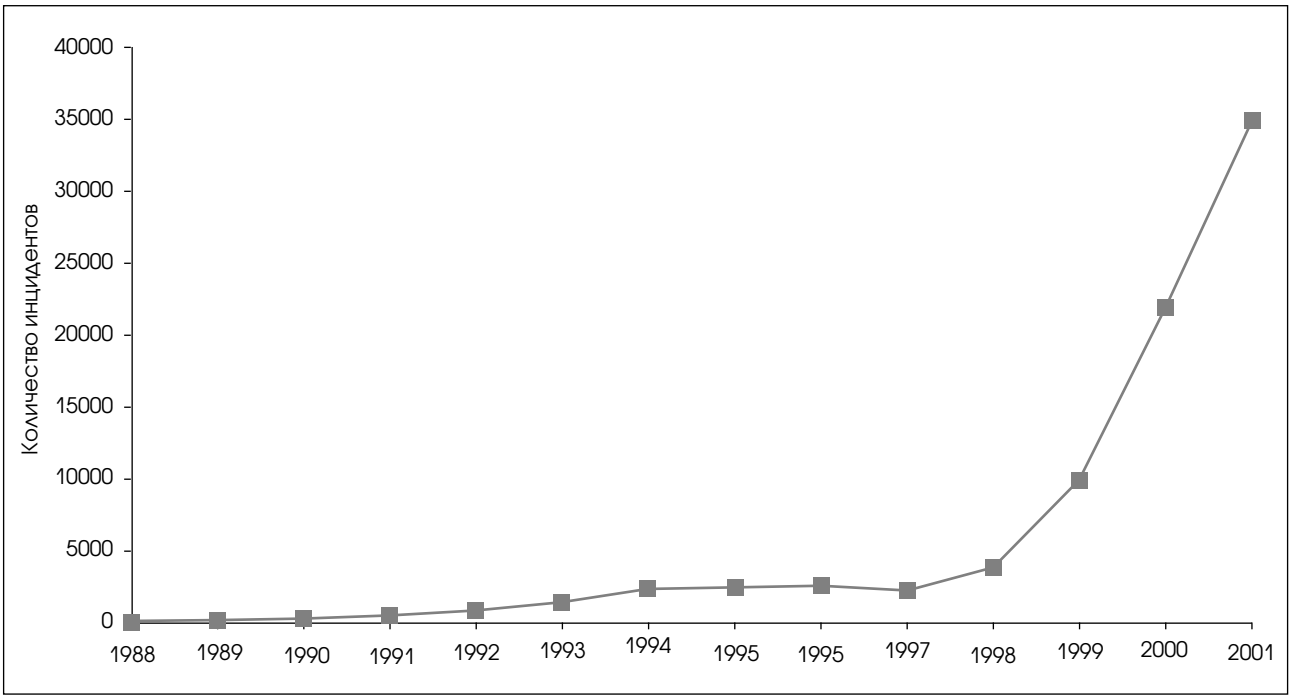


Рис. 21. Рост количества зарегистрированных инцидентов, связанных с незаконным вторжением в информационные ресурсы США

оценкам США ежегодно несут финансовые потери в сумме $5 млрд. из-за сбоев оборудования, потери и искажения данных, компьютерного мошенничества и хулиганства, связанных с нарушением регламента использования информационных систем и сетей.

Из 282 выборочных проверок соблюдения мер информационной безопасности в правительственных учреждениях и ведомствах США 19 относились к секретной информации. Из них 15 (79%) были связаны с прямым ущербом деятельности организации, 7 (37%) имели отношение к доступу к файлам (чтению, изменению и уничтожению данных и программ, отказу в обслуживании или подключению). По оценкам специалистов из 1004 происшествий, связанных с информационными системами, 164 носили уголовный характер. При этом 116 (87%) происшествий были непосредственно связаны с сотрудниками[43].

В связи с этим в последнее время все чаще звучат голоса в пользу лишения администраторов сетей и баз данных их главной привилегии — монопольного права распоряжаться всеми ресурсами, поскольку потенциальная возможность злоупотребления служебным положением этой категорией служащих может иметь самые серьезные последствия. Выход из создавшегося положения видится в применении классического правила «двух ключей», когда только двое, а возможно трое и более людей владеют полной, исчерпывающей информацией о системе безопасности информационной системы (сети), а следовательно, и могут изменять порядок доступа к ее ресурсам. Тем самым риск раскрытия секретности существенно снижается, хотя никто не может поручиться за то, что двое или трое человек не смогут вступить в преступный сговор, если они будут в этом так или иначе заинтересованы.

Интересно и то, что в конечном итоге движет людьми, пытающимися под страхом уголовного наказания пробиться сквозь многочисленные «стены», «экраны» и «шлюзы» с тем, чтобы добраться до заветной для них информации. Среди множества мотивов и причин, толкающих хакеров на компьютерные преступления, эксперты[44] выделяют две основные группы: личные и корпоративные (рис. 22).

К первой группе относятся такие личные мотивы как любопытство, месть, меркантильность и вандализм. Последнее, по мнению специалистов, скорее свидетельствует о патологии в психике личности и проявляется на протяжении всей жизни человека как самоутверждение через разрушение, в то время как первые три являются проявлением естества человеческой природы, претерпевшей мало изменений за последние несколько тысяч лет. Корпоративные мотивы, а вернее цели групповых интересов связаны в основном с конкуренцией, разведкой (шпионажем) и военным превосходством и ,в конечном счете, находятся в сфере финан-

[43] Critical infrastructure protection. Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities. GAO. September 12, 2001.
[44] State of the Practice of Intrusion Detection Technologies, CMU/SEI-99-TR-028, ESC-99-028 January 2000.

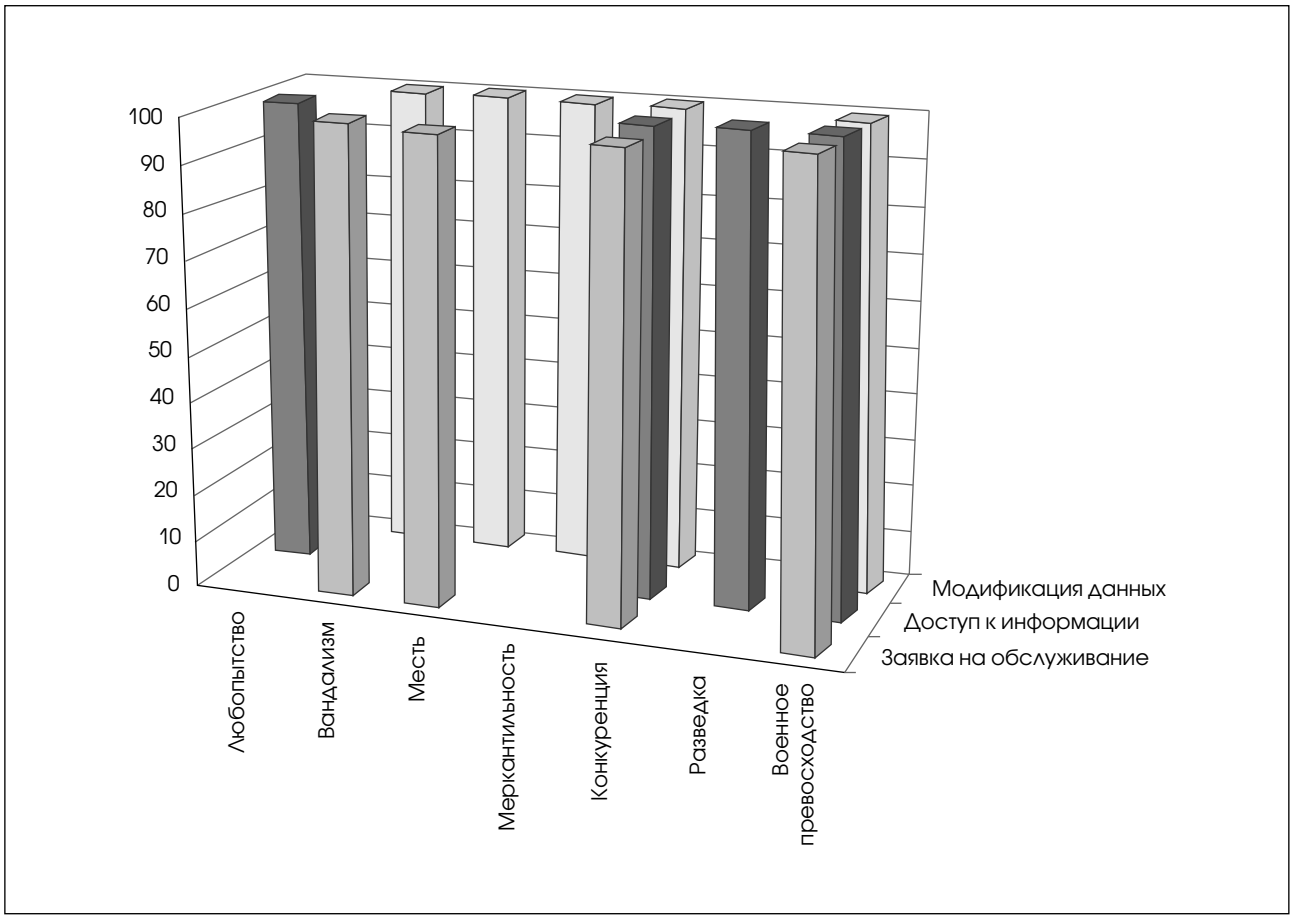


Рис. 22. Структура мотивов и последствий вторжения хакеров в информационные ресурсы

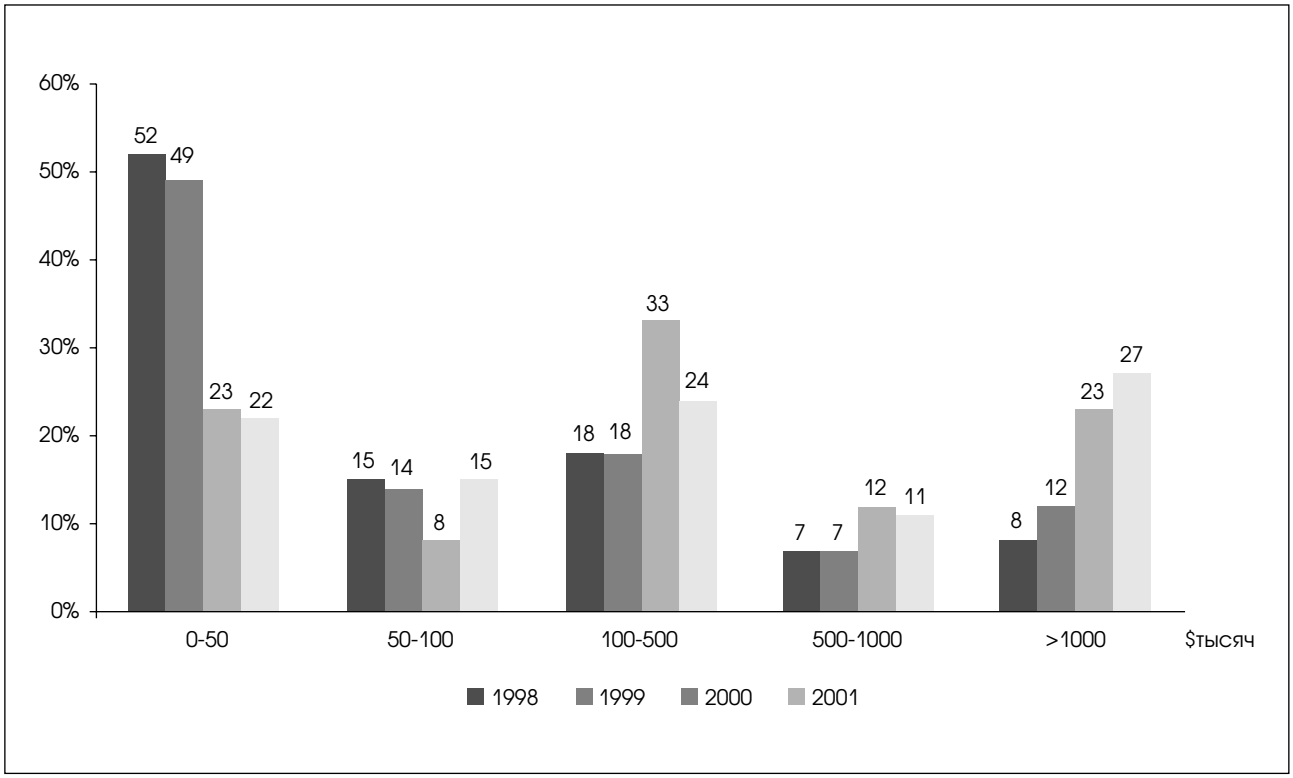


Рис. 23. Динамика структуры затрат на информационную безопасность в частном секторе США

совых, производственно-экономических, научно-технических и военно-политических интересов государств, корпораций и компаний, пытающихся таким образом решить проблему безопасности в бизнесе, торговле, дипломатии и вооруженном противоборстве.

Заметим, что последствия реализации как личных, так и групповых мотивов, с точки зрения информационной безопасности объекта преступных устремлений (например, информационной системы банка или инфраструктуры государства) имеют много общего. В целом их можно свести к трем основным составляющим процесса обработки информации: заявке на обслуживание, доступу к данным, манипуляции (модификации) данных. Характерно, что конкуренция и военное превосходство, как корпоративные мотивы, затрагивают все три составляющие данного процесса, имея своей конечной целью в различных сочетаниях вызвать отказ в обслуживании, затруднить или, напротив, получить доступ к данным, преднамеренно модифицировать данные в своих интересах.

При этом вандализм и месть, как личные побудительные мотивы, нацелены только на провоцирование ситуации отказа в обслуживании (например, отключение электроэнергии) и (или) модификацию данных (например, суммы доходов для уплаты налогов), и индифферентны к доступу информации, как таковому. В то же время любопытство и меркантильность толкают человека целенаправленно либо только на доступ к информации (например, к личной переписке), либо на модификацию данных (например, личного счета в банке).

Таким образом, рассмотренная нами структура мотивов поведения хакеров в пространстве достижимых целей нарушения информационного процесса может являться основой для последующей разработки модели компьютерного преступления.

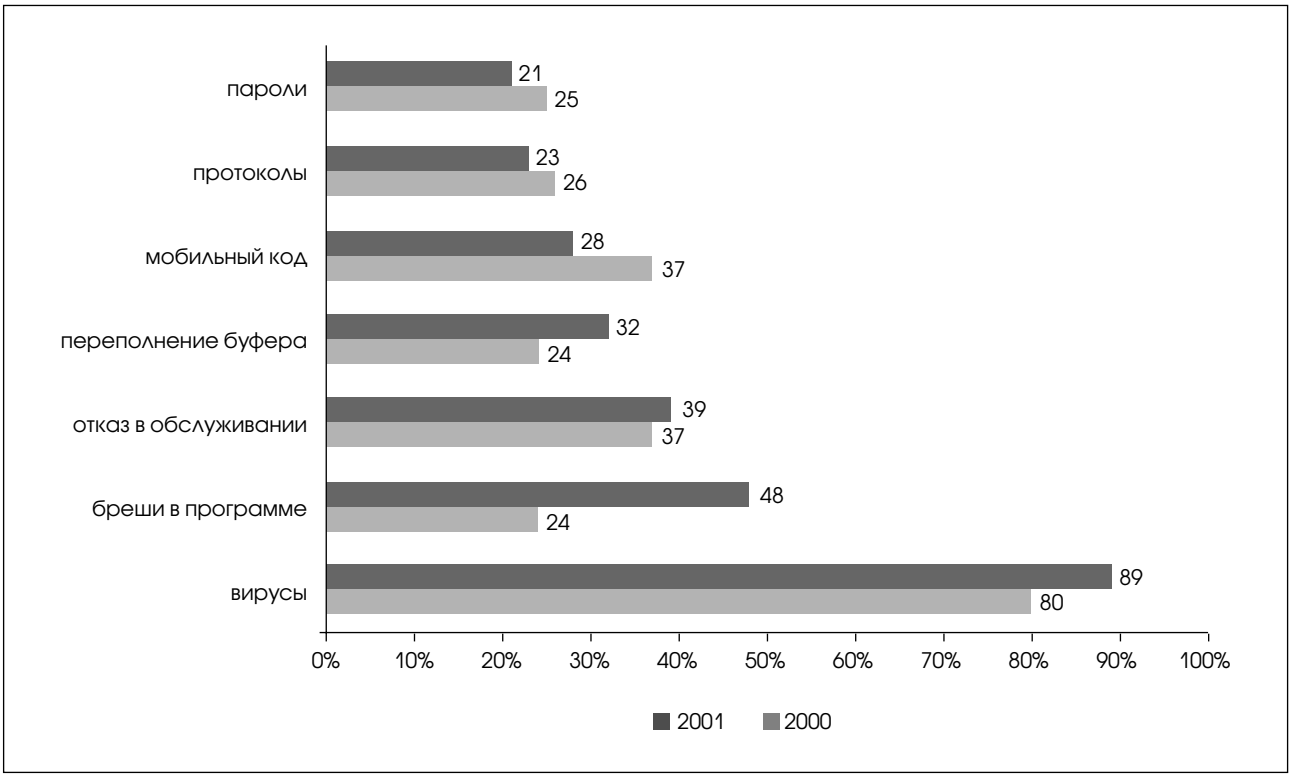


Рис. 24. Динамика структуры внешних угроз информационной безопасности

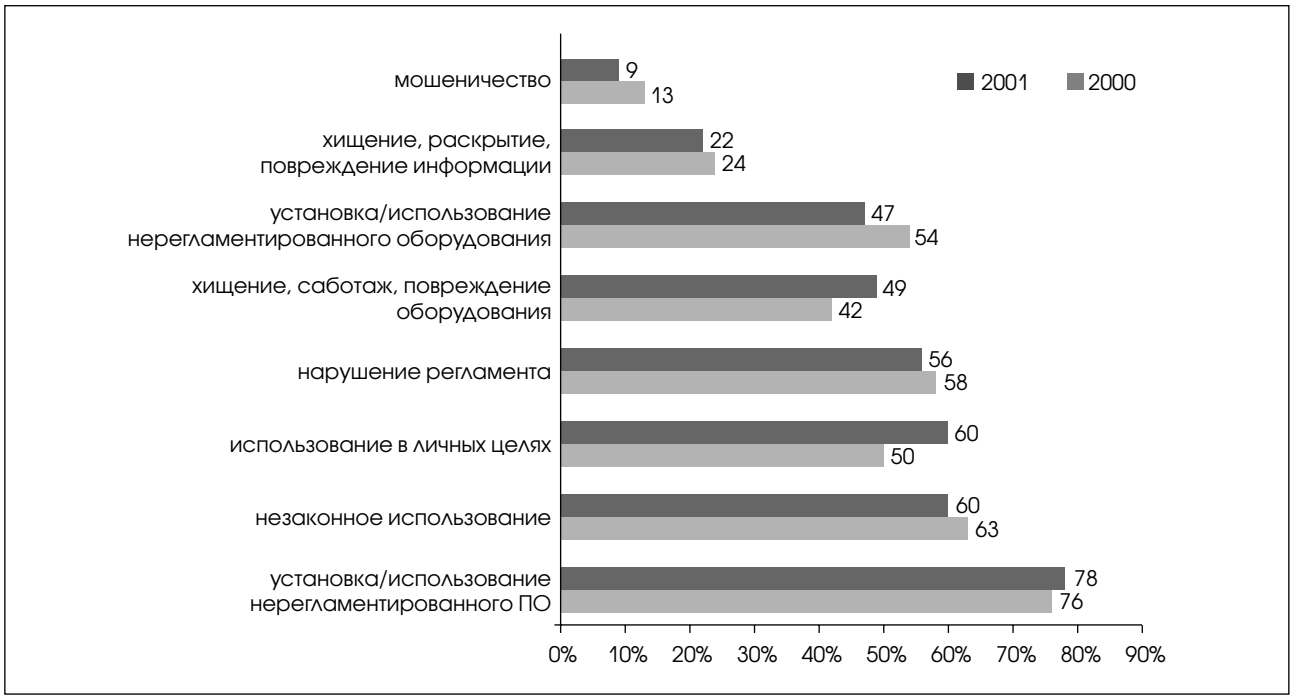


Рис. 25. Динамика структуры внутренних угроз информационной безопасности

Внешние и внутренние угрозы информационной безопасности

Анализ тенденций финансирования программ в области ИБ в частном секторе (рис. 23) показывает, что доля организаций, увеличивших за последние четыре года свои годовые затраты в сумме свыше $1 млн., увеличилась с 8% в 1998 г. до 27% в 2001 г., т.е. более чем в 3 раза. При этом количество организаций, затративших за год на ИБ менее $50 тыс. снизилось соответственно за этот период с 52% до 22%, т.е. более чем в 2 раза. Какие же причины, а вернее угрозы ИБ побуждают предпринимателей расходовать эти деньги?

Согласно проведенным в США в период с июля по август 2001 года исследованиям[45] на основе выборочного online опроса 2500 специалистов в области ИТ были получены следующие экспертные оценки характера и степени внешних и внутренних угроз ИБ, которые вызывают повышенную озабоченность у всех категорий персонала, независимо от занимаемого положения, возраста и пола.

Среди внешних угроз ИБ (рис. 24) согласно полученным результатам исследований за последние 2 года возрос практически в 2 раза процент инцидентов, связанных с использованием так называемых брешей в системном программном обеспечении для несанкционированного проникновения через Интернет в информационные ресурсы, на 10% увеличилось количество случаев нарушения нормальной работы из-за влияния программ-вирусов, на 2% увеличилось количество отказов в обслуживании, связанных фактически на треть (до 32%) с переполнением буфера при спамах в электронной почте.

Наибольшую проблему представляют происшествия, связанные с отказом в обслуживании (DOS — Denial-of-Service), поскольку в результате их негативного проявления организация, как правило, на длительное время теряет доступ к ресурсам и услугам Интернета. Так в результате одного из проведенных исследований в США в 2001 г. в течение трех недель наблюдались и фиксировались результаты и последствия свыше 12 тысяч атак (нападений, вторжений) на 5 тысяч хост-ЭВМ в Интернете, принадлежащих 2 тысячам организаций[46]. Анализ этой статистики выявил, что в 90% случаях продолжительность отказа в обслуживании по времени достигала 1 часа, что представляет серьезную опасность для предприятий так называемого непрерывного цикла работы (транспорт, энергетика, связь, неотложная медицинская помощь и др.).

Анализируя структуру внутренних угроз (рис. 25), эксперты отмечают, как наиболее серьез-

[45] 2001 Industry Survey — Information Security, October 2001.
[46] Managing the Threat of Denial-of-Service Attacks, CERT® Coordination Center, October 2001.

ные с точки зрения нарушения системы мероприятий в области ИБ, имевших место за последние два года, такие негативные проявления человеческого фактора в работе персонала как самовольная установка и использование нерегламентированного ПО (до 78% внутренних происшествий), увеличение случаев использования оборудования и ресурсов в личных целях (на 10%). Одновременно отмечается снижение на 7% количества случаев, связанных с установкой и использованием нерегламентированного оборудования вследствие ужесточения контроля со стороны администрации.

Интересно, что эти же тенденции проявляются и в военной области. Проводившаяся в феврале 2001 г. Службой генерального инспектора выборочная проверка условий эксплуатации программного обеспечения, установленного на объектах информационной инфраструктуры МО, показала, что даже в Пентагоне, где действуют жесткая дисциплина и порядок, имеют место серьезные нарушения правил информационной безопасности.

В частности, в нарушение официальных регламентирующих документов (DOD Instruction 5200.40, DOD Directive 5200.28), устанавливающих «личную ответственность со стороны персонала за каждым закрепленным программным продуктом», далеко не все используемые системные и прикладные приложения имеют своих постоянных владельцев. Кроме того, несмотря на существующий порядок, определяющий сроки эксплуатации приложений после их обязательной сертификации, распространена практика так называемых «летучих голландцев» — не учтенных программ и программ с просроченными сертификатами.

Результаты проверки оказались для руководства Пентагона не утешительными: из 4939 приложений, учтенных в базе данных Управления информационных систем МО, были идентифицированы как уникальные (не повторяющиеся по названию) — 1365, из которых только 36,7% полностью удовлетворяли требованиям ИБ (имели сертификаты и ответственных за эксплуатацию), 40% частично удовлетворяли этим требованиям, а 23,3% не удовлетворяли полностью[47]. По мнению экспертов, наличие такого большого количества (288) программных продуктов, не имеющих необходимых сертификатов и ответственных за их эксплуатацию сотрудников, несет в себе потенциальную угрозу для безопасности не только военной, но и национальной инфраструктуры в целом.

Вот почему для американских военных стал уже по существу хрестоматийным лозунг «народ и армия — едины», стирающий во многом условные грани между чисто военными и гражданскими аспектами ИБ и стимулирующий взаимный обмен опытом, технологиями и стандартами между государственным и частным сектором.

Подведем итоги

Обилие фактов, цифр, диаграмм и схем, представленных в данной статье, может привести в замешательство даже самого искушенного читателя, справедливо пытающегося отыскать тот заветный бугорок в океане информации, встав на который можно охватить всю картину в целом. Ибо сказано в Библии — «многие знания умножают печали человеческие», на что Козьма Прутков, как известно, изрек еще более авторитетно — «нельзя объять необъятное». Увидеть скрытый порядок и закономерность в видимом хаосе нам поможет волшебная палочка-выручалочка — математическая статистика, прибегнуть к которой автор решился после долгих и мучительных философских размышлений о смысле жизни — to be or not to be.

На основе статистического анализа бюджетных затрат на информационные технологии и информационную безопасность, а также с учетом данных независимых комиссий, в которых частично содержатся сведения об общем количестве информационных систем, автором были построены регрессионные модели, связывающие между собой эти параметры в целом.

Используя полученную на основе регрессионного анализа статистических данных математическую модель, можно, в частности, определить количество критически важных информационных систем (ИС), как в целом по стране, так и в отдельно взятом министерстве или ведомстве. Распределение количества критически важных ИС и их удельного веса в общем количестве ИС по ведомствам в процентном соотношении приведено на рис. 26 и рис. 27.

Анализ диаграммы показывает, что наибольшее количество критически важных ИС находится в Пентагоне (49%), а среди гражданских ведомств — у НАСА (18%), что не удивительно, принимая во внимание известную всем обеспокоенность американских военных по поводу хакеров и повышенный интерес американских ученых к геофизическим и космическим проблемам.

Однако, если посмотреть на этот феномен в другом ракурсе, с точки зрения удельного веса, за-

[47] Implementation of DOD information security policy for processing accomplished at defense enterprise computing centers Report No. D-2001-183, September 19, 2001.

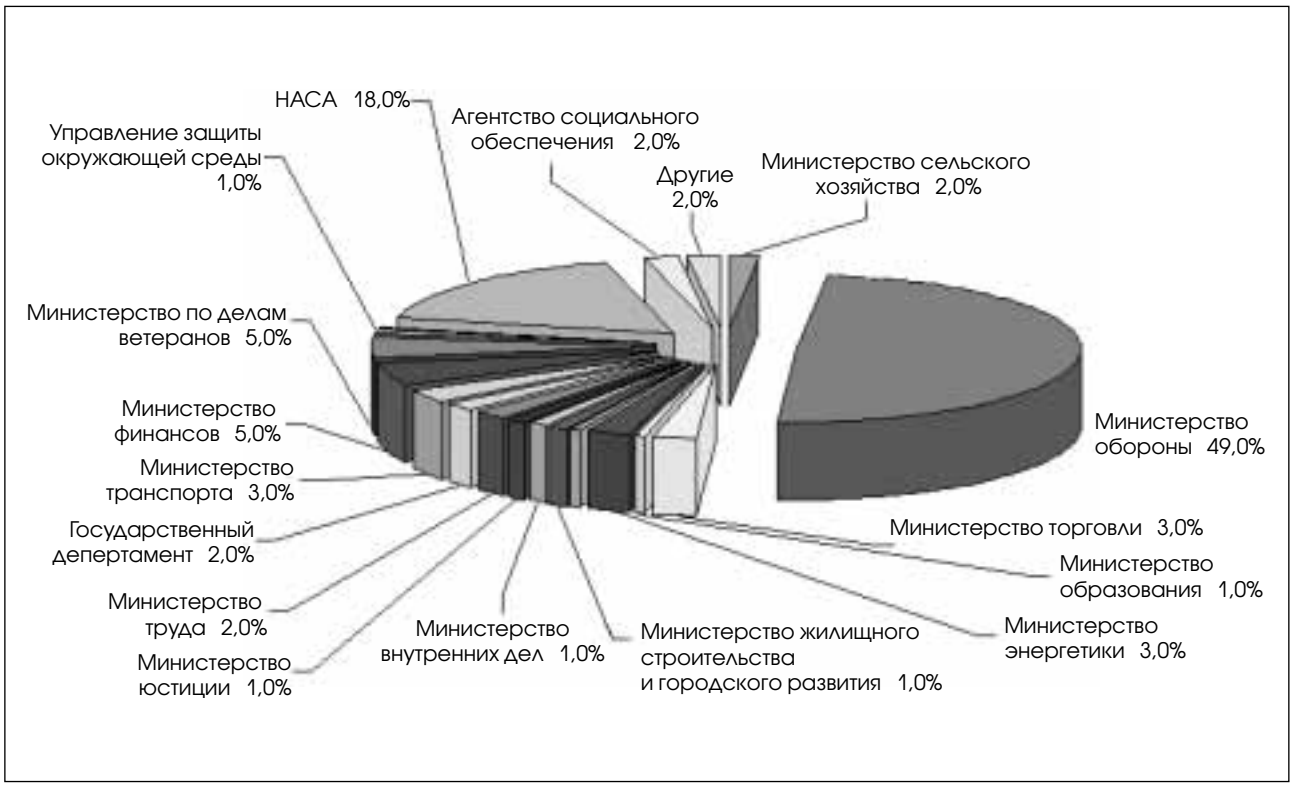


Рис. 26. Распределение количества критически важных информационных систем по министерствам и ведомствам США

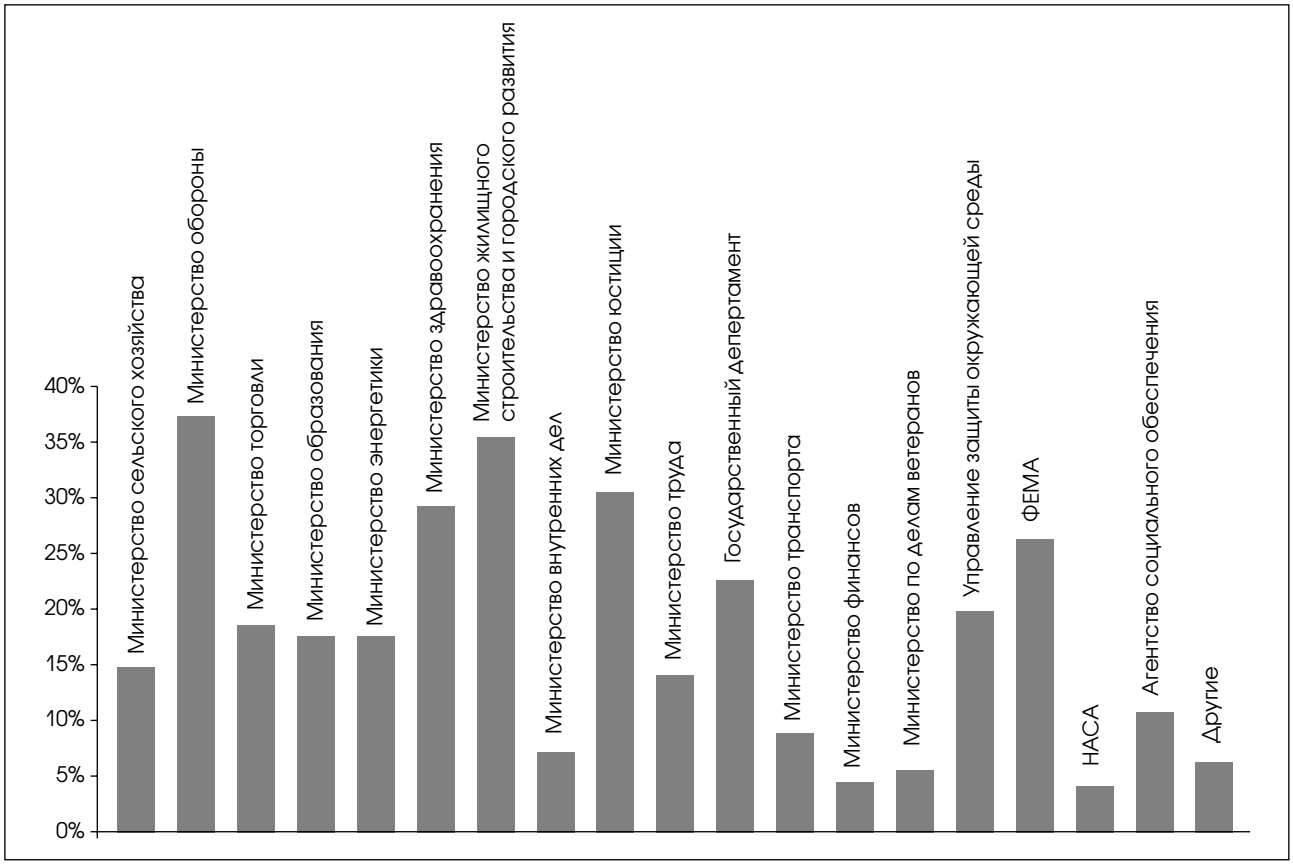


Рис. 27. Удельный вес критически важных информационных систем в общей совокупности информационных систем министерств и ведомств США

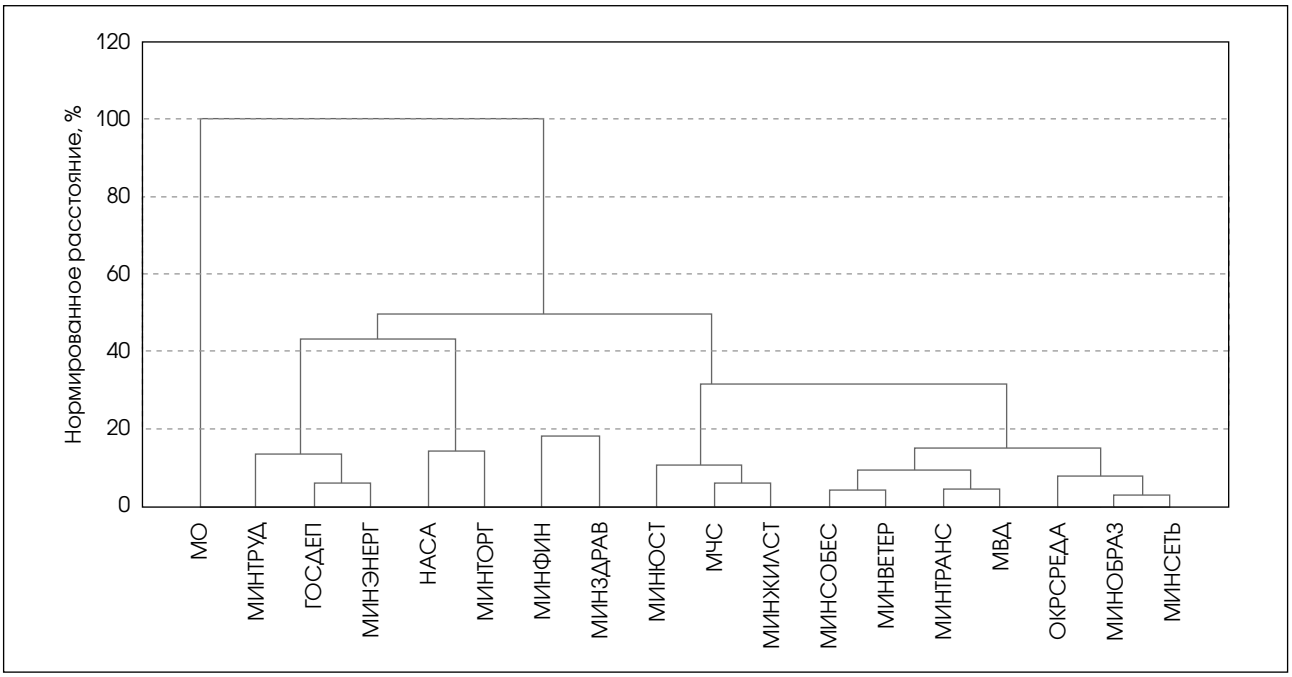


Рис. 28. Таксономия информационных ресурсов федерального правительства США

нимаемого критически важными ИС в общей совокупности ведомственных ИС, то перед нами предстанет несколько иная картина. Наряду с Пентагоном (37%) по этому показателю практически на равных стоит Минжилстрой (35%), следом за которыми буквально в затылок выстроились Минюст (30%), Минздрав (29%) и МЧС (26%). Иными словами, чтобы хорошо воевать, строить, судить, лечить и спасать американцы не просто используют информационные технологии, системы и сети, а уже не могут без них обойтись при всем своем желании.

Интересно, что приведенные выше и полученные на основе моделирования данные хорошо согласуются с результатами другого независимого исследования рынка ИТ, в котором утверждается, что «около 30% всех серверов правительственных учреждений США связано с обработкой транзакций реляционных баз данных»[48]. Именно эти серверы и входят в число так называемых критически важных (mission-critical information systems)[49] информационных систем как в военной, так и гражданской сфере государственного управления.

На основе кластерного анализа, который позволяет группировать данные вокруг нескольких центров в многомерном пространстве, можно построить таксономию (классификацию) объектов информационной инфраструктуры, используя все перечисленные выше показатели. Полученная на основе метода Уорда для евклидовых метрик таксономия (рис. 28) дает читателю весьма наглядное представление об особенностях построения и составе групп информационных ресурсов федерального правительства США. Заметим, что ресурсы пяти ведомств (Минтруда, Госдепа, Минэнерго, НАСА и Минторга) оказываются объединенными в одну общую группу, в то время как ресурсы 12 остальных — в другую, что наводит на размышления не только об уровне и качестве жизни американцев, но и первопричинах этого устойчивого во времени феномена — достойной зарплате по квалифицированному труду, на основе дешевых иностранных энергетических ресурсов, благодаря гибкой внешнеполитической линии, торговой экспансии и космическим технологиям. С другой стороны, ресурсы Пентагона (МО) уравновешивают, а вернее гарантируют работу ресурсов всех гражданских ведомств, что не требует пояснений. Более детальный анализ данной таксономии автор предлагает выполнить читателю самостоятельно, не забывая о том, что от 80 до 90% информационных ресурсов США контролируются частным капиталом.

Используя полученную таксономию и ее матрицу расстояний между объектами, которые отражают проведенный нами кластерный анализ наиболее важных элементов и их взаимоотношений, можно на основе уже другого метода — анализа иерархий[50] определить собственные значения векто-

[48] Value of Total Cost of Ownership in the Federal IT Market, Kevin Plexico INPUT, April 6, 2001.
[49] FY 2001 DOD information security status for government information security reform. Report No. D-2001-184, September 19, 2001.

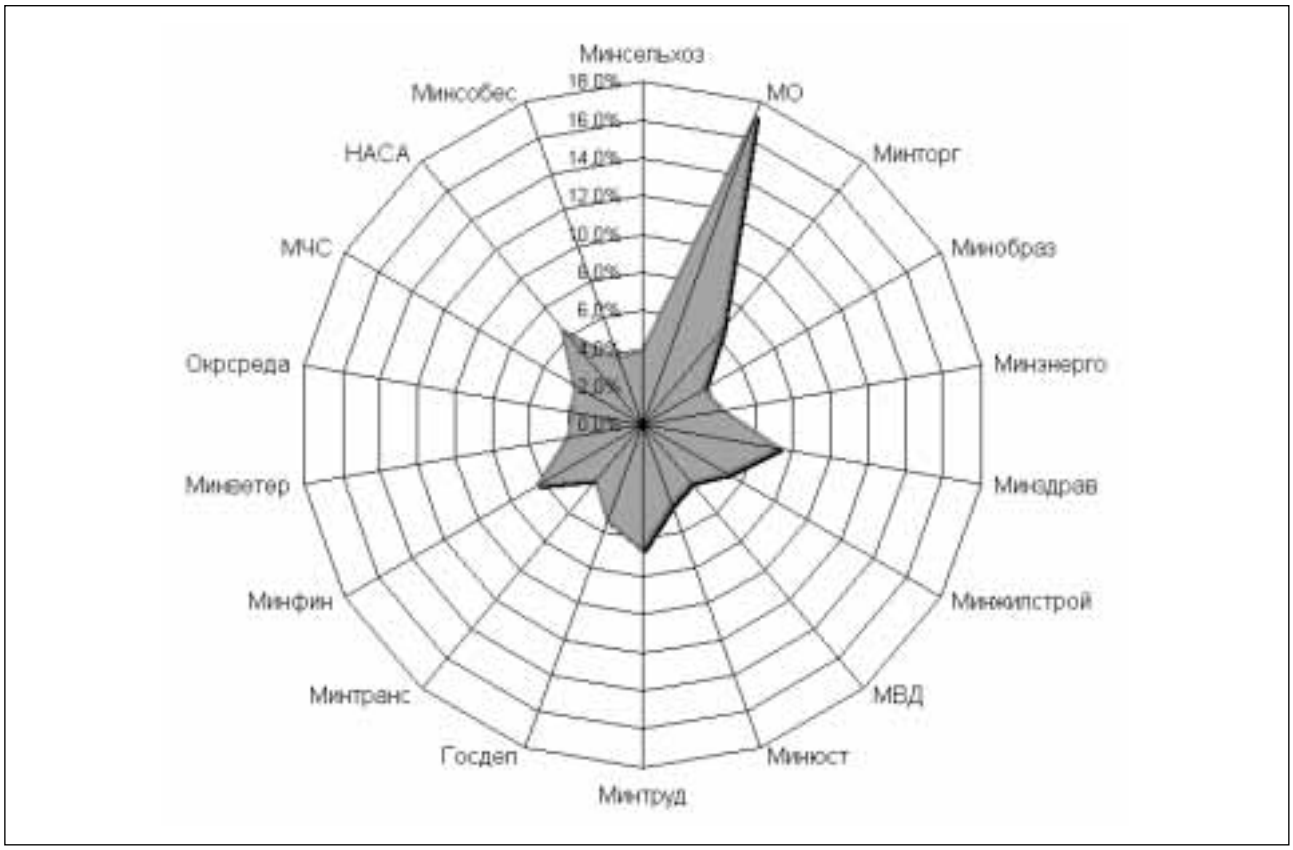


Рис. 29. Иерархия информационных ресурсов федерального правительства США

ра приоритетов иерархии информационных ресурсов федерального правительства США, т.е. степень их влияния на инфраструктуру государства в целом (рис. 29). На диаграмме хорошо видно, что наивысшим приоритетом в настоящее время пока еще пользуется военное ведомство (МО), вклад которого условно соответствует относительной величине порядка 17% в общей массе информационных ресурсов федерального правительства. Характерно, что в представленной «звезде» рангов или приоритетов информационных ресурсов ведомств уже знакомые нам НАСА (6,5%), Минторг (6,5%), Минтруд (6,5%), Минфин (6,3%), и Минздрав (7,2%) довольно энергично, образно говоря, «тянут одеяло на себя» в борьбе за свое существование, сообразуясь при этом с интересами национальной безопасности. Очевидно, что имеющийся на сегодня перекос в приоритетах в конечном итоге будет устранен, и «звезда» вначале примет пропорциональные очертания, а затем будет постепенно трансформироваться в правильный многоугольник, символизирующий собой цель информатизации американского общества.

И все же наибольший интерес для нас представляет не сама структура затрат, классификация ресурсов, распределение в ней приоритетов и адекватное ей количество информационных систем, а та закономерность (пропорция), по которой происходит увеличение ассигнований на развитие ИТ и обеспечение ИБ в целом. Одна из этих моделей, представляющая собой трехмерное изображение аппроксимирующей поверхности множественной нелинейной регрессии представлена на рис. 30.

Автор взял на себя смелость дать этой поверхности соответствующее ее физическому смыслу красивое и звучное название — «склон безопасности».

Говоря языком альпинистов, американцы упорно карабкаются вверх по этому склону по тропе Клинтона в надежде достичь той заветной вершины Буша-младшего, с которой они смогут беспечно созерцать крошечные фигурки шпионов, террористов, мошенников, жуликов и хакеров, тщетно пытающихся добраться на недосягаемую для них высоту от подножия Буша-старшего, в чье правление и вышел на свет пресловутый призрак информационной войны.

Двухмерная проекция этой модели (вид сверху) представлена на рис. 31.

Но как известно, чем выше в гору, тем круче подъем и тяжелей дышать, да и страховка нужна хорошая: не равен час сойдет лавина. О том, что

[50] Т.Саати Принятие решений. Метод анализа иерархий. — «Радио и связь», Москва, 1993 г.

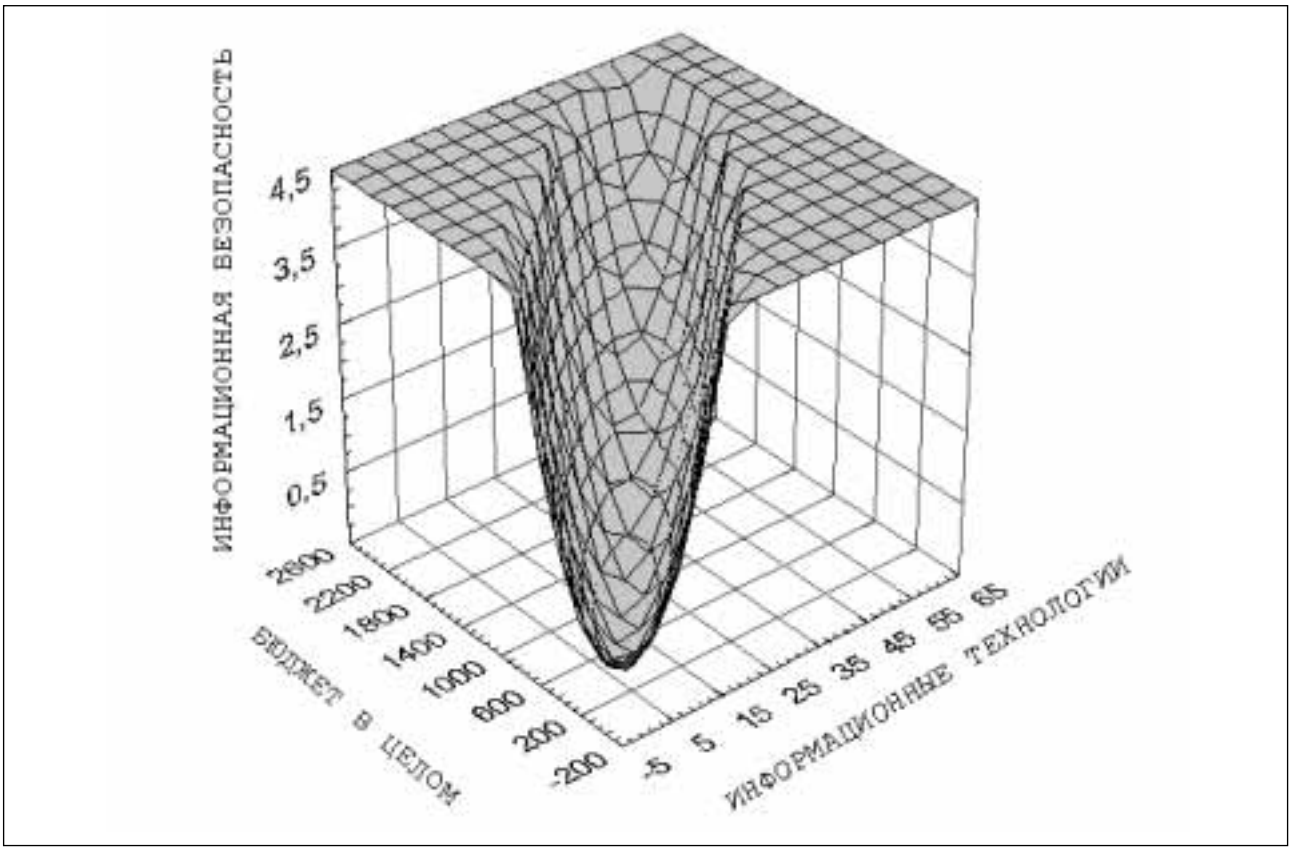


Рис. 30. Трехмерная регрессионная модель бюджетных затрат США на информационные технологии и информационную безопасность в $млрд

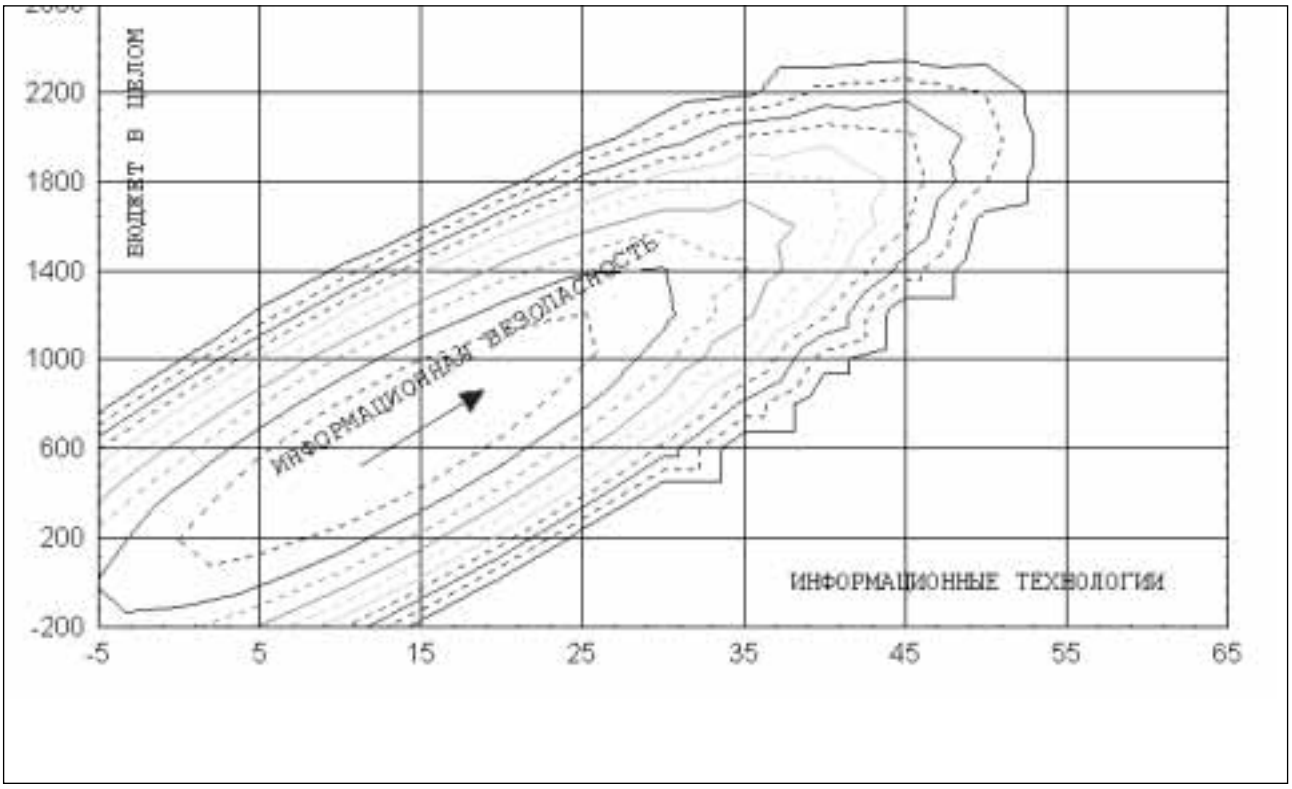


Рис. 31. Проекция трехмерной регрессионной модели бюджетных затрат США на информационные технологии и информационную безопасность в $млрд

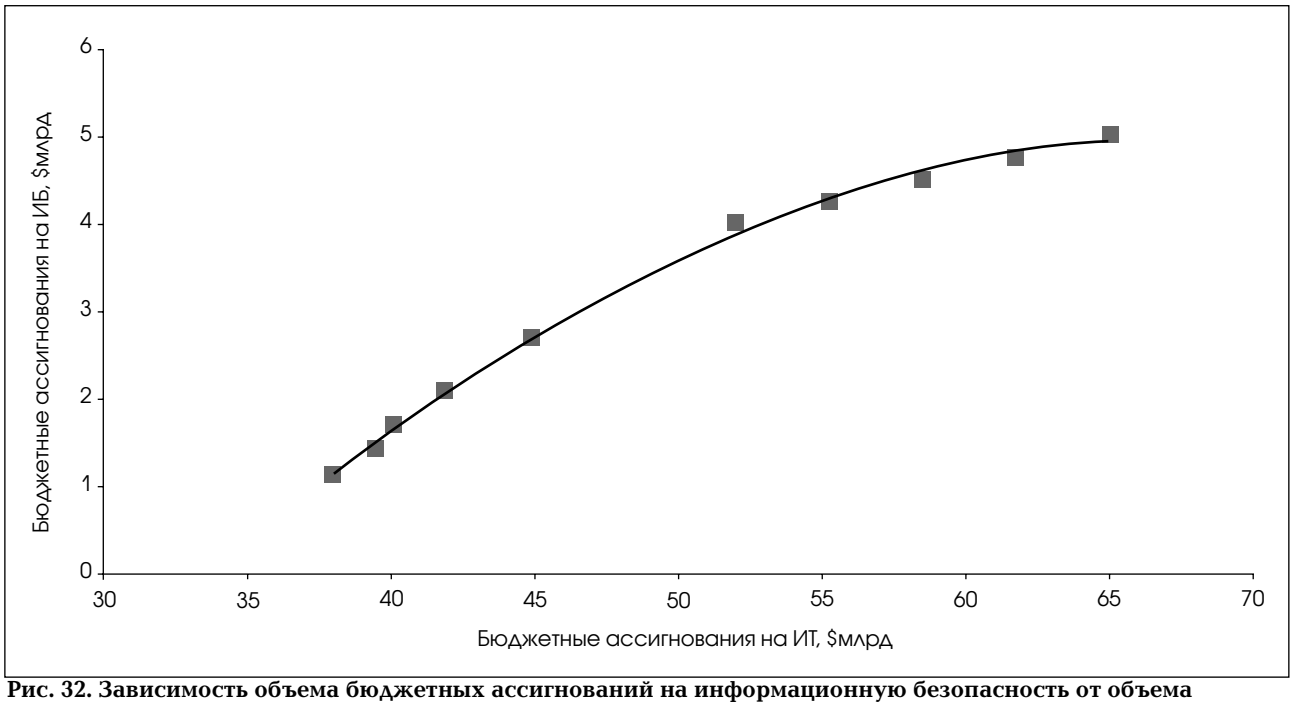


Рис. 32. Зависимость объема бюджетных ассигнований на информационную безопасность от объема ассигнований на информационные технологии в США

подъем уже идет на пределе сил альпинистов говорит не только тяжелый груз дефицита госбюджета, но и замедление этого восхождения, прогнозируемый пик которого отчетливо виден на следующем графике (рис. 32).

Отметка в $5 млрд. и есть та цена вопроса, превышение которой означает тратить ежегодно на информационную безопасность больше, чем можешь потерять от хакеров. Для сравнения, на решение «проблемы 2000» за 5 лет было израсходовано в общей сложности $8 млрд.

Читателю будет не безынтересно узнать, что использованные в данной работе классические методы математической статистики в настоящее время в США переживают подлинный бум, сформировавшись в мощное прикладное направление стратегического анализа больших массивов данных в интересах достижения так называемого «превосходства в принятии решений» (decision superiority) в самых различных областях (банковском деле, торговле, микробиологии, медицине, метеорологии, производстве и др.). Американская компания StatSoft, лидер среди разработчиков программных продуктов в этой области, определяет понятие «добыча данных» (data mining) как процесс аналитического исследования больших массивов информации с целью выявления определенных закономерностей и систематических взаимосвязей между переменными, которые затем можно применить к новым совокупностям данных. После событий 11 сентября особый интерес к технологии «добычи данных» проявляют американские спецслужбы (ЦРУ и ФБР), которые за последнее время справедливо подверглись серьезной критике за низкую эффективность использования информации в интересах оперативного прогнозирования и своевременного предотвращения террористических актов[51].

Итак, подведем итог всем нашим рассуждениям о бюджете, зарплате, кадрах, технологиях и безопасности. Многовековой человеческий опыт говорит нам о том, что еще не было таких проблем, для решения которых рано или поздно не создавались самые совершенные научно-технические решения, какими бы дорогими и разорительными они не были: достаточно вспомнить американскую программу полетов на Луну «Аполлон» или российскую программу «Буран» — аналог американского «Шатла», открытых по престижным и закрытых по экономическим соображениям.

Но этот же опыт одновременно и предупреждает нас — за новыми решениями старых проблем скрываются неизвестные и быть может еще более сложные проблемы и новые угрозы, связанные с ними. Как утверждают специалисты ведущего производителя микроэлектроники — компании Интел, закон ее основателя Гордона Мура[52], сформулированный им еще в середине 60-х годов прошлого века, сохранит свою актуальность как минимум на ближайшие 25-30 лет, а это значит, что

[51] FBI counting on IT vs. Terrorism, FCW, May 20, 2002.

персональный компьютер с процессором, работающим на тактовой частоте 30 ГГц и выполняющим 1 триллион (10^{12}) операций в секунду появится в продаже уже в 2010 г.[53] Какими возможностями будет располагать по своему усмотрению пользователь этого настольного Cray-XP не знает даже Интел: чужая душа — потемки.

Кто знает, не наступит ли тогда время строгих ограничений и запретов на распространение программных продуктов с алгоритмами векторной обработки данных для домашних суперЭВМ, за инсталляцию которых в США будут привлекать к уголовной ответственности в интересах информационной безопасности национальной инфраструктуры.

И все же пора сказать о главном — смотреть и злорадствовать, как твой сосед восстанавливает, ремонтирует и перестраивает дом после пожара, и считать при этом чужие деньги — дело не такое уж и хитрое, а вот извлекать уроки и делать выводы это удел бережливых и дальновидных, тем более, что таких денег нам с вами не видать в обозримом будущем, а проблем у нас и самих хватает.

В конце концов русский человек и без компьютера проживет — крепкий здоровьем и сметливый умом будет, а вот американец ...

Когда верстался номер:

В верхнюю палату Конгресса США (после рассмотрения в сенатской Комиссии по торговле, науке и транспорту) поступил новый законопроект S2182 об увеличении финансирования НИОКР в области информационной безопасности с $880 млн. до $977 млн. (11%) на предстоящие пять лет. Инициатор законопроекта сенатор Рон Вайден (шт. Орегон) предложил создать специальный координирующий орган при Национальном институте стандартов и технологий США, входящем в Министерство торговли — Управление программ информационной безопасности (Office for Information Security Programs), который будет осуществлять контроль за всеми работами, выполняемыми совместно с Национальной академией наук в области безопасности информационных сетей и их программного обеспечения, выделяя специальные гранты университетам для совместных исследований с промышленностью[54] .

Источники

1. Блицкриг как предтеча информационной войны, www.agentura.ru, 2001.
2. В США принят план защиты информационных систем. JetInfo, №8 (87), 2000.
3. Гражданская оборона информационных ресурсов. Известия, №95 (25933) от 31.05.2001.
4. Новые приоритеты в информационной безопасности США. Jet Info, №10, ноябрь, 2001 г.
5. Пентагон готовится к информационной войне, «Красная звезда», 17 октября 1995 г.
6. Т.Саати. Принятие решений. Метод анализа иерархий. — «Радио и связь», Москва, 1993 г.
7. A Case Study in Survivable Network System Analysis CMU/SEI-98-TR-014 ESC-TR-98-014 September 1998.
8. A Report by a Panel of the National Academy of Public Administration for the Chief Information Officers Council and the Administrative Office of the U.S Courts, August 2001, The Transforming Power of Information Technology: Making the Federal Government an Employer of Choice for IT Employees.
9. Border agency overhaul proves tricky for Bush team. Government Executive Magazine, 29 March 2002.
10. Budget of the US Government, FY 2002. Office of Management and Budget.
11. Computer security. Improvements Needed to Reduce Risk to Critical Federal Operations and Assets. GAO. November 9, 2001.
12. Critical infrastructure protection. Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities. GAO. September 12, 2001.
13. Defending America's Cyberspace. National Plan for Information Systems Protection, Version 1.0. An Invitation to a Dialogue, The White House 2000.
14. Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations, MILCOM-2001.
15. Defining IT Security Requirements for Federal Systems and Networks Employing Common Criteria Protection Profiles in Key Technology Areas NIST-NSA Technical Working Group.
16. DOD gets good marks overall, Federal Computer Week, 4 February, 2002.
17. Electronic Government. Challenges to Effective Adoption of the Extensible Markup Language. Report to the Chairman, Committee on Governmental Affairs, U.S. Senate GAO-02-327, April 2002.

[52] Каждые 18 месяцев плотность вентилей (транзисторов) на единицу площади кристалла микросхемы увеличивается в 2 раза.
[53] Intel exec: Moore's law keeps going and going. Government Computer News, 19 March 2002.
[54] Late changes to a security R&D bill call for NIST cybersecurity office, Government Computer News, 20 May 2002

18. FBI counting on IT vs. Terrorism, FCW, May 20, 2002.
19. FY 2001 DOD information security status for government information security reform. Report No. D-2001-184, September 19, 2001.
20. FY 2001 Report to Congress on Federal Government Information Security Reform. OMB, 2002.
21. GEIA Predicts Significant Growth in the Information Assurance Market, January 11, 2002.
22. Global Information Grid support to CINC requirements (DSC Study FY00-05, FY01-05).
23. Implementation of DOD information security policy for processing accomplished at defense enterprise computing centers Report No. D-2001-183, September 19, 2001.
24. Implementing the President's Management Agenda for E-Government, February 27, 2002.
25. Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense. Office of the Secretary of Defense August 27, 1999.
26. Information Assurance in Networked Enterprises: Definition, Requirements, and Experimental Results CERIAS, TR 2001-34 School of Industrial Engineering, No. 01-05 Purdue University January 2001.
27. Information sharing. Practices That Can Benefit Critical Infrastructure Protection. GAO .October 2001.
28. Information warfare TS 3600.1, DOD, 21 December 1992.
29. Intel exec: Moore's law keeps going and going. Government Computer News, 19 March 2002.
30. Managing the Threat of Denial-of-Service Attacks, CERT® Coordination Center, October 2001.
31. Mid-Career Hiring Trends Report. The Partnership for Public Service — February 22, 2002.
32. Modeling the Revolution in Military Affairs, Autumn/Winter 1998-99 / JFQ.
33. Navy sets up a network command. GCN 29 March 2002.
34. NET Guard would be a volunteer expert force. Government Computers News, January 21, 2002.
35. Network Centric Warfare Conference: Wednesday 19th & Thursday 20th September 2001, Waldorf Meridien Hotel, London.
36. Network-Centric Computing. Preparing the Enterprise for the Next Millennium. Computer Technology Research Corp. http://www.itworks.be/reports/.
37. On the definition of survivability. Department of Computer Science University of Virginia, June 2001.
38. Overview of Atteck Trends. CERT® Coordination Center. Carnegie Mellon University, 2002
39. Performance Information for Major IT Investments, February 4 2002, President's Budget for 2003,cross-reference Chapter 22 of the Analytical Perspectives Section, of the 2003 Budget. Page 1 of 89.
40. Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures (Main). Transition Office of the President's Commission on Critical Infrastructure Protection (PCCIP) and the Critical Infrastructure Assurance Office (CIAO).
41. Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'2000), Hilton Head Island, South Carolina, January 25-27, 2000.
42. Research on mitigating the insider threat to information systems. RAND. Conference Proceedings, August 2000.
43. State of the Practice of Intrusion Detection Technologies, CMU/SEI-99-TR-028 ESC-99-028 January 2000. Networked Systems Survivability Program.
44. Survivable Network Systems: An Emerging Discipline CMU/SEI-97-TR-013 ESC-TR-97-013 Software Engineering Institute Carnegie Mellon University Pittsburgh, May 1999.
45. Towards a National Strategy. Government Computer News, 29 March 2002.
46. The Anatomy of the Grid. Enabling Scalable Virtual Organizations. Ian Foster, Carl Kesselman, Steven Tuecke.
47. Using Information Technology To Transform The Way We Learn. Report to the President. February 2001.
48. Value of Total Cost of Ownership in the Federal IT Market, Kevin Plexico INPUT, April 6, 2001.
49. What is information warfare, National Defense University, August 1995.
50. 2001 Industry Survey — Information Security, October 2001.

Фотоматериалы перепечатаны из газеты «New York Times»

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

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Россия, 127006, 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