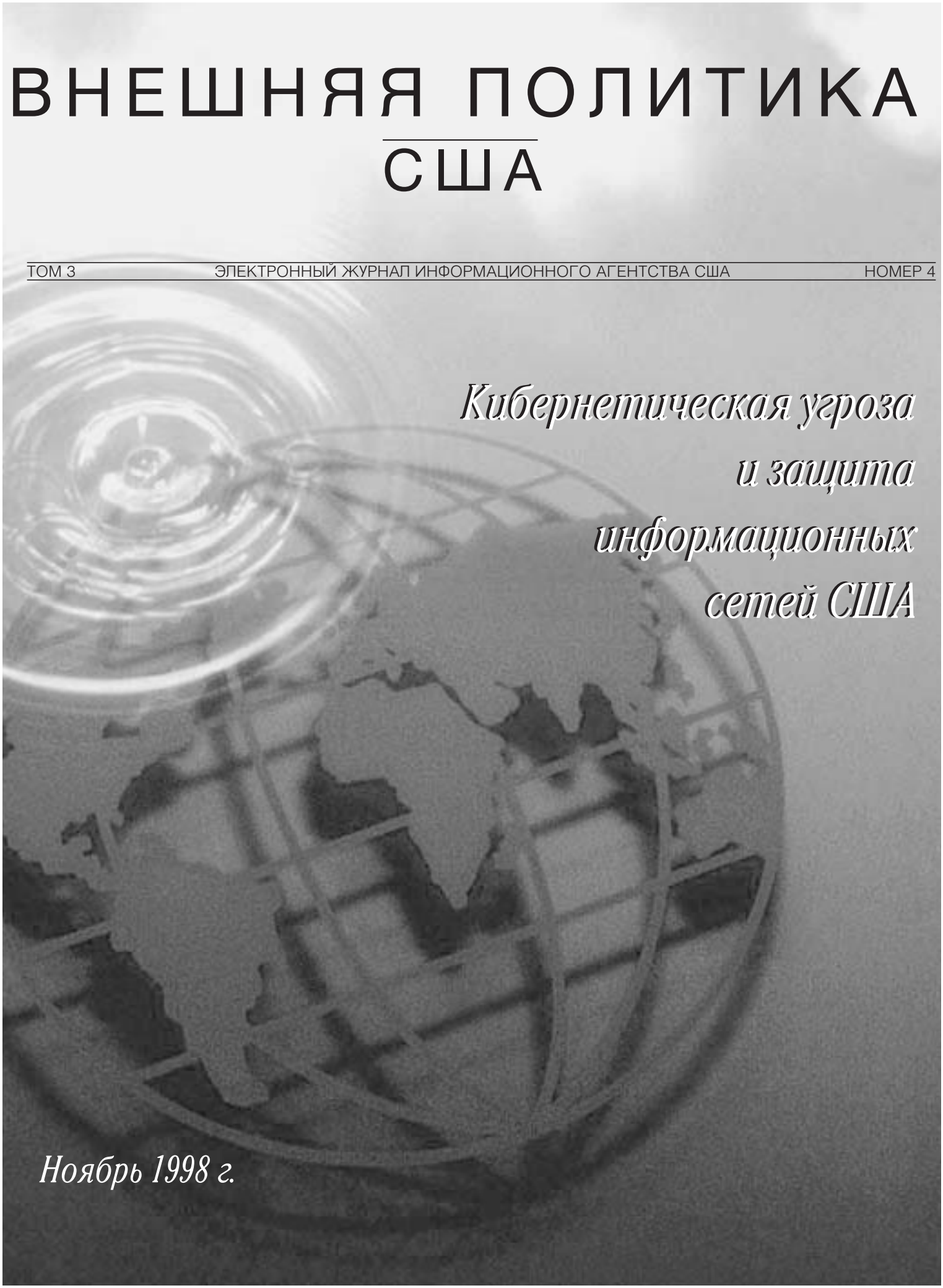
ВНЕШНЯЯ ПОЛИТИКА США

ТОМ 3 ЭЛЕКТРОННЫЙ ЖУРНАЛ ИНФОРМАЦИОННОГО АГЕНТСТВА США НОМЕР 4



Кибернетическая угроза и защита информационных сетей США

Ноябрь 1998 г.

ВНЕШНЯЯ ПОЛИТИКА
США

Кибернетическая угроза и защита информационных сетей США

«На пороге 21-го века наши противники расширили поля сражений – от физического пространства к кибернетическому… Вместо того, чтобы высаживаться на наши берега или посылать бомбардировщики, они могут предпринять кибернетические атаки против наших критически важных военных систем и нашей экономики… Если мы хотим, чтобы наши дети выросли в условиях безопасности и свободы, мы должны бороться с этими новыми угрозами 21-го столетия также решительно, как мы боролись со страшными угрозами нашей безопасности на протяжении нынешнего столетия».

Из выступления Президента Клинтона на церемонии торжественного вручения дипломов выпускникам Академии ВМС США
22 мая 1998 г.

Этот выпуск журнала «Внешняя политика США» посвящен реакции США на проблемы, с которыми мы раньше никогда не сталкивались – проблемы Информационного века. Официальные лица США, занимающие ключевые должности в правительственных организациях, рассказывают об инициативах, направленных на защиту американских информационных сетей от кибернетических атак и развитие сотрудничества между правительством и частным сектором в области выработки мер безопасности. Сенатор США сообщает о реакции Конгресса на дебаты по проблемам информационной войны, профессор рассказывает о том, как университеты откликнулись на новые приоритетные задачи страны, эксперт частного научно-исследовательского института дает широкую обзорную характеристику понятия и эволюции информационной войны, а специалисты частных корпораций делятся опытом сотрудничества американских компаний между собой и с правительством в целях удовлетворения потребностей в области безопасности в век кибернетики.

ВНЕШНЯЯ ПОЛИТИКА США

Электронный журнал Информационного агентства США

КИБЕРНЕТИЧЕСКАЯ УГРОЗА И ЗАЩИТА ИНФОРМАЦИОННЫХ СЕТЕЙ США

СОДЕРЖАНИЕ

ФОКУС

ОБОРОНА СТРАНЫ ОТ КИБЕРНЕТИЧЕСКОЙ АТАКИ: ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СРЕДЕ 6

Генерал-лейтенант Кеннет А. Минихэн
Директор Агентства национальной безопасности США

ЗАЩИТА ИНФОРМАЦИИ – ГЛАВНАЯ ЗАДАЧА НОВЕЙШЕГО ПЕРИОДА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ 10

Джон Хэмри
Заместитель министра обороны США

ИНТЕГРИРОВАННЫЙ ПОДХОД В ОТРАЖЕНИИ НОВЫХ УГРОЗ 13

Интервью с Джефри А. Ханкером, директором Управления безопасности инфраструктуры США

ПРОБЛЕМА 2000 ГОДА 19

Джон Коскинен
Председатель Президентского совета по компьютерной проблеме 2000-ого года

КОММЕНТАРИИ

ПРИЗРАКИ В МАШИНАХ? 21

МАРТИН ЛИБИЦКИ
ВЕДУЩИЙ НАУЧНЫЙ СОТРУДНИК НАУЧНО-ИССЛЕДОВАТЕЛЬСТКОГО ИНСТИТУТА РЭНД

ЧТО ВЫСШЕЕ ОБРАЗОВАНИЕ ПРОТИВОПОСТАВЛЯЕТ ИНФОРМАЦИОННОЙ ВОЙНЕ **26**

Чарльз У. Рейнольдс
Заведующий Отделением компьютерных наук Университета Джеймса Мэдисона

С ПОЗИЦИЙ ЧАСТНОГО СЕКТОРА

ОБМЕН ОПЫТОМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫГОДЕН КАК ЧАСТНОМУ, ТАК И ГОСУДАРСТВЕННОМУ СЕКТОРУ **30**

Интервью с Ховардом Шмидтом,
начальником Отдела информационной безопасности корпорации «Майкрософт»

СТРАТЕГИИ БОРЬБЫ С УГРОЗАМИ ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ **34**

Джеймс А. Лингерфелт
Консультант ІИМ по вопросам общественной безопасности

СПРАВКА: ЗАЩИТА ЖИЗНЕННО ВАЖНЫХ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ США **41**

Директива Президента США No. 63

КИБЕРНЕТИЧЕСКАЯ УГРОЗА И ЗАЩИТА ИНФОРМАЦИОННЫХ СЕТЕЙ США АННОТАЦИИ СТАТЕЙ **43**

Аннотации недавних статей

КИБЕРНЕТИЧЕСКАЯ УГРОЗА И ЗАЩИТА ИНФОРМАЦИОННЫХ СЕТЕЙ США ИЗБРАННАЯ БИБЛИОГРАФИЯ **44**

В фокусе – другие точки зрения

КИБЕРНЕТИЧЕСКАЯ УГРОЗА И ЗАЩИТА ИНФОРМАЦИОННЫХ СЕТЕЙ США ОСНОВНЫЕ САЙТЫ ИНТЕРНЕТА **45**

Линки к источникам в Интернете по вопросам, относящимся к данной теме

ВНЕШНЯЯ ПОЛИТИКА
США

Электронный журнал Информационного агентства США Том 3 • Номер 4 • Ноябрь 1998 г.

Электронные журналы ЮСИА выходят каждый три недели. В них обсуждаются сложные проблемы, стоящие перед Соединенными Штатами. Они также информируют общественность о событиях, происходящих в этой стране. Журналы выходят в сериях: «Экономические перспективы», «Глобальные проблемы», «Вопросы демократии», «Внешняя политика США» и «США: общество и ценности». Они содержат анализ, комментарии и информационные материалы по обсуждаемой теме. Все журналы переводятся на французский и испанский языки.

Некоторые номера журналов переводятся также на арабский, португальский и русский языки, причем два последних варианта выходят в гипертекстовом режиме и формате Adobe Acrobat. *Мнения, высказываемые в этих журналах, не обязательно отражают взгляды или политику правительства США.*

 Текущие или предыдущие номера журналов можно получить с домашней страницы Информационной службы США (ЮСИС) во Всемирной компьютерной сети по адресу: "http://www.usia.gov/journals/journals.htm". *Журналы предоставляются в нескольких электронных форматах для упрощения их просмотра, передачи, вывода и печати. Комментарии и замечания можно присылать в местное отделение ЮСИС или в редакцию:*

Editor, U.S. Foreign Policy Agenda
Political Security – I/TPS
U.S. Information Agency
301 4th Street, S.W.
Washington, D.C. 20547
United States of America

Вы можете также использовать
следующий адрес электронной
почты: ejforpol@usia.gov

Этот номер «ВНЕШНЕЙ ПОЛИТИКИ США» можно найти на домашней странице ЮСИС во Всемирной компьютерной сети по адресу: "http://www.usia.gov/journals/itps/1198/ijpe1198.htm".

ОБОРОНА СТРАНЫ ОТ КИБЕРНЕТИЧЕСКОЙ АТАКИ: ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СРЕДЕ

Генерал-лейтенант Кеннет А. Минихэн
Директор Агентства национальной безопасности США

Агентство национальной безопасности США «использует свой уникальный опыт разработки фундаментальных технологий для выявления посягательств на компьютерные системы страны и защиты от них», говорит генерал-лейтенант ВВС Кеннет А. Минихэн. Он подчеркивает, что «информационное превосходство в информационный век – несомненно дело государственной важности.»

«НАМ ГРОЗИТ ОПАСНОСТЬ. ЖИЗНЬ В АМЕРИКЕ ВО МНОГОМ ЗАВИСИТ ОТ КОМПЬЮТЕРОВ. С ПОМОЩЬЮ КОМПЬЮТЕРОВ ОСУЩЕСТВЛЯЕТСЯ УПРАВЛЕНИЕ СИСТЕМАМИ РАСПРЕДЕЛЕНИЯ ЭЛЕКТРОЭНЕРГИИ, СИСТЕМАМИ СВЯЗИ, СРЕДСТВАМИ АВИАЦИИ И ФИНАНСАМИ. КОМПЬЮТЕРЫ ИСПОЛЬЗУЮТСЯ ДЛЯ ХРАНЕНИЯ ВАЖНЕЙШЕЙ ИНФОРМАЦИИ, НАЧИНАЯ С ИСТОРИЙ БОЛЕЗНИ И БИЗНЕС-ПЛАНОВ И КОНЧАЯ СВЕДЕНИЯМИ О СУДИМОСТИ. И ХОТЯ МЫ ДОВЕРЯЕМ КОМПЬЮТЕРАМ, ОНИ ПОДВЕРЖЕНЫ РИСКУ КАК СЛУЧАЙНЫХ СБОЕВ В РЕЗУЛЬТАТЕ НЕСОВЕРШЕННОЙ КОНСТРУКЦИИ ИЛИ НЕДОСТАТОЧНОГО КОНТРОЛЯ ЗА КАЧЕСТВОМ, ТАК И – ЧТО БОЛЕЕ ТРЕВОЖНО – РИСКУ УМЫШЛЕННЫХ ПОСЯГАТЕЛЬСТВ. ВООРУЖИВШИСЬ КОМПЬЮТЕРОМ, СОВРЕМЕННЫЙ ВОР МОЖЕТ УКРАСТЬ БОЛЬШЕ, ЧЕМ ИСПОЛЬЗУЯ ОГНЕСТРЕЛЬНОЕ ОРУЖИЕ. ЗАВТРАШНИЙ ТЕРРОРИСТ СМОЖЕТ ПРИЧИНИТЬ БОЛЕЕ СЕРЬЕЗНЫЙ УЩЕРБ С ПОМОЩЬЮ КЛАВИАТУРЫ, ЧЕМ С ПОМОЩЬЮ БОМБЫ».

«Компьютеры в опасности», Национальный исследовательский совет, 1991 г.

ВВЕДЕНИЕ

Наверное, в приведенных выше словах самое примечательное то, что они были написаны еще на заре информационного века. До недавнего времени наша страна не придавала им большого значения. Соединенные Штаты и весь остальной мир по-прежнему не задумываясь используют достижения информационной революции, все глубже и глубже погружаясь в кибернетическое пространство.

Информационные технологии продолжают быстро внедряться в жизнь и экономику нашей страны, которая является элементом глобального сообщества. «Информационная супермагистраль» в полном смысле стала неотъемлемым элементом экономики.

Соединенные Штаты ведут за собой мир в информационный век, но при этом сами они почти полностью зависят от информационных технологий – компьютеров и глобальных сетей, которые связывают эти компьютеры воедино. Эта зависимость превратилась в очевидную и непосредственную угрозу нашему экономическому благосостоянию, безопасности нашего общества и нашего государства.

Существующие в мире глобальные компьютерные сети, которые часто называют «кибернетическим пространством», не знают физических границ. Расширяя наши контакты с помощью кибернетического пространства, мы все больше подвергаем себя опасности посягательств со стороны старых и новых противников, число которых увеличивается. Террористы, радикально настроенные группы, наркодельцы, действующие лица в системе организованной преступности и враждебно настроенные к нам государства будут использовать многочисленные сложнейшие орудия информационной войны. Информационная война может дополнить или целиком заменить собой войну в привычном ее понимании, что в значительной степени усложняет и расширяет список угроз, которые необходимо предвидеть и предотвратить. Опасности подвергается не только информация, хранящаяся или

передающаяся в кибернетическом пространстве, но и все компоненты нашей национальной инфраструктуры, зависящие от информационных технологий и от своевременного доступа к надежным данным. К этим компонентам относится сама телекоммуникационная инфраструктура, наши банковская и финансовая системы, система электроснабжения и другие энергетические системы, такие как нефте- и газопроводы, транспортные сети, системы водоснабжения, системы медицинских услуг и здравоохранения, полиция, пожарная и спасательная службы, а также государственные органы и учреждения всех уровней. Все они необходимы для успешной экономической деятельности и обеспечения национальной безопасности.

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ – ОБЩЕНАЦИОНАЛЬНАЯ ЗАДАЧА

22 мая 1998 г. Президент подписал директиву за номером 63 (ПДР-63) о мерах по защите важнейших объектов инфраструктуры. В этой директиве говорится: «Я намерен обеспечить принятие Соединенными Штатами всех необходимых мер для скорейшего устранения любых серьезных недостатков, делающих важнейшие объекты нашей инфраструктуры, и особенно наши компьютерные системы уязвимыми как к физическому, так и компьютерному нападению.

Общенациональная задача состоит в том, чтобы не позднее 2000 г. в Соединенных Штатах был разработан первоначальный комплекс мер в этой области, а не позднее, чем через пять лет были созданы средства и возможности для защиты важнейших объектов нашей инфраструктуры от умышленных акций, способных нанести существенный ущерб:

- Федеральному правительству в осуществлении важнейших задач в сфере национальной безопасности и обеспечения охраны здоровья и безопасности граждан.

- Правительствам штатов и местным органам власти в поддержании общественного порядка и предоставлении населению основных видов услуг.

- Частному сектору в обеспечении нормального функционирования экономики и работы важнейших телекоммуникационных, энергетических, финансовых и транспортных служб».

Реализация этой масштабной задачи потребует значительного напряжения сил и совместных усилий правительственных органов и частных компаний, отвечающих за работу важнейших объектов инфраструктуры. Согласно директиве Президента, федеральное правительство должно подать пример, обеспечив надежную работу федеральных систем. Но одновременно в президентской директиве указывается, что государство не сможет решить это проблему в одиночку. Работа каждого федерального ведомства и агентства в значительной степени зависит от услуг, предоставляемых частным сектором – речь идет об энергоснабжении, телекоммуникациях, транспорте и так далее. В связи с этим президентская директива предусматривает формирование партнерских отношений между государственным и частным сектором с целью разработки и реализации комплексного плана защиты национальной кибернетической инфраструктуры и борьбы с угрозой электронного терроризма. Сегодня встает непростая задача привлечения частного сектора к подобным мероприятиям в общенациональных масштабах. В настоящих условиях жесткой конкуренции в целях увеличения прибыли частные компании стремятся получить разного рода рыночные преимущества, включая понижение производственных издержек. Усиленные меры защиты компьютерных систем потребуют как увеличения капиталовложений, так и определенного сотрудничества с конкурентами.

ВАЖНЕЙШИЕ ЭЛЕМЕНТЫ

Любая стратегия, имеющая целью укрепление важнейших объектов нашей инфраструктуры, должна состоять из трех основных элементов: повышения степени защиты от посягательств на компьютерные системы, выявление подобных посягательств в тот момент, когда они происходят, противодействие им и/или восстанавление инфраструктуры после нанесения ей ущерба.

Меры по усилению защиты от посягательств на компьютерные системы основаны на технологиях кодирования информации – включая опознавательные цифровые коды – обеспечивающих подтверждение личности пользователя, целостность

информации, невозможность отрицать факт ее получения, а также конфиденциальность – то есть все, что необходимо для информационной защиты. Самым мощным средством защиты от посягательств на компьютерную информацию, вероятно, служит система опознавательных цифровых кодов. Встроенные опознавательные цифровые коды также обеспечивают целостность электронной информации и невозможность отрицать факт ее получения по системам компьютерной связи. Кодирование применяется в настольных компьютерах, файловых серверах и в компьютерных сетях для обеспечения конфиденциальности правительственной, деловой и личной информации, не подлежащей разглашению. Технологии кодирования, которые когда-то были исключительной прерогативой правительственных органов, сегодня широко применяются в коммерческой практике и представляют собой основное средство информационной защиты. 16 сентября 1998 г. вице-президент США объявил о крупных изменениях в мерах по контролю экспорта из США технологий кодирования, что подчеркивает важное значение таких технологий для защиты важнейших объектов инфраструктуры, глобальной электронной коммерции и экономического благополучия страны.

Поскольку технологии кодирования уже достигли необходимого уровня развития, встает задача последовательного и эффективного применения этих технологий во всех важнейших звеньях нашей инфраструктуры. Для этого потребуется создание рамочных условий, в которых услуги по кодированию информации могли бы комплексно предоставляться на всех уровнях. Необходимо также формирование особой вспомогательной инфраструктуры, то есть системы криптозащиты на основе публичного ключа, которая обеспечивала бы надежные и глобально распознаваемые цифровые подписи и сертификацию шифрующего ключа. По сути такая инфраструктура позволяла бы людям обладать уникальными «электронными удостоверениями личности», которые соответствовали бы всем требованиям информационного века. Услуги в этой области начинают появляться в частном секторе в связи со спросом на них со стороны глобальной электронной коммерции. Но ими можно воспользоваться и при защите важнейших объектов инфраструктуры. Сегодня не существует еще достаточно совершенных или эффективных технологий для того, чтобы прогнозировать, выявлять или реагировать на посягательства в отношении компьютерных систем. В настоящее время у Соединенных Штатов мало возможностей для выявления или распознавания посягательств на компьютерные системы правительственных или частных объектов инфраструктуры, и еще меньше возможностей для того, чтобы реагировать на такие посягательства. Способность идентифицировать посягательства на компьютерную систему одного или нескольких стратегических объектов инфраструктуры и соответствующим образом реагировать на такие посягательства безусловно представляет собой важнейшую задачу в сфере национальной безопасности. Дело осложняется еще и тем, что любое вторжение в компьютерные системы традиционно рассматривается как правонарушение и находится в компетенции правоохранительных органов. Когда происходит такое вторжение, нарушителя выявляют (если это возможно), арестовывают и подвергают суду. Но многие частные компании неохотно предоставляют информацию о вторжениях в их компьютерные системы, опасаясь негативного освещения в прессе (например, газетных заголовков типа: «В результате компьютерного вторжения банк потерял миллионы долларов», или «Компьютерные взломщики вывели из строя телефонную сеть»), а также негативной реакции со стороны общественности. Для того, чтобы построить эффективную национальную систему защиты компьютерных сетей, необходимо разработать новые «правила игры», создающие возможности для более открытого и динамичного сотрудничества между частным сектором, правоохранительными органами и службами национальной безопасности.

НОВАЯ РОЛЬ АГЕНТСТВА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ДЕЛЕ ЗАЩИТЫ ИНФОРМАЦИИ

В условиях информационного века традиционные задачи, которые выполняет Агентство национальной безопасности, такие, как электронная разведка и обеспечение безопасности информационных систем, эволюционируют в направлении обеспечения информационного превосходства Соединенных Штатов и их союзников. Главное в решении этой задачи – глубокое понимание глобальной информационной инфраструктуры и уязвимости информационных систем, объединенных в сети. АНБ уже предпринимает ряд мер по разработке технических

основ защиты важнейших объектов нашей инфраструктуры.

Как уже упоминалось выше, технологии кодирования информации получили широкое распространение в коммерческой практике и служат основным средством защиты информационных систем от внешних посягательств. Плохо то, что многие продукты, которые уже существуют сегодня в этой сфере, не обеспечивают надежного взаимодействия друг с другом и имеют разную степень надежности, а, кроме того, существует множество методов кодирования информации, которые часто не согласуются друг с другом. Так, например, существует кодирование электронной почты, кодирование файлов, кодирование вебсайтов, кодирование отсылок (линков) и кодирование виртуальных частных компьютерных сетей – и этот список можно продолжить. Чтобы поправить сложившееся положение, АНБ установило партнерские отношения с ведущими поставщиками технологий по защите информации с целью разработки общей основы кодирования информации, обеспечивая единообразие методов информационной защиты в рамках целого предприятия. Такая основа определяет пути согласованного применения технологий кодирования информации на предприятии, а также взаимодействия с другими обеспечивающими безопасность технологиями и продуктами, например, такими, как системы блокировки, серверы, маршрутизаторы, операционные системы, системы выявления вторжений, системы выявления преднамеренно дефектных кодов, средства проверки и инфраструктура публичных электронных ключей.

Другая сторона проблемы состоит в разной степени надежности разнообразных средств защиты, имеющихся на рынке. С целью решения этого вопроса АНБ установило партнерские отношения с Национальным институтом стандартов и технологий (НИСТ). В рамках этого партнерства АНБ и НИСТ будут осуществлять аттестацию коммерческих лабораторий, с тем, чтобы они могли проводить экспертизу средств защиты, подтверждая параметры защиты, о которых заявляет продавец, либо их соответствие критериям защиты, применяемым в конкретной компьютерной сети. Испытания продуктов будут проводится аттестованными лабораториями на платной основе; при этом лаборатория и фирма, реализующая продукт на рынке, будут договариваться о размерах оплаты и сроках.

Наконец, Агентство национальной безопасности считает, что в стране должен быть создан общий для всех набор средств защиты информации, имеющей важное значение с точки зрения национальной безопасности, и в связи с этим использует имеющийся у него уникальный опыт в разработке фундаментальных технологий для создания общенациональных возможностей по выявлению посягательств на компьютерные системы и реагированию на них. Эти технологии предусматривают интегрированное использование целого ряда датчиков, которые могут применяться на важнейших объектах инфраструктуры и в самой телекоммуникационной инфраструктуре, и которые обладают широким диапазоном аналитических возможностей для динамичного распознавания угроз, возникающих со стороны глобального кибернетического пространства в отношении важнейших объектов инфраструктуры. Эти технологии должны стать общими для органов национальной безопасности, федеральных учреждений, промышленных отраслей и региональных органов и должны обеспечивать одновременное выявление посягательств, защиту от них и восстановление работы важнейших служб и объектов инфраструктуры.

ЗАКЛЮЧЕНИЕ

Нынешний высокий уровень благосостояния нашей страны во многом опирается на достижения информационного века и на наше глобальное лидерство в области информационных технологий. Наше дальнейшее лидерство и процветание в системе глобальной экономики будут во многом зависеть от того, сумеет ли наша страна возглавить усилия в деле защиты информации в условиях глобальной информационной среды, которую мы сами помогали создавать. Издав Директиву-63, администрация США ясно дала понять, что настало время действовать, а со своей стороны Агентство национальной безопасности США готово откликнуться на этот призыв и предоставить имеющиеся у него технический опыт и знания. Информационное превосходство в информационный век – несомненно дело государственной важности.

ЗАЩИТА ИНФОРМАЦИИ – ГЛАВНАЯ ЗАДАЧА НОВЕЙШЕГО ПЕРИОДА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ

Джон Хэмри
Заместитель министра обороны США

Защита жизненно важных информационных ресурсов станет «одной из главных задач в области национальной безопасности на ближайшие годы», – считает заместитель министра обороны США Джон Хэмри. Отметив, что на Пентагон возложена ответственность по защите 28 тыс. различных компьютерных систем, он предупредил, что оборона виртуального мира от кибернетической угрозы «требует не только технического решения, но и правильного управления и постоянного внимания к этому вопросу».

С точки зрения обеспечения безопасности, Соединенные Штаты пережили пять периодов, при этом переход от одного периода к другому означал переход от определенного прошлого к совершенно неопределенному будущему. Первый период длился с начала войны за независимость до середины 20-х годов 19-го века, когда роль Соединенных Штатов в системе международной безопасности, где все еще доминировала Европа, была ограничена.

С середины 30-х годов до конца 19-го столетия, пока шел процесс разрушения старой политической структуры Европы, мы, отделенные от нее Атлантическим океаном, занимались своими собственными делами. Этот второй период завершился с окончанием Первой мировой войны и возникновением Советского Союза. Третий период длился с 1920 по 1946 год и характеризовался глобальным экономическим спадом и одновременно подъемом международного коммунистического движения на фоне распада Европы. Эти события привели к кризису американской демократии и системы свободного предпринимательства во время Великой депрессии, а напряженность в области международной безопасности привела в конечном итоге ко Второй мировой войне.

В период холодной войны доминировал двухполюсный мир. Соединенные Штаты возглавляли движение международного сообщества, направленное на создание институтов для восстановления разрушенной экономики стран Европы и решение проблем в странах третьего мира, связанных с распадом старых европейских империй. В то же время Соединенные Штаты возглавляли движение стран свободного мира, направленное на сдерживание распространения коммунизма во всем мире, вплоть до развала Советского Союза.

В настоящее время происходит переход к новой эпохе, которая, по-видимому, будет характеризоваться возрождением старых факторов угрозы – национализма и этнических конфликтов. Еще одна сторона этого нового периода связана с ослаблением контроля и распространением современных технологий, а также динамичным развитием новых совершенно поразительных технических возможностей, которые несут в себе огромный потенциал как добра, так и зла. Сейчас мы живем в постоянном страхе из-за того, что «бесконтрольные ядерные ракеты» или химическое и биологическое оружие может попасть в руки террористов.

Новейший период в области обеспечения безопасности США будет также связан с проблемой кибернетической безопасности. Стремительный рост и распространение информационных технологий оказали существенное воздействие на все сектора американской экономики и правительство. Информационные технологии способствовали колоссальному экономическому развитию, качественно усовершенствовали средства связи и позволили американским предпринимателям участвовать в конкурентной борьбе более эффективно и успешно, чем когда бы то ни было. Соединенные Штаты и мир в целом в очень серьезной степени опираются на информационную технологию – этого нельзя было вообразить еще буквально несколько лет назад.

Это особенно справедливо в отношении американских военных. Министерство обороны применяет информационные технологии, чтобы произвести, как мы говорим, революцию в военной сфере, которая охватывает передачу и обработку огромного объема информации для получения более достоверных разведданных, радикальное совершенствование средств управления и контроля, внедрение более современных методов работы и разработку более мощных систем вооружения. Эта революция имеет огромное значение, особенно если мы хотим сохранить способность защищать интересы США сегодня и подготовиться к отражению угрозы в будущем.

Революция информационных технологий охватывает все сферы деятельности Министерства обороны как в полевых условиях, так и в штабах. Очень скоро наши солдаты на уровне первичного подразделения будут иметь средства связи, которые позволят командирам точно знать о местонахождении каждого отдельного солдата, обстановке вокруг него и даже ритме сердца, то есть почти исчерпывающие сведения с поля боя. Наши моряки направляют домой с кораблей в открытом море послания по электронной почте, применяя технологию, очень схожую с той, которая используется для нацеливания крылатых ракет. Летчикам приходится сейчас отсеивать в перенасыщенном потоке информации ту, которая им необходима в полете.

Мы применяем новейшую технологию в сфере материально-технического снабжения для соединения передовых рубежей с тылом. К концу века мы обязались перейти к процессу закупок без оформления каких-либо бумаг. Созданное у нас Объединенное управление электронных программ обеспечивает закупку всего необходимого на уровне подразделений и широко использует основанные на Интернете электронные «торговые центры» для покупки всего – от ручек до гидравлических силовых приводов. Мы очень широко используем Интернет, начиная от оплаты транспортных расходов и заканчивая спутниковой связью, и добились огромных успехов в публикации материалов в электронных средствах информации.

Короче говоря, Министерство обороны США в полной мере использует потенциал микросхем для создания вооруженных сил 21-го века. Однако, при этом необходимо осознавать, что вместе с новыми технологиями приходят и новые опасности. Те же самые технические средства, которые позволяют нам достигать высокую эффективность, могут быть использованы для нападений в кибернетическом пространстве теми, кто не может нанести нам удар на обычном поле боя. Это совершенно другое – и очень важное – направление в области национальной безопасности. Технологические средства и возможности, которые ранее были доступны только государствам, стали доступны частным лицам. Защита информационных ресурсов станет поэтому одной из главных задач в области национальной безопасности на ближайшие годы.

Мало кто оспаривает тот факт, что защита информации имеет важное значение. В Министерстве обороны мы уже столкнулись с первой волной кибернетической угрозы как на учениях, так и в реальной обстановке. Для того, чтобы оценить степень нашей уязвимости, мы в прошлом году провели учение. Нашими «противниками» была группа из 35 человек, перед которыми была поставлена задача проникнуть в компьютерные системы Министерства обороны США. В их распоряжении имелись только общедоступные средства, готовые технологии и программное обеспечение, которое открыто продается или которое можно загрузить с Интернета. Действуя в таких условиях, эта группа в течение трех месяцев смогла атаковать нас, проникнуть в наши несекретные сети и фактически могла серьезно нарушить работу наших средств связи и систем энергоснабжения.

В феврале этого года мы испытали организованное нападение против компьютерных систем Пентагона в период интенсивного развертывания сил в районе Персидского залива. Оказалось, что это сделали два подростка из Калифорнии, но в тот момент такой удар мог оказаться гораздо серьезнее. Как наши учения, так и эти ограниченные удары сыграли роль предупредительных сигналов о том, что более серьезные удары обязательно последуют, вопрос лишь в том, когда и где.

Для предотвращения этой угрозы прежде всего надо изменить образ нашего мышления. Традиционно американцы думали о безопасности как об ограде вокруг двора, которая устанавливает границы и защищает огороженную территорию. Если

в ограде появляется дыра, ее можно заделать и опять оказаться в безопасности. Такой образ мышления хорошо работал в прошлом, но в кибернетическом пространстве границы отсутствуют. Переход к будущему должен быть отмечен не только достижениями в области технологии, но и большей гибкостью мышления. Мы должны осознать, что безопасность в виртуальном мире требует не только технического решения, но и правильного управления и проявления постоянного внимания к этому вопросу.

Изменение образа мышления может оказаться одной из самых трудных задач. Не осознавая этого, мы сейчас предоставляем, например, потенциальным противникам информацию, на добывание которой они раньше тратили сотни миллионов долларов, проводя разведывательные операции. У нас был один военный объект, у которого, как считалось, была прекрасная страница в Интернете. На ней была изображена проекция объекта с воздуха, где были обозначены здания с надписями «Операционный центр» и «Центр технической поддержки». Эта страница очень нравилась общественности, но в то же время предоставляла ценную информацию для наведения на цель тем, кто хочет нанести нам ущерб.

Более широко осознавая связанные с этим проблемы, необходимо предпринять конкретные меры по защите наших информационных данных. В прошлом году Министерство обороны США попыталось определить потребности по защите нашей информационной инфраструктуры. Темпы развития информационной технологии осложняют эту проблему. В Министерстве обороны имеется 28 тыс. различных компьютерных систем, причем все они совершенствуются и заменяются. Но необходимо понять их уязвимые места. Задача защиты информации схожа с войной, и мы соответствующим образом подходим к ее решению, назначив для координации усилий командира Объединенной тактической группы по защите компьютерной сети Министерства обороны. Министерство обороны вносит также большой вклад в работу Национального центра защиты информации и Управления защиты важнейшей информации при Президенте США.

Безусловно, необходимо предпринимать и другие действия. В настоящее время 95 процентов наших коммуникаций осуществляется по обычным телефонным и факсимильным линиям, в результате чего важным элементом защиты информации становится шифрование. Одним из наиболее опасных сценариев действий в виртуальном мире может стать такой, когда наши бойцы получат ложные сообщения, которые будут их дезинформировать. Поэтому без надежного шифрования вся информационная инфраструктура, от которой мы зависим, оказывается уязвимой. В ответ на эту угрозу мы сейчас работаем над тем, чтобы в рамках Министерства обороны можно было гарантировать цифровое «удостоверение личности» пользователей и разработать надежную систему связи на основе публичного шифровального ключа. Мы должны усовершенствовать процесс кодирования с тем, чтобы информация, которую мы передаем и обрабатываем с помощью электронных средств, была в безопасности и поддавалась проверке. Министерство обороны предпринимает также важные шаги по обеспечению безопасности сети в более широком плане. Мы устанавливаем средства контроля за системами связи и работаем над обеспечением контроля конфигурации в условиях постоянно изменяющейся и динамичной среды. Мы устанавливаем программные блокировки, создаем центры контроля за сетями, цифровые опознавательные коды и создаем инфраструктуру безопасности.

Защита информации, шифрование и безопасность сетей составляют одну из самых серьезных проблем, с которыми когда-либо сталкивалось Министерство обороны. Используя последние достижения в области информационной технологии, необходимо обеспечить доступ к информации, на которую мы опираемся, и ее защиту. Мы предпринимаем огромные шаги в этом направлении, однако предстоит еще многое сделать. В это трудное время необходимо использовать опыт специалистов по информационной технологии как в Министерстве обороны, так и в частном секторе и правительстве, чтобы защитить жизненно важные для нас компьютерные системы. Мы должны сделать так, чтобы наша страна так же успешно функционировала в условиях современного периода в обеспечении безопасности, как и в прошлом.

ИНТЕГРИРОВАННЫЙ ПОДХОД В ОТРАЖЕНИИ НОВЫХ УГРОЗ

Интервью с Джефри А. Ханкером, директором Управления безопасности инфраструктуры США

Для защиты основных объектов инфраструктуры США на случай кибернетического нападения необходима «полная поддержка со стороны частного сектора», – сказал д-р Джефри А. Ханкер, директор Управления безопасности инфраструктуры США. «Стоящая перед нами в настоящее время угроза постоянно увеличивается, – сказал он. – Поэтому необходимо действовать незамедлительно и как можно скорее достичь реальных результатов в деле ее предотвращения». Ханкер дал интервью Сюзан Эллис.

ВОПРОС: Вы, как директор Управления безопасности инфраструктуры США, занимаетесь составлением единого общенационального плана по отражению факторов физической и кибернетической угрозы в отношении объектов связи, транспорта, энергетики и других элементов жизненно важной инфраструктуры нашей страны. Какова главная проблема, стоящая перед вами в связи с выполнением новых задач в рамках инициативы, о которой Президент Клинтон объявил в мае этого года?

ХАНКЕР: Главная проблема, которую очертил Президент, связана с тем, что для современной эпохи характерны новые опасности, с которыми мы никогда до сих пор не сталкивались. В частности, благодаря тому, что средства телекоммуникации и Интернет так тесно связаны сейчас с системой энергоснабжения, основными системами транспорта и телекоммуникациями, можно нарушить работу этих систем с помощью так называемого кибернетического нападения, воспользовавшись компьютером и Интернетом для проникновения в эти системы, вывода их из строя или нарушения их функционирования. Такой удар может не только, например, оказать воздействие на боевые операции, но и нарушить работу жизненно важных служб, от которых зависит экономика страны и повседневная жизнь американцев: электроснабжение, телефонная связь, транспорт.

Это совершенно новый фактор угрозы, который появился в связи с бурным развитием технологий и повышением взаимосвязанности различных отраслей американской экономики. Основная проблема, стоящая перед нами, – это осведомление американцев об этом новом виде угрозы и сотрудничество с бизнесменами и промышленниками в обеспечении защиты от этих видов кибернетических нападений.

ВОПРОС: Это действительно нечто совершенно новое, не так ли?

ХАНКЕР: Да. За последние десять лет мы связали воедино все экономические секторы нашей страны, что обеспечило значительный экономический рост и способствовало процветанию, которое переживает сейчас Америка. Однако, это породило и новые формы уязвимости, которые явились следствием нашей зависимости от электронных и информационных средств. Иными словами, это дало в руки наших противников, – будь то отдельные страны, террористические группы или преступные картели – новые возможности для нанесения удара против нас.

ВОПРОС: Какие правительственные ведомства участвуют в работе по противодействию этой угрозе и как ваше управление взаимодействует с ними?

ХАНКЕР: В федеральном правительстве насчитывается одиннадцать крупных ведомств, которым Президент дал указание работать вместе. Среди основных ведомств – Министерство обороны и подчиненные ему организации; разведывательные органы и правоохранительные органы – Федеральное бюро расследований, Центральное разведыва-

тельное управление и Министерство юстиции. Я также считаю, что большое значение имеют Министерство торговли, Министерство финансов и Министерство транспорта. Все они призваны работать над созданием общенационального плана. Еще важнее то, что все они призваны сотрудничать с частным сектором, так как почти все так называемые критически важные объекты инфраструктуры, по которым могут быть нанесены удары, находятся фактически в собственности частного сектора. И если мы не обеспечим сотрудничество и всестороннюю поддержку со стороны частного сектора в создании средств защиты, то мы далеко не уйдем.

ВОПРОС: Как вы будете определять успех в выполнении своей задачи?

ХАНКЕР: Это очень сложно, так как это – новая проблема, и виды ударов и типы угрозы, от которых Президент попросил нас защитить страну, постоянно изменяются и обновляются. В некоторых случаях ничего еще не произошло, и поэтому определить степень успешности работы будет довольно сложно. Я полагаю, что одним из параметров успеха станет то, как частный сектор – владельцы и операторы сетей энергоснабжения, а также таких секторов экономики, как транспорт, банковская система и финансы – сумеет объединиться и будет вместе с правительством разрабатывать план действий. В течение последующих шести – двенадцати месяцев будет видно, как пойдет формирование этого партнерства. Это и станет первым крупным показателем успеха.

ВОПРОС: В какие временные параметры вы пытаетесь уложиться?

ХАНКЕР: У нас очень сжатые сроки, поскольку эта угроза, которой обеспокоен Президент – скоординированные, изощренные электронные удары по критически важным объектам инфраструктуры страны, – существует уже сейчас. Президент призвал разработать общенациональный план, обеспечивающий потенциал защиты от новых видов кибернетических ударов к 2000 году. Он также призвал обеспечить к 2003 г. наличие надежных средств по защите страны. Стоящая перед нами угроза постоянно увеличивается. Поэтому необходимо действовать незамедлительно и как можно скорее достичь реальных результатов в деле ее предотвращения.

ВОПРОС: Как я понимаю, вы планируете подготовить что-то уже в ноябре?

ХАНКЕР: Да, вы правы. Фактически одной из самых первых мер, намеченных Президентом в его обращении в мае, было следующее: в течение шести месяцев, которые заканчиваются в ноябре, ведомства федерального правительства должны обеспечить существенный прогресс в области разработки планов защиты своих критически важных объектов инфраструктуры. Это означает, что наряду с другими ведомствами, Министерство финансов и Министерство обороны разработают процесс обеспечения защиты от электронных ударов. Во-вторых, Президент призвал нас разработать основные ориентиры более широкого общенационального плана действий, предусматривающего тесное сотрудничество с частным сектором, объединение работы целого ряда различных ведомств и привлечение университетов и научно-исследовательских институтов; так что работа идет в разных направлениях. Мы не сможем в ноябре представить национальный план, однако, мы представим основные ориентиры для его разработки.

ВОПРОС: Как вы оцениваете характер и степень угрозы для критически важных объектов инфраструктуры США, и какие сектора наиболее уязвимы?

ХАНКЕР: Для того, чтобы оценить степень угрозы и уязвимость критически важных объектов американской инфраструктуры, необходимо начать с понимания того, как развивается экономика. За последние два года в результате развития Интернета, который каждые десять месяцев удваивается по размеру и числу потребителей, взаимосвязанными стали все основные службы, от работы которых зависит повседневная жизнь американцев, – электроснабжение, банки и телекоммуникации. Эти системы, составляющие основу нашего экономического роста и необходимые для выполнения жизненно важных функций безопасности в общенациональном масштабе, оказались сейчас очень уязвимыми.

В начале этого года в период развертывания сил для ответных действий в отношении Ирака у нас

появились свидетельства того, что компьютерные взломщики (хакеры) проникли в секретные компьютерные системы Министерства обороны. На протяжении нескольких недель, пока наши сотрудники пытались определить, откуда ведутся эти атаки, это вызывало обеспокоенность на высших уровнях правительства. Исходило ли это от Ирака или его союзников? Но оказалось, это были просто два подростка в Соединенных Штатах, которым помогал советами кто-то из-за рубежа. Это пример того, насколько мы уязвимы.

В другом случае подросток из Массачусетса сумел отключить в своем штате большой участок телефонной сети, «ослепив» тем самым на некоторое время крупный аэропорт и создав реальную угрозу для воздушных полетов. Если такого рода ущерб могут нанести отдельные компьютерные взломщики, то представьте себе, что может произойти в результате изощренного организованного удара, нацеленного на выведение из строя крупных участков наших энергосистем и телекоммуникаций или взлома секретной компьютерной сети. Именно таков характер угрозы, с которой мы имеем дело. И существует множество признаков того, что в других странах люди знают об этом и разрабатывают определенный вид наступательного потенциала для того, чтобы нанести удар по Америке с помощью электронных средств.

ВОПРОС: В качестве директора Агентства безопасности инфраструктуры США вы координируете реализацию программы просвещения и обучения в этой области. Какова ваша главная идея и как вы пропагандируете ее среди американского населения?

ХАНКЕР: Очень важно в разговоре об обучении и просвещении иметь в виду две задачи. Первая касается осведомленности о проблеме. Мы имеем дело с новой эрой в обеспечении безопасноти, то есть с угрозой нового типа, которая лишь недавно стала вызывать беспокойство. Поэтому важным направлением нашей миссии безусловно является осведомление людей. И я очень удовлетворен тем, что официальные лица на уровне министров хорошо понимают характер этой угрозы. Бизнесмены м руководители учебных заведений тоже отлично понимают это.

Вторая задача – определить, что мы можем сделать в этом плане? И именно поэтому мы укрепляем партнерство между частным сектором и различными правительственными ведомствами для того, чтобы в ближайшие месяцы и ближайшие годы предпринять реальные меры в ответ на эту угрозу.

ВОПРОС: Как бы вы охарактеризовали степень нашей зависимости от компьютеров не только в нашей частной жизни, но и в сфере функционирования всего нашего общества?

ХАНКЕР: Взгляните на свой дом, взгляните на кабинет, в котором вы работаете, – и вы увидите нашу зависимость от электронных систем. Мы идем в банк и используем автоматический банкомат. Это электронная система, соединенная проводами в пределах страны и с зарубежными странами. Наша система электроснабжения все больше и больше управляется через Интернет. Работа воздушного транспорта и железных дорог целиком зависит от электронных систем. И даже в таких компаниях, о которых не подумаешь, что это компьютерные компании или компании по разработке программного обеспечения, работа и производительность зависят от соединенных друг с другом информационных систем.

По имеющимся оценкам, от одной третьей до одной второй экономического роста нашей страны за последние два года, а также новые сотни тысяч рабочих мест были обусловлены электронной торговлей. Компьютеры лежат в основе нашего будущего экономического роста. Они обеспечивают безопасность повсеместно, будь то транспортировка грузов и военнослужащих в разные части мира или сбор жизненно важной информации и разведданных о факторах угрозы. По существу все это основывается на новых электронных системах.

ВОПРОС: Как вы сотрудничаете с представителями частного торгового и промышленного секторов в обеспечении защиты американских информационных систем и средств связи?

ХАНКЕР: Тесное сотрудничество с частным сектором действительно необходимо для выполнения той цели и задачи, которые поставил Президент. Возможно, это покажется странным, но это факт:

90–95 процентов коммуникационных систем Министерства обороны принадлежит частным компаниям и эксплуатируются ими. И это имеет жизненно важное значение. Если мы не привлечем частный сектор, мы далеко не продвинемся.

Сейчас я участвую в совещаниях с официальными лицами из различных министерств, включая Министерство финансов и Министерство транспорта, а также с руководителями частного сектора, представляющими критически важные отрасли инфраструктуры, такие, как банковская система и транспорт; эти встречи направлены на развитие партнерских отношений между правительством и частным сектором.

В сентябре я побывал в г. Шарлотт, штат Северная Каролина, где встретился с мэром и другими представителями городских и местных властей, а также руководителями некоторых крупных банков. Шарлотт – второй по величине банковский центр страны. И я поехал туда, чтобы заручиться участием шарлоттских банков в этом партнерстве.

Мы планируем провести серию встреч в конце осени, в которых будут принимать участие Президент, вице-президент, советник по национальной безопасности, а также руководители энергетического сектора, банковской и финансовой сферы, транспортной и других критически важных отраслей инфраструктуры, что позволит еще больше укрепить это партнерство.

Это длительный процесс. Укрепление партнерских связей, в особенности там, где мы ранее никогда не сотрудничали, не может произойти в одночасье. При этом я с чувством глубокого удовлетворения отмечаю те ответные действия, осознание ситуации и реальное сотрудничество, проявление которых я наблюдаю среди исполнительных директоров и руководстводителей всех отраслей промышленности, с которыми я работал.

ВОПРОС: Сотрудничает ли ваше агентство с высшими учебными заведениями и участвует ли в их программах, направленных на поиск наиболее оптимальных путей защиты американских информационных и других критически важных структур?

ХАНКЕР: Высшие учебные заведения должны стать важной составной частью создаваемого нами партнерства. В сентябре я уже встречался с ректорами и деканами нескольких крупных университетов, таких как университет штата Северная Каролина, университет Пердью, Массачусетский технологический институт, университет штата Виржиния. Передо мной стояли две задачи. В настоящий момент наша страна испытывает явную нехватку специалистов в области компьютеров и информационной технологии. А угроза кибернетического удара лишь еще больше усугубит эту проблему. Будет возрастать потребность в людях, имеющих специальную подготовку. Именно университеты находятся на передовых рубежах подготовки специалистов, которые нам потребуются.

Потребуются также научные исследования и разработки, которые позволят найти новые решения и разработать новые технологии для защиты наших информационных систем. Главным участником этого процесса станут университеты.

ВОПРОС: Как на директоре Агентства безопасностти инфраструктуры США, на вас лежит ответственность за разработку законодательных инициатив. Как вы взаимодействуете с американским Конгрессом и как вы оцениваете влияние Конгресса на политику и стратегию, связанные с задачами вашего Агентства?

ХАНКЕР: Сотрудничество с Конгрессом – очень важная часть нашей работы. И я хотел бы подчеркнуть, что интерес со стороны Конгресса чрезвычайно высок. Конгресс оказывает широкую помощь в борьбе с этой новой формой террористической угрозы или угрозы национальной безопасности. Я предполагаю, что мы будем продолжать сотрудничать с Конгрессом при решении нескольких серьезных вопросов, в частности, в отношении необходимых ресурсов.

Мы полагаем, что продолжая выполняемую нами сегодня работу, Президент включит в бюджет на 2000-й финансовый год инициативу, направленную на защиту критически важных объектов инфраструктуры. Она будет предусматривать выделение средств на научные исследования и разработки, на реализацию новых программ подготовки специалистов в области информационной технологии как для федерального правительства, так и для част-

ного сектора, а возможно и других программ. Поэтому очень важное значение будет иметь выделение финансовых и других средств.

Члены Конгресса США рассмотрят также существующий пакет законов, относящихся к обеспечению безопасности компьютерных систем. Зачастую компьютерный взломщик проходит через несколько различных компьютеров, прежде чем он попадает в компьютер, куда стремится. В соответствии с существующими законами, в настоящее время при выслеживании компьютерного взломщика, если он действуют на территории нескольких штатов, требуется получение ордеров на обыск от судей в этих штатах. Мы намереваемся в тесном сотрудничестве с Конгрессом рассмотреть различные юридические процедуры и меры защиты, которыми мы располагаем.

ВОПРОС: Видите ли вы необходимость в более широком международном сотрудничестве и взаимодействии в области защиты основных объектов инфраструктуры, и если да, то как можно этого добиться?

ХАНКЕР: Международный аспект характерен для всего, что связано с кибернетическим миром. Мы говорим об угрозе, которая может прийти из-за рубежа, но она может возникнуть и внутри страны. При таком нападении нет необходимости в том, чтобы люди находились поблизости от учреждений или объектов, по которым они наносят удар.

За прошедший год мы столкнулись с ситуацией, когда находившийся в Германии компьютерный взломщик, оказавшийся на самом деле гражданином Индии, проник в финансовую систему в Майами, пытаясь выманить деньги. Таким образом, в данный инцидент, направленный непосредственно против американской организации, были вовлечены две страны и граждане трех стран. Это лишь небольшая иллюстрация международного характера этой проблемы.

Президентская Комиссия по защите критически важных объектов инфраструктуры США опубликовала в прошлом году доклад на основе результатов двухлетней работы. Ее рекомендации были заложены в основу инициативы, о которой Президент объявил в мае. В этой инициативе международный аспект определяется как один из самых важных.

Президент поручил Госдепартаменту возглавить переговоры с другими странами об обмене информацией и о возможности заключения новых договоров и подписания протоколов, направленных на отражение террористических или других возможных видов ударов. Уже целый ряд стран проявил к этому интерес. Я встречался с представителями канадского и мексиканского правительств и знаю также, что по этому вопросу велись переговоры в рамках НАТО и других международных организаций.

Так что этот вопрос вызывает большой интерес, но мы находимся еще на самом первом этапе международного сотрудничества в этой сфере.

Еще один важный момент связан с тем, что работа по защите от кибернетического удара – независимо от того, будет ли он нанесен со стороны организованной преступности, террористических группировок или других стран – во многом совпадает с работой над тем, что называется компьютерной проблемой 2000 года. «Проблема-2000» – это несколько иное, так как мы точно знаем, когда эта проблема возникнет. И создали эту проблему мы сами, потому что много лет назад программисты не учли тот факт, что для 2000-го года потребуется другое обозначение дат, чем для 1900-го года. (В старых компьютерных системах для обозначения календарной даты используются только две последние цифры.)

Но во многих отношениях отражение угрозы, связанной с «Проблемой-2000», требует того же комплекса мер, что и защита от кибернетического удара. Различные институты, компании и органы федерального правительства должны сначала выявить, какими системами они располагают и как они взаимосвязаны, а затем решить, какие системы наиболее важны и каким образом их защитить.

Еще один аспект проблемы 2000-го года, во многом сходный с угрозой кибернетического удара, связан с созданием национального потенциала для адаптации и перестройки систем в случае возможных неполадок в 2000-м году. Это также станет моделью для общенационального плана ответных

мер в случае кибернетического удара. Этой работой будут заниматься основные отрасли промышленности, штатные и местные органы управления, призванные принимать ответные меры в случае чрезвычайной ситуации, а также ведомства федерального правительства. По различным аспектам общей повестки дня, связанной как с решением «Проблемы-2000», так и с предотвращением опасности кибернетического нападения, мое управление тесно сотрудничает с Джоном Коскиненом, специальным советником Президента по проблеме 2000-го года.

ПРОБЛЕМА 2000 ГОДА

Джон Коскинен
Председатель Президентского совета по компьютерной проблеме 2000-ого года

Джон Коскинен, возглавляющий работу правительства США в области решения компьютерной проблемы 2000 года, считает, что главное препятствие, которое необходимо преодолеть, связано с недостаточным пониманием данной проблемы «главами правительств, журналистами, руководителями предприятий и широкой общественностью» во всем мире. Он опасается, что «бездействие и непонимание могут привести к воплощению наихудших сценариев». Вместе с тем он подчеркивает, что, «предприняв необходимые шаги сейчас, мы сможем свести к минимуму возможные сбои и, будем надеяться, осуществить плавный переход к 2000 году».

В настоящее время мир стоит перед одной из самых серьезных задач информационного века. Многие компьютерные системы, а также компьютерные микросхемы – встроенные во все устройства от персональных компьютеров до бытовой техники и сложного технологического оборудования – настроены так, что при вступлении в новое тысячелетие время в них будет автоматически переведено назад.

Суть проблемы в том, что многие более старые компьютерные системы и микропроцессоры, как называют компьютерные микросхемы, используют для обозначения даты лишь две последние цифры порядкового номера года. Таким образом, с наступлением 2000 г. эти микросхемы могут воспринять запись «00» как 1900 год, а не как 2000-й. Обусловленные этим функциональные нарушения способны привести к серьезным сбоям в работе энергетических систем, водоочистных сооружений, финансовых сетей, телекоммуникаций и систем управления воздушным движением во всем мире. В нашем все более взаимосвязанном мире с глобальной экономикой компьютерные сети сильны лишь настолько, насколько сильно их слабейшее звено. Каждая страна, естественно, испытает свои собственные трудности с определенными системами, но мы все оказались перед одной и той же проблемой.

Почему же разработчики программ совершили столь очевидную ошибку? Тридцать лет назад доступный объем компьютерной памяти был гораздо меньше, чем сейчас, поэтому программисты в целях экономии памяти широко применяли сокращения типа использования двух цифр для записи года. Они исходили из того, что создаваемые ими программы выйдут из употребления и будут заменены новыми задолго до 2000 года. Однако, на практике многие большие и сложные компьютерные системы, подобные тем, которыми пользуются банки, страховые компании или брокерские фирмы, претерпели процесс постепенной эволюции с добавлением новейших средств программного обеспечения в действующие системы. В результате любой организации, эксплуатирующей крупномасштабные, соединенные друг с другом компьютерные системы, придется проверить миллионы строк программ, с тем, чтобы определить, как записываются даты, а затем переписать программы с учетом данной проблемы. После этого нужно будет запустить эти приложения, чтобы посмотреть, как они работают, и, наконец, проверить стыки каждой программы с внутренними и внешними приложениями, которые она использует.

Технологические исправления не представляют большой сложности, однако в силу самого масштаба проблем, связанных с 2000 годом, мы сталкиваемся с чрезвычайно сложной организационной и управленческой задачей. Вот лишь один пример: имеется ограниченное количество специалистов, обладающих достаточной квалификацией для

решения этой проблемы, – программистов, хорошо знакомых со старыми компьютерными языками, которые давно уже вышли из употребления.

Для координации работ по данной проблеме в пределах тех многочисленных систем, которые использует правительство США, Президент Клинтон образовал совет из представителей более 30 ведомств. Наша первоочередная задача состоит в обеспечении бесперебойной работы государственных служб: выплат по медицинским страховкам, пособий по безработице и сбора налогов. Более масштабная задача, поставленная Президентом, состоит в достижении 100-процентного «соответствия 2000 году», то есть исправления всех компьютерных систем федерального правительства США к марту 1999 г. При совете также созданы рабочие группы, в задачи которых входит взаимодействие по данной проблеме с властями штатов и местными органами, а также анализ соответствующей деятельности частных компаний в 35 секторах экономики – таких, как транспорт, телекоммуникации и финансы.

Кроме того, нас беспокоит состояние работ по проблеме 2000 года в других странах, поскольку многие компьютерные системы пересекают государственные границы, и в условиях глобальной экономики ни одна страна не представляет собой изолированный цифровой остров. Для решения проблемы мы используем каналы международных организаций. ООН приняла резолюцию, содержащую призыв ко всем государствам-членам этой организации предпринять необходимые шаги и к 1 октября представить Генеральной Ассамблее информацию о своей работе в данном направлении. Всемирный банк провел 20 региональных конференций с целью привлечения внимания к этому вопросу. Международный валютный фонд согласился использовать все свое влияние для того, чтобы побудить страны направить ресурсы на решение данной проблемы. Государственный секретарь Маделен Олбрайт направила телеграммы в посольства США по всему миру, поручив послам изучить уровнь готовности стран к 2000 году. Информационное агентство США возглавляет рабочую группу Президентского совета, задачи которой – привлекать общественное внимание к данной проблеме, выполнять функции информационного канала и уделять основное внимание совместному с другими странами планированию действий на случай непредвиденных обстоятельств.

К сожалению, в данный момент, когда до 1 января 2000 г. осталось меньше 500 дней, я считаю, что самой большой проблемой остается недостаточное понимание ситуации главами правительств, журналистами, руководителями предприятий и широкой общественностью многих стран. Первый шаг, который должны предпринять страны и частные компании, – учет всех операций, осуществляемых на компьютерах, и разработка плана внесения необходимых исправлений. Второй критически важный шаг – разработка планов на случай непредвиденных обстоятельств. Президентский совет по проблеме 2000 года обратился ко всем государственным учреждениям США с просьбой разработать два типа планов. Во-первых, какими будут наши действия, если некоторые из наших компьютерных систем выйдут из строя? Во-вторых, что мы будем делать в случае непредвиденных обстоятельств, если сбой дадут системы, связанные с нашими системами?

Сбои, связанные с 2000 годом, вероятно, начнутся до наступления нового тысячелетия, когда на устаревших систем начнут рассчитывать или планировать будущие события. В данный момент трудно точно предсказать, что именно произойдет. В Интернете некоторые эксперты из числа тех, кого обычно не относят к разряду паникеров, предсказывают частые сбои в работе систем, что приведет к отключениям энергии, проблемам с организацией движения, экономическому спаду, а в некоторых регионах, возможно, и к дефициту продовольствия. Хотя я склонен к большему оптимизму, чем авторы этих мрачных прогнозов, меня особенно беспокоят страны, в которых бездействие и непонимание могут привести к воплощению наихудших сценариев. Главное заключается в том, что, предприняв необходимые шаги сейчас, мы сможем свести к минимуму возможные сбои и, будем надеяться, реализовать плавный переход к 2000 году.

ПРИЗРАКИ В МАШИНАХ?

Мартин Либицки
Ведущий научный сотрудник научно-исследовательского института РЭНД

По мнению автора, обеспечение выполнение закона правоохранительными органами является одним из главных направлений в укреплении глобальной информационной безопасности. Он призывает к «гармонизации национальных законов, призванных защищать сети от электронных вторжений, многостороннему сотрудничеству в делах о компьютерных атаках, пересекающих национальные границы, заключению международных договоров о выдаче хакеров, а также готовности к введению санкций против тех, кто покровительствует хакерам». По его мнению, готовность обмениваться информацией о научно-исследовательских и опытно-конструкторских работах, о наличии признаков атак и предупреждений о них, а также о фактах атак и реакции на эти попытки «также может повысить эффективность мер защиты, предпринимаемых каждой страной».

Если кто-то ищет себе новых поводов для беспокойства, то за ними не надо далеко ходить. В нашу жизнь повсеместно проникли компьютеры и другие цифровые устройства. То, что раньше делалось вручную, теперь автоматизировано; на смену аналоговой форме пришла цифровая; некогда изолированные друг от друга вещи стали взаимосвязанными. И нам ничего не остается делать, как полагаться на эти устройства. Если они выйдут из строя, мы пропадем.

Доверчивость к компьютерам, порождаемая зависимостью от них, была бы вознаграждена, если бы компьютеры делали только то, что им положено делать. Некоторые из них действительно выходят из строя сами по себе и мы справляемся с этой ситуацией. Но существует возможность, что они могут вывести из строя нас, попав в руки людей с недобрыми намерениями. В подобных обстоятельствах они могут не просто дать сбой, а раскрыть тайны, которые им доверили, или начать выдавать искаженную информацию – да еще так, что это будет незаметно до тех пор, пока не станет слишком поздно. Приведенные в действие процессы уже невозможно будет повернуть вспять.

В чем причины этой уязвимости? Цифровые устройства работают быстро, стоят недорого, обладают высокой точностью и редко забывают то, что им сказано. Но они воспринимают все настолько буквально, что это повергает в ужас, и обычно не в состоянии понять последствий того, что их просят сделать, или оценить честность тех, кто их просит об этом.

Возможные последствия умышленного вывода систем из строя или внесения в них искажений имеют огромные масштабы. Захватив власть над ключевыми системами, составляющими основу общества, компьютерные хакеры теоретически могут подслушивать телефонные разговоры, делать неправильные соединения и вообще полностью парализовать телефонное обслуживание. Они также могут отключать электроэнергию. Они могут препятствовать движению буквально триллионов долларов, еженедельно переходящих из рук в руки на международных финансовых рынках. Они могут мешать работе аварийных служб. Они способны лишать американских военных возможности быстро реагировать на кризисы за границей. Они в состоянии выведывать личные медицинские секреты. Они могут вносить путаницу в функционирование транспортных систем, подвергая пассажиров опасности, и делать многое другое... Та жизнь, которой мы все живем и которая всем нам хорошо знакома, остановилась бы.

Компьютерные атаки, предпринимаемые с достаточной систематичностью, – это уже настоящая война только другими средствами. Отсюда общее

понятие «информационной войны». Однако в широком смысле слова информационная война – атака на информацию противника и вторжение в процессы принятия им решений – так же стара, как и сами войны. Подобные тактические действия включают в себя психологические атаки, нападения на командование противника, шпионаж и контршпионаж, а также операции против инфраструктур и систем наблюдения противника. Во время Гражданской войны в США (1861–1865 гг.) проводились пропагандистские операции, снайперы держали под прицелом генералов противника, наблюдатели летали на воздушных шарах, диверсанты перерезали телеграфные провода, устраивались кавалерийские пикеты и применялись средства отвлечения кавалерии. И все это справедливо и для информационной войны. Вторая мировая война ознаменовалась уже наступлением электронной войны в форме радиолокации, электронной дезинформации, радиочастотных помех, шифровки и дешифрирования с помощью компьютеров.

Компьютерные атаки превосходно вписываются в этот континуум военных действий. Если можно разрушить штаб противника с помощью артиллерии, что плохого в том, чтобы попробовать менее насильственные средства для проникновения туда и вывода из строя компьютерных систем, управляющих завтрашними сражениями? Согласно представлениям военной стратегии, сложившимся к 1920 г., применение воздушной силы против гражданских целей позволяло избежать ужасы окопной войны. Стратегическая информационная война справляется с этим лучше.

Являются ли современные общества уязвимыми? Большинство информационных систем обладает гораздо меньшей степенью безопасности, чем они могли бы иметь. А многие – даже меньшей, чем должны. Атакам подвергались самые разнообразные типы сетей и систем – Интернет, телефонные системы, транспорт, финансовые учреждения и корпорации.

По всем признакам компьютерные атаки представляют собой серьезную проблему. Согласно недавней оценке ФБР, они обходятся американской экономике в сумму от полумиллиарда до пяти миллиардов долларов в год. Эта оценка допускает многие погрешности, но, в каком-то смысле, они красноречивы. Ведь в действительности никто не знает реального числа кибернетических атак. Многие свидетельства носят характер анекдотов и слухов. Чаще же при оценках приходится просто экстраполировать и делать поправку, учитывая расхожие истины типа «только любители оставляют отпечатки пальцев, профессионалы – никогда» или «люди никогда не хотят говорить о том, как сильно они пострадали». Таким образом, компьютерные атаки подобны айсбергу, а роль «Титаника», по-видимому, отведена Америке.

Но это все теория... Может ли она стать реальностью? В отличие от практически всех других форм ведения войны, проникновение в киберпространство не требует применения силы. Если хакеры проникают в систему, то неизбежно теми же путями, по которым идут ее законные пользователи. Некоторые из этих путей представляют собой особенности системы, другие – ее неустранимые погрешности, то есть как бы тоже особенности, но «незапротоколированные». В обоих случаях движение по этим путям находится под полным контролем любого человека, работающего с данной системой. А поскольку это так, достаточной защитой является бдительность.

Методы защиты действительно существуют. Многие информационные системы являются многослойными. Есть способы отсеять нелегальных пользователей от легальных. Имеются средства, не позволяющие легальным пользователям умышленно или непреднамеренно контролировать компьютерные системы, а также устройства, обеспечивающие безопасность. Так что даже перехват контроля не создает общественной опасности.

Хакеры со своей стороны должны прежде всего обмануть систему, заставив ее принять их за легальных пользователей, например, похитив или разгадав пароль. Во-вторых, они должны получить привилегии контроля (часто путем эксплуатации эндемических ошибок), которых нет у большинства обычных пользователей. Пользуясь подобными привилегиями «суперпользователей», хакеры могут стирать ключевые файлы, заполнять другие сбивающей с толку бессмыслицей или создавать запасной вход для последующего повторного проникновения.

Разумеется, системы защиты при необходимости могут быть более эффективными, чем те, что применяются в настоящее время.

В большинстве систем для ограничения доступа пользуются паролями. Однако с паролями связано много проблем: слишком многие из них легко разгадать, их можно перехватить во время их перемещения по сетям и они слишком часто хранятся на тех участках сервера, где и должны, «по логике вещей», и поэтому их легко найти. Для решения этих проблем применяют такие криптографические методы, такие как цифровые подписи – в этом случае фиксирование и воспроизведение сообщений для получения доступа не срабатывает. Цифровые подписи даже помогают обеспечить возможность отслеживания автора любого изменения, вносимого в базу данных или программу, если оно подписано электронным способом. Это также полезно в случае, если хакер является сотрудником данной организации, которому доверены привилегии при использовании ее систем.

Компьютерные и сетевые операционные системы восприимчивы к таким вводимым хакерами программам, как вирусы (средства программного обеспечения, заражающие одни программы и заставляющие их заражать другие), троянские кони (кажущиеся пригодными для использования программы со скрытыми ловушками) и логические бомбы (программы, бездействующие до специального сигнала). Программы защиты от вирусов могут работать, но если проблемы не исчезают, почему бы не поместить все важнейшие файлы на неизменяемый носитель (например, CD-ROM)? Использование такого носителя, кроме того, может предотвратить стирание или искажение информации цифровыми следами потенциального хакера. В самом деле, с учетом низкой стоимости подобных устройств больше не может быть достаточно весомого предлога для потери информации.

Подвергать системы риску могут также другие системы, воспринимаемые ими как заслуживающие доверия. Против этой опасности можно предпринять две меры предосторожности: отбор перечня заслуживающих доверия систем и ограничение количества сообщений, на которые будет реагировать собственная система. К примеру, банковские системы делают это для защиты своих компьютеров от поступления дезинформации с банкоматов, установленных на улицах. Компьютер игнорирует любую информацию банкомата, не относящуюся к законным операциям. При этом ни одна законная операция не может причинить ущерб банковскому компьютеру.

Наконец, можно прибегнуть к крайней мере предосторожности – отключению от сети. Многие системы, например, атомные электростанции будут работать почти так же хорошо, даже если их отключить от внешнего мира.

Насколько далеко должны заходить владельцы системы, обеспечивая их защиту? Относительно недорогая система безопасности, например, защита от внешнего проникновения и детекторы внедрения, выглядит достаточно эффективной в современных условиях. В конце концов, система в офисе, используемая для делопроизводства, может быть не настолько ценной, чтобы тратить большие суммы на ее защиту – несанкционированное проникновение лишь временно нарушит обычный ритм работы. Многие компании не считают, что они сталкиваются с серьезной угрозой, а потому тратят мало средств на обеспечение безопасности. Возможно, они правы. Но что если они ошибаются? В случае возникновения угроз или по мере их возникновения владельцы систем могут усилить меры безопасности даже на короткое время, например, лишив пользователей возможности входить в систему с домашнего компьютера или ограничив выполнение определенных операций.

В самом деле, именно недостаток надежных систем обеспечения безопасности в масштабах общенациональной информационной инфраструктуры порождает сегодня некую уверенность в том, что компьютерные системы при необходимости можно сделать безопасными. Но ведь эффективная защита от ядерной войны оставалась в течение десятилетий технологически невозможной, и в наши дни, если даже возможна, будет очень дорого стоить... Многие системы могут временно выйти из строя, и мы можем как-то пережить это. Но совсем другое дело, если они долго будут находится в таком состоянии, пока инженеры будут лихорадочно пытаться восстановить их основные функции. Любой, кто намерен подвергнуть риску информационную инфраструктуру США, должен понимать, что сама угроза сделать это – если ее воспримут

серьезно – исчезнет вскоре после ее объявления, поскольку люди отреагируют на нее.

Какой должна быть роль правительства? В состоянии ли те, кто несет ответственность за защиту страны на суше, на море, в воздухе и в космосе, защитить страну и в киберпространстве? И должны ли они это делать?

Правительство способно оказать помощь, но есть многие вещи, которых правительство не может – или не должно – делать. Да, электроэнергия имеет важное значение, но защита энергоснабжения от хакеров почти всецело зависит от того, как энергетические компании управляют своими компьютерными системами. Сюда относятся сетевое и операционное программное обеспечение, которое они покупают, способы конфигурации этого программного обеспечения, предоставление и защита привилегий доступа, а также включение в производственные и распределительные системы компаний различных механизмов защиты от сбоев и их устранения вручную. Невозможно себе представить, что какая-либо энергетическая компания захочет, чтобы правительство «защищало» ее, указывая, как ей решать эти вопросы. И вообще правительство не может построить защитную стену вокруг Соединенных Штатов уже потому, что огромное количество внутренних сетей выходят за их пределы и охватывают весь земной шар.

Правительство может осуществлять и действительно осуществляет соблюдение законов, защищающих от компьютерных атак. В этой области оно добилось некоторых успехов, учитывая то, насколько анонимными и затерявшимися в огромной мире могут быть хакеры. До сих пор большинство известных широкой аудитории хакерских атак, которые были выявлены, оставалось делом рук любителей, а не профессионалов.

Должно ли правительство пытаться остановить информационную войну, угрожая возмездием агрессорам? Предположим, что их личности можно установить. Правительство США может пригрозить ответными действиями типа «око за око». Но у многих «плохих» государств, государств, не признающих международных правовых норм, мало что есть в качестве соизмеримых систем. Скажем, у Северной Кореи нет фондового рынка, который можно было бы разрушить. И наоборот, представляется проблематичной силовая реакция на атаку в информационной войне, в результате которой есть потеря времени и денег со стороны государства-жертвы, но нет раненых.

И хотя многое из того, что может сделать правительство для укрепления безопасности информационных систем, носит косвенный характер, президентская Комиссия по защите критически важной инфраструктуры и другие организации выработали следующие рекомендации:

- обеспечить защиту электронных систем правительства, поскольку они имеют важное значение с точки зрения национальной безопасности и создания стандарта для других;

- использовать научно-исследовательские и опытно-конструкторские работы, а также подключение первых пользователей для содействия быстрой разработке инструментов обеспечения безопасности;

- распространять предупреждения о грозящих атаках в информационной войне – если их можно обнаружить, что само по себе отнюдь не легкая задача;

- содействовать созданию правовых рамок, побуждающих частные структуры к оптимальному уровню защиты своих систем;

- создать независимый информационный центр, способствующий сотрудничеству и конфиденциальному обмену опытом между частными организациями в области защитных мер.

В целом подобного рода меры применяются все шире.

К сожалению, остающиеся в силе и пугающие многих ограничения на шифрование, введенные ранее правительством США, затормозили развитие этого одного из наиболее эффективных инструментов защиты систем. Они также значительно повысили недоверие к тому, что вообще делает правительство в области проблем, связанных с информационной войной.

Что касается международной деятельности, то распространение большинства из этих правительст-

венных мероприятий за рубежом может положить начало целенаправленным международным действиям против информационной войны.

Обеспечение выполнения законов – важнейшая область. Гармонизация национальных законов, призванных защищать сети от электронных вторжений, многостороннее сотрудничество в делах о компьютерных атаках, пересекающих национальные границы, заключение международных договоров о выдаче хакеров, а также готовность к введению санкций против тех, кто покровительствует хакерам – все это может способствовать укреплению глобальной информационной безопасности.

Готовность обмениваться информацией о научно-исследовательских и опытно-конструкторских работах, о наличии признаков атак и предупреждений о них, а также о фактах атак и реакции на эти попытки также может повысить эффективность защитных мер, предпринимаемых каждой страной. Однако эти области часто относятся к сфере деятельности разведывательных органов, которые, как известно из истории, не отличались открытостью в подобных вопросах.

Выводы и перспективы. В период после окончания холодной войны в мире возросло число абсолютно новых, нетрадиционных угроз. Страшных, но пока гипотетических, как, например, ядерный терроризм... К ним относится и информационная война. Чем шире информационные системы охватывают общество – его структуры обороны, коммерческую и повседневную жизнь, – тем большее значение для всех нас приобретает надежность этих систем. Возможность нанесения серьезного ущерба действительно существует, особенно если подобные попытки предпринимает на систематической основе противник, обладающий крупными финансовыми ресурсами. Но, с другой стороны, поразительно и то, что при всей относительной дешевизне информационной войны до сих пор зафиксировано очень мало случаев нанесения действительно значительного ущерба.

Об истинных опасностях, связанных с атаками на компьютерные системы, говорят два обстоятельства. Одно из них – то, как люди реагируют на компьютерную проблему 2000 года. Предположим, что значительная часть мировых информационных систем в полночь 31 декабря 1999 г. выйдет из строя. Приведет ли это к панике и параличу? Или люди быстро найдут способы обходиться без компьютеров? Или в течение некоторого времени они сумеют обходиться без информации? Если же появятся судебные иски, какие прецеденты будут созданы для привлечения людей к ответственности за ущерб, нанесенный в случае выхода их систем из строя?

Другое обстоятельство более недавнее. Если попытаться представить себе наиболее вероятного террориста, развязывающего серьезную информационную войну, это будет некто, кому нечем рисковать (т.е. не страна), у кого где-то спрятаны несколько сот миллионов долларов, кто разбирается в технологии, располагает международной сетью друзей-злодеев и хочет во что бы то ни стало свести счеты (истинные или мнимые) с Соединенными Штатами или какой-то другой страной. Узнаете? Если да, то события следующего года могут показать, попытаются ли подобные «сильные» личности или группы поставить ту или иную страну на колени с помощью информационной войны или приложат свои усилия в каком-то ином направлении.

ЧТО ВЫСШЕЕ ОБРАЗОВАНИЕ ПРОТИВОПОСТАВЛЯЕТ ИНФОРМАЦИОННОЙ ВОЙНЕ

Чарльз У. Рейнольдс
Заведующий Отделением компьютерных наук Университета Джеймса Мэдисона

В эпоху, когда «злобный вандализм, преступность и международная информационная война» могут создавать угрозу для информационной структуры страны, растет спрос на специалистов в области информационной безопасности – говорит д-р Чарльз Рейнольдс. В своей статье он рассказывает о том, как высшая школа сотрудничает с правительством и промышленными структурами в решении этой проблемы в рамках инициативы 1997 г., носящей название «Национальный коллоквиум по безопасности информационных систем» Рейнольдс, исполняющий в 1998 г. обязанности председателя исполнительного комитета этого коллоквиума, также рассказывает об усилиях, предпринимаемых Университетом Джеймса Мэдисона для решения приоритетных общенациональных задач в отражении угроз информационным сетям США.

НЕОБХОДИМОСТЬ ЗАЩИТЫ ИНФОРМАЦИОННОЙ И КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Все стороны нашей жизни и все аспекты социальной, экономической и политической систем все в большей степени зависят от надежного функционирования информационной и коммуникационной инфраструктуры. Наши финансовые и транспортные системы, объекты энергоснабжения и водоснабжения, а также другие важнейшие объекты инфраструктуры зависят в своей работе от информационной и коммуникационной инфраструктуры. Между тем, последняя наиболее уязвима для актов злобного вандализма, преступных действий и международной информационной войны. Все это может создавать угрозу для этой и других зависящих от нее инфраструктур. В связи с этим можно с уверенностью говорить о том, что задача обеспечения безопасности и надежности нашей информационной и коммуникационной инфраструктуры входит в число общенациональных приоритетов.

Чтобы противостоять угрозам, возникающим в условиях эпохи информационных технологий, нашей стране нужны грамотные специалисты, которые понимали бы растущую уязвимость важнейших элементов инфраструктуры, а также профессионалы в области информационной безопасности, которые владели бы самыми современными методами защиты информации.

ОБЩЕНАЦИОНАЛЬНЫЙ ДИАЛОГ СО СТРУКТУРАМИ ВЫСШЕГО ОБРАЗОВАНИЯ

В связи с необходимостью защиты критически важных объектов инфраструктуры нашей страны в мае 1997 г. был учрежден Национальный коллоквиум по безопасности информационных систем, перед которым была поставлена задача организовать диалог между лидерами в сфере государственного управления, промышленности и высшего образования для совместной разработки требований к обучению в сфере информационной безопасности. Коллоквиум также ставит перед собой задачу стимулировать разработку и расширение учебных программ по информационной безопасности, особенно на уровне базового университетского курса и программы для получения степени магистра.

На своей второй ежегодной встрече, которая состоялась в июне 1998 г. в Университете Джеймса Мэдисона в г. Харрисонбурге, штат Виржиния, участники коллоквиума договорились о том,

что их работа будет способствовать разработке учебных программ, учитывающих требования, сформулированные правительством и промышленными кругами, и основанных на самом передовом опыте.

Участники коллоквиума также ставят перед собой задачу оказания содействия учебным заведениям путем дальнейшего создания и обмена ресурсами, связанными с обучением в области информационной безопасности. Участники коллоквиума призывают учебные заведения к включению курсов по безопасности информационных систем в различные учебные планы, в соответствии с интересами потребителей в 21-м веке, а также курсов, призванных удовлетворить растущий спрос на профессионалов в области безопасности информационных систем.

На своем ежегодном заседании в 1998 г. Коллоквиум принял широкую программу действий. Поставлены задачи перед правительственными учреждениями, промышленными структурами и высшими учебными заведениями, которые они будут выполнять как на индивидуальной основе, так и в сотрудничестве друг с другом.

Среди совместных задач особое место отводится определению тех знаний, навыков и подходов, которыми должен обладать профессионал в области информационной безопасности и на основе которых могли бы быть разработаны соответствующие стандарты. Поскольку информационная безопасность как область знаний только формируется, необходимо выявить лучшие примеры практической деятельности в этой области и включить их в профессиональные стандарты, способствуя их совершенствованию. Наконец, все три группы участников коллоквиума должны преодолеть нежелание специалистов в области информационной безопасности следовать каким-либо стандартам, поскольку любая профессиональная деятельность предполагает элемент дисциплины.

Обсуждая рекомендации для частных промышленных структур, участники коллоквиума считают, что промышленный сектор должен обеспечивать учебные заведения финансовыми средствами, оборудованием и компьютерными программами, помогать университетам поддерживать надежное функционирование имеющихся у них компьютерных систем, проводить курсы обучения на местах для профессорско-преподавательского состава, в том числе и для тех, кто ранее не работал в области информационной безопасности, а также финансировать стажировки студентов.

Коллоквиум призвал правительство к разработке курсов в области информационной безопасности и предоставлении их высшей школе, а также к стимулированию создания университетских центров по защите инфраструктуры по образу и подобию центров изучения материалов под эгидой Национального научного фонда и центров изучения проблем транспорта под эгидой Министерства транспорта.

Участники коллоквиума призвали специалистов в области информационной безопасности к установлению более тесных контактов с преподавательским составом высших учебных заведений, к организации дополнительного числа конференций по вопросам информационной безопасности, созданию новых вебсайтов в Интернете, увеличению числа публикаций по вопросам защиты информационных сетей США. Они также подчеркнули необходимость создания формальной системы премирования лучших учебных программ в области информационной безопасности.

Концентрируя свое внимание на высших учебных заведениях, участники коллоквиума призвали их увеличивать число учебных программ, делающих упор на информационной безопасности, и включать такие курсы в базовые учебные программы.

Особое значение придается изучению этических и культурных аспектов, связанных с современными информационными системами. Здесь следует обратить внимание на то, как сохранить традиционные ценности в условиях информационной эры и какие изменения могут быть внесены в эти ценности.

Поскольку человек формирует свои этические и культурные ценности на раннем этапе жизни, рекомендуется, чтобы высшие учебные заведения также разрабатывали учебные программы в области информационной безопасности для средних школ, при участии последних.

Признав, что высшее образование также представляет собой профессиональную деятельность, опи-

рающуюся на определенные стандарты, участники коллоквиума рекомендовали учебным заведениям обращаться в соответствующие организации по аккредитации за помощью в вопросах включения в учебные программы курсов по информационной безопасности.

Наконец, исходя из того, что повышение уровня образования необходимо на протяжении всей жизни человека в условиях быстро развивающегося технологического общества, участники коллоквиума рекомендовали высшим учебным заведениям организовать у себя программы повышения квалификации для специалистов, уже работающих в области информационной безопасности.

Участники коллоквиума рекомендовали, чтобы преподаватели курсов по информационной безопасности разрабатывали методики проведения лабораторных занятий и обменивались ими, создавали компьютерные игры, формирующие ценности, необходимые для воспитания ответственных и информационно грамотных работников, создавали возможности для обмена учебными материалами и выпускали больше учебных пособий, особенно по практической стороне дела.

В своей программе действий участники коллоквиума также призвали специалистов в области юридического образования оказать содействие американским юристам в более глубоком понимании вопросов, связанных с информационной безопасностью.

МЕТОДЫ ОБУЧЕНИЯ С ПОМОЩЬЮ ИНТЕРНЕТА

Для современного технологического общества характерен спрос на профессиональных специалистов в области информационной безопасности. Поскольку технологии все время видоизменяются, профессионалы должны на протяжении всей жизни обновлять и расширять свои знания и навыки. При этом они должны быть готовы к переориентации на новые специальности, поскольку и в этой области рынок труда меняется по мере изменения тенденций в технологическом развитии.

В последние годы ощущается особенно острая нехватка специалистов в области информационной безопасности. Такой спрос на квалифицированных специалистов, в свою очередь, вызывает спрос на новые возможности в области образования, реализация которых давала бы стране новых профессионалов и перепрофилировала уже работающих специалистов на работу в новых направлениях. Между тем, было бы наивно полагать, что уже работающие профессионалы захотят прерывать свою карьеру и семейный уклад жизни и превращаться в студентов, посещающих традиционные университетские занятия. Именно в связи с необходимостью в постоянном обучении профессиональных специалистов без отрыва от их карьеры или семейной жизни и возникает такой большой интерес к обучению на основе Интернета. Университет Джеймса Мэдисона откликнулся на это требование времени и в рамках своей магистратуры создал программу профессионального обучения в области информационной безопасности на основе Интернета.

Речь идет об основанной на возможностях Интернета программе обучения, предусматривающей договорные отношения с организациями, которые могут обеспечить надежность процедур прохождения тестов своими сотрудниками.

Программа состоит из 13 курсов продолжительностью семь недель каждый и в целом занимает немногим более двух лет. Группа обучающихся, называемая «когортой», вместе начинает обучение и вместе проходит все 13 курсов по очереди.

Основанная на Интернете программа обучения сочетает в себе самостоятельные занятия с работой под руководством преподавателей, а также групповые занятия, которые координируются неким центральным органом, предоставляющим целую сеть услуг. С помощью преподавателей и компьютерных технологий обеспечивается система передачи знаний обучающимся, в рамках которой поддерживаются высокие образовательные стандарты и в то же время допускается гибкость, основанная на учете потребностей обучающихся. Предусмотрено проведение групповых электронных дискуссий и критического анализа концепций, связанных с информационной безопасностью. Каждый курс состоит из серии материалов, рекомендованных для прочтения, и задач, которые должны решить учащиеся.

Презентации концепций может видеть любой человек в мире и в любое время, если у него есть доступ к Интернету. Занятия в каждом классе ориентированы на практическое закрепление усвоенных концепций и материалов.

ПРОГРАММА ОБУЧЕНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УНИВЕРСИТЕТЕ ДЖЕЙМСА МЭДИСОНА

Тот, кто проходит полный курс обучения в рамках программы по информационной безопасности в Университете Джеймса Мэдисона, получает степень магистра компьютерных наук со специализацией в вопросах информационной безопасности. Данная программа основана на нормативе, утвержденном Агентством национальной безопасности, и предусматривает получение знаний и навыков, необходимых для понимания взаимосвязи между информационной безопасностью и информационными технологиями, а также для умения соотносить технические и человеческие составляющие информационной безопасности и информационных технологий. В основу курса, предлагаемого в Университете Джеймса Мэдисона, положены знания в области административного управления, менеджмента, анализа, а также применения компьютерных технологий с упором на вопросы информационной безопасности. Управление программами в области информационной безопасности включает в себя поддержание и защиту конфиденциального характера информации, ее целостности, доступности, подлинности и применимости в границах приемлемого риска.

Обучаясь в группах, участники программы:

- Получают знания и навыки, требующиеся для понимания взаимосвязи между информационной безопасностью и технологическим развитием информационных систем и необходимые для реализации программ по защите от преступных посягательств и выявлению таких посягательств;

- Получают дополнительную подготовку в технических вопросах, в вопросах надзора и политики, связанных с информационной безопасностью и компьютерными технологиями с точки зрения уязвимости, возможных угроз и анализа возможных рисков;

- Приобретают более широкие знания, необходимые для эффективной работы специалистов, менеджеров, администраторов и практических работников в области информационной безопасности в связи с планированием, анализом и реализацией методов и программ обеспечения информационной безопасности;

- Учатся находить взаимосвязь между техническими и человеческими составляющими информационной безопасности и компьютерных технологий применительно к защите систем;

- Учатся разбираться в вопросах, связанных с базами данных и устройством информационных систем, операционных систем и сетей, а также с разработкой компьютерных приложений, которые применяются для предотвращения преступных посягательств и выявления случаев проникновения в компьютерные сети.

Программа обучения начинается с подготовительной части, предназначенной для тех, кому нужно усовершенствовать вычислительные навыки, прежде чем переходить к основной части программы. Затем следуют три курса в области компьютерных наук, предусматривающие изучение методов управления базами данных, операционными системами и компьютерными сетями, а также методов разработки компьютерных приложений. Это создает прочную основу для третьего этапа обучения, на котором происходит знакомство с принципами информационной безопасности, концепциями надежности информационных систем, а также методами безопасного хранения и передачи информации, в частности, путем ее кодирования. На четвертом этапе происходит изучение методов управления и администрирования деятельности по обеспечению информационной безопасности, в том числе анализа рисков и слабых мест, методов и процедур проверки надежности информационных систем, а также юридических, этических и корпоративных аспектов. На последнем этапе обучения перед участниками программы ставится задача комплексного применения всех полученных знаний в ходе анализа уровня безопасности конкретной информационной системы.

ОБМЕН ОПЫТОМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫГОДЕН КАК ЧАСТНОМУ, ТАК И ГОСУДАРСТВЕННОМУ СЕКТОРУ

Интервью с Ховардом Шмидтом, начальником Отдела информационной безопасности корпорации «Майкрософт»

Правительственные учреждения и многие частные корпорации теперь имеют возможность «связываться друг с другом и оказывать друг другу содействие» в случае возникновения угроз в адрес их информационных ресурсов и других критически важных систем, – говорит Ховард Шмидт, заведующий Отделом информационной безопасности корпорации «Майкрософт». Он приводит примеры широкого сотрудничества между корпорациями по вопросам, связанным с угрозой информационной войны. «Когда речь заходит о безопасности, то вопрос о конкуренции отодвигается на задний план, – считает Шмидт. – Мы разрабатываем стандарты вместе с нашими конкурентами и партнерами с тем, чтобы всем вместе создавать и поддерживать надежный уровень безопасности».

ВОПРОС: Как вы оцениваете уязвимость важнейших инфраструктур США к вторжению в их компьютерные системы? Насколько готовы США к защите от подобных посягательств?

ШМИДТ: Моя оценка во многом совпадает с той, которую дает президентская Комиссия по защите ключевых объектов инфраструктуры: необходима дальнейшая работа в этой области. Как показал анализ, эти вопросы не были до сих пор приоритетными. Что же касается нашей способности противостоять таким посягательствам, то я думаю, что президентская Комиссия по защите ключевых объектов инфраструктуры уже многое сделала для того, чтобы объединить усилия частного и государственного секторов в целях коллективного противостояния такому вторжению и принятия ответных мер.

ВОПРОС: Вы сотрудничаете с этой комиссией?

ШМИДТ: Да, мы сотрудничаем с этой комиссией. Их представители несколько раз приезжали к нам сюда в Редмонд, штат Вашингтон. Я тоже несколько раз ездил в Вашингтон на встречи с ними. По сути дела, мы создаем довольно широкий форум, в рамках которого представители правительственных организаций и частного сектора могут обсуждать пути совершенствования инфраструктуры.

ВОПРОС: Какие организационные изменения осуществляются в вашей компании в связи с возникновением новых угроз современным технологиям?

ШМИДТ: Позвольте мне перефразировать ваш вопрос, потому что мы не считаем их угрозами, направленными против технологии. Мы рассматриваем это как применение технологии для создания новых возможностей совершать какие-то действия, направленные против более широкой аудитории. В принципе, наша позиция такова: характер самих угроз не изменился, но теперь они усилены новыми технологиями.

В связи с этим год назад мы создали программу, которой очень гордимся – «Программу информационной надежности Майкрософт», позволяющую нам связать воедино ряд направлений работы внутри компании по защите нашей информации или обеспечению ее надежности. Мы создали специальную организационную структуру, объединяющую различные программы и функции, в том числе план действий в чрезвычайных ситуациях, систему сохранения и классификации данных, стратегию резервной поддержки, группу информационной безопасности как таковую, группу физической безопасности в той части, которая касается охраны информации, а также группу безопасности программных продуктов, поскольку «Майкрософт» разрабатывает программное обеспечение.

В рамках этой структуры установлены связи между всеми направлениями данной области. Это касается не только безопасности нашей информации и систем, но и включения в разрабатываемые нами продукты опыта, накопленного в области информационной безопасности, в целях повышения их качества.

ВОПРОС: Если говорить о стратегиях защиты от информационной войны, в какой степени вы согласуете свою деятельность с другими корпорациями?

ШМИДТ: В достаточно большой степени. По сути дела, у нас существует целый ряд различных групп. Например, Ассоциация по вопросам безопасности информационных систем, представляющая собой некоммерческую организацию, участники которой работают в сфере информационной безопасности. В нее входят представители «Чарльз Шваб Компани», «Ю-эс Спейс Эллайанс», «Эр Тач Селлюлар», а также представители правительственных организаций. Мы принимаем участие в конференциях и сотрудничаем с «Гартнер Груп», крупной консультационной фирмой в компьютерной области. Мы также участвуем в инициативе, выдвинутой бывшим сенатором Сэмом Нанном, который многое сделал в области защиты инфраструктуры. Он координирует работу регулярного форума по вопросам информационной безопасности при Технологическом институте штата Джорджия в Атланте, в котором мы тоже принимаем участие.

Так что в частном секторе мы организовали довольно интенсивный обмен информацией и передовым опытом в области безопасности. Существуют и другие группы, например, Федеральный комитет расследований в компьютерной области и Ассоциация по расследованию преступлений в области высоких технологий, в состав которых входят представители как государственного, так и частного сектора. У нас установлены хорошие связи, и мы довольно тесно сотрудничаем друг с другом.

Когда речь заходит о безопасности, то вопрос о конкуренции отодвигается на задний план. Мы разрабатываем стандарты вместе с нашими конкурентами и партнерами, с тем, чтобы всем вместе создавать и поддерживать надежный уровень безопасности.

ВОПРОС: Не могли бы вы более подробно рассказать о том, какую работу проводит ваша организация с государственным сектором в решении новых проблем, связанных с информационными системами?

ШМИДТ: Для этого мы используем несколько путей. Разумеется, разработчики программ, которыми мы все пользуемся, поддерживают очень тесные связи со всеми правительственными организациями, с тем, чтобы выпускаемые ими продукты удовлетворяли потребности федерального правительства в области обеспечения безопасности объектов инфраструктуры.

С другой стороны, поскольку мы предоставляем услуги в режиме “on-line”, мы сами входим в состав инфраструктуры и часто содействуем людям, проводящим расследования в этом режиме, оказывая им техническую поддержку. В настоящее время у нас действует круглосуточная телефонная линия для сотрудников правоохранительных органов, которые занимаются расследованием незаконной деятельности в Интернете.

Мы также регулярно проводим встречи, где обсуждается передовой опыт. Мы часто выступаем с докладами в государственных учреждениях. Так, например, несколько месяцев назад я выступал с обширным докладом в Университете национальной обороны в Вашингтоне. В сентябре я участвовал в конференции на тему: «Защита кибернетического пространства–98», проводившейся в Вашингтоне. Мы участвуем в подобного рода форумах, поскольку они дают возможность для обмена опытом, который идет на пользу всей нашей индустрии.

ВОПРОС: Считаете ли вы, что правительство должно играть более заметную роль в деле защиты важнейших объектов инфраструктуры, и если да, то какова должна быть эта роль, по вашему мнению?

ШМИДТ: В принципе, я считаю, что роль правительства должна состоять в продолжении сотрудничества с частным сектором. И я думаю, что президентское директивное решение за номером 63

(ПДР 63), в соответствии с которым создано Управление по обеспечению работы критически важных объектов инфраструктуры, создает хорошую основу для продуктивного сотрудничества правительства с частным сектором. Я думаю, что при такой позиции правительства – даже без нового законодательства или новых регуляций – мы можем многое сделать вместе с правительством для того, чтобы важнейшие объекты инфраструктуры на самом деле были хорошо защищены.

ВОПРОС: Видите ли вы противоречия в Соединенных Штатах между корпорациями, испытывающими потребность в информации, и правительством, стремящимся к обеспечению защиты информации?

ШМИДТ: В принципе, я не вижу каких-либо противоречий. Я думаю, что мы все хотим обеспечить максимальную безопасность и одновременно конфиденциальность корпоративной, правительственной, личной и другой информации. И хотя между нами могут быть определенные разногласия в подходах к этой проблеме, определяющее значение имеет все-таки тот факт, что все мы согласны с необходимостью коллективных усилий с целью защиты инфраструктуры.

ВОПРОС: Существуют ли пути более тесного сотрудничества между государственным и частным сектором в целях разработки эффективных средств защиты от действий террористов или других враждебных сил?

ШМИДТ: По-моему, я уже ответил на этот вопрос; главное здесь состоит в том, что сегодня между различными государственными организациями и множеством частных компаний наведены мосты и существуют возможности для взаимодействия и взаимопомощи. Я считаю, что сегодня мы можем предоставить эффективную техническую помощь группам, поддерживающим правоохранительные органы. Конечно, мы еще не завершили разработку форм осуществления этой поддержки, но она оказывается уже сейчас и будет совершенствоваться в будущем.

ВОПРОС: Какие средства защиты встраивает корпорация «Майкрософт» в свои программы, помогая потребителям защитить себя от информационных посягательств?

ШМИДТ: Вообще-то я не занимаюсь этим непосредственно, но могу сказать, что представители «Майкрософт» проводят регулярные встречи с потребителями. Нас всех беспокоят вопросы информационной безопасности. Разработчики программных продуктов «Майкрософт» постоянно работают над повышением уровня их защиты, сотрудничая как с нами, так и со специалистами по информационной безопасности, поскольку мы сами работаем на своих программах. Таким образом, обеспечивается постоянная обратная связь для того, чтобы выпускаемые продукты были максимально защищены сейчас и в будущем, в случае выявления дополнительных слабых мест.

ВОПРОС: Считаете ли вы, что нынешний уровень технологического контроля позволяет создать достаточную защиту от компьютерных вирусов и компьютерных террористов?

ШМИДТ: В последнее время много говорят о различных вирусах и тому подобных вещах. По мере их появления мы рассматриваем их как любой другой вид незаконной деятельности. Мы, представители частного сектора и правительства, вместе пытаемся бороться с ними и предпринимать профилактические меры в отношении таких угроз, пытаясь предвидеть действия, которые могут быть кем-то предприняты в будущем. Пока мы делимся друг с другом информацией и пользуемся крупными информационными системами, от которых во многом зависит жизнь общества, всегда будут люди, которые попытаются нанести вред таким системам. Главное состоит в том, что, располагая технологиями, грамотными специалистами и понимая грозящие нам опасности, мы, как я полагаю, сумеем обеспечить достаточно эффективную защиту этих систем.

ВОПРОС: Есть ли у вас технология, с помощью которой можно защитить компанию от непрерывного потока сообщений, посылаемых компьютерным террористом по электронной почте?

ШМИДТ: Да, существует целый ряд встроенных механизмов, а также усовершенствований и дополнительных программ, которые мы включаем в свои программы и которые используют другие компании для решения подобных проблем. В рамках нашей «Программы партнерства в вопросах безопасности» мы вместе с другими компаниями

разработали ряд очень и очень хороших средств – я имею в виду компьютерные программы – которые могут реально помочь в деле защиты от вирусов, перехвата «бомб», присылаемых по электронной почте, и тому подобных вещей. Мы уже далеко продвинулись в решении этой проблемы. ◉

СТРАТЕГИИ БОРЬБЫ С УГРОЗАМИ ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ

Джеймс А. Лингерфелт
Консультант ИИМ по вопросам общественной безопасности

По мнению Лингерфелта, эксперта по технологиям и стратегическому планированию в правоприменении, самая большая угроза информационным системам и базам данным исходит не от компьютерных суперхакеров, преследующие «злые» цели, а скорее из источников, которым мы абсолютно доверяем. Автор подчеркивает, что «реалистичная оценка угроз и требований в сфере безопасности с последующей разработкой и реализацией соответствующих мер безопасности может обеспечить эффективную защиту от большинства угроз и не потребует чрезмерных расходов». В своей статье он указывает на те области, где наиболее часто возникают реальные угрозы, и предлагает семь основных стратегий планирования мер безопасности, связанных с защитой информационных технологий.

Правоохранительные и следственно-судебные органы получили беспрецедентную возможность с помощью информационных технологий изменить методы своей работы и сделать их более совершенными. Между тем, многие ведомства неохотно используют эту возможность, поскольку опасаются, что, заменив или дополнив свои закрытые компьютерные системы персональными компьютерами и автоматизировав отчеты и компьютерные сети, они станут более уязвимыми к посягательствам со стороны хакеров. Высокая стоимость мер по защите всей информационно-технологической системы от несанкционированного доступа со стороны суперхакеров в сочетании с потенциальным ущербом, связанным с потерей секретной и важной информации, может казаться достаточно убедительным основанием избегать возможного риска от использования информационных технологий, несмотря на все связанные с ними преимущества.

Несомненно, информационные системы, ресурсы и базы данных, благодаря их стремительному развитию, становятся все более уязвимыми к несанкционированному доступу. Но в действительности символическая фигура сверхумного хакера, которая наводит такой большой страх, редко представляет собой наибольшую угрозу. Наибольшая опасность для компьютерных систем и баз данных исходит скорее из источников, которым мы вполне доверяем и на которые не обращают внимания полиция и следственно-судебные органы. Реалистичная оценка угроз и требований в сфере безопасности, с последующей разработкой и реализацией соответствующих мер безопасности может обеспечить эффективную защиту от большинства угроз и не потребует чрезмерных расходов.

ФАКТЫ И ИХ ВОСПРИЯТИЕ

Многие правоохранительные органы вкладывают большие средства в информационные технологии. Но это сопровождается увеличением числа случаев вторжения хакеров в информационные системы полиции.

Появляется все большее сообщений и о незаконном использовании информации, хранящейся в полицейских базах данных, о хищении информации и основанных на информационных технологиях ресурсов, которыми располагает полиция. Подобные случаи стали такими частыми, что многие полицейские подразделения боятся открывать свои информационные системы. Между тем, новые требования, предъявляемые к правоохранительным органам, заставляют их изменять методы получения, обмена и распространения информации.

Эти изменения связаны с необходимостью введения информационных систем на местах, упорядочения рабочих процессов, передачи информации за

пределы правоохранительных органов и обмена информацией с другими организациями и отдельными лицами.

Некоторые организации привлекают свой персонал к выполнению новых функций, увеличивая тем самым нагрузку оперативных сотрудников. Другие внедряют новые системы, но используются они только для выполнения новых функций и не становятся частью или дополнением старой системы. Это только усложняет работу информационных технологий и увеличивает затраты на нее – как в кадровом отношении, так и в отношении времени и денег.

Как уже отмечалось, внутренние опасности, исходящие из источников, которым мы вполне доверяем, приносят более серьезный ущерб, чем вторжения в информационные системы извне. Ниже приводятся несколько случаев, вызванных именно такими внутренними причинами:

- Компьютерная сеть целого управления была выведена из строя вирусом, попавшим в нее с дискет, розданных плановым отделом для сбора статистических данных о деятельности управления.

- Начальник разведывательного управления, в ведении которого находилась многоступенчатая разведывательная структура, прикрепил к своему монитору листок, на котором был записан его код пользователя и пароль, а также подробные инструкции о порядке входа в информационную систему.

- Высокопоставленный сотрудник полицейского управления продал организованной преступной группировке файл, в котором содержались описания и номерные знаки всех автомобилей, находившихся в пользовании тайных полицейских агентов.

- Неопытный сетевой администратор, организовывавший компьютерную сеть в полицейском управлении, предоставил всем пользователям привилегии управления данной сетью.

- Программистам, создававшим приложения в крупном полицейском управлении, было разрешено ввести в систему новый код без предварительной тщательной проверки, в результате чего вся система вышла из строя на сутки.

- Власти одного из штатов создали вебсайт в Интернете, но не позаботилось о создании защиты доступа. В тот же день идентификатор пользователя и парольный файл попали в распоряжение хакеров. Надо отдать должное властям этого штата – они рассказали о случившемся властям других штатов, что позволило последним избежать повторения ошибки.

Все вышеприведенные случаи не имеют никакого отношения к внешнему вторжению суперхакера. В последнем примере речь идет о том, что создатели информационного ресурса просто оставили дверь открытой. Все эти инциденты могли быть предотвращены при наличии элементарного планирования, более серьезной подготовки сотрудников и более ситсематического надзора.

Подводя итог сказанному, можно утверждать, что широкое использование информационных технологий повысили угрозу вторжения извне. Однако пропорции этой угрозы не меняются. Если представить ее в виде отдельного куска пирога, то увеличивается лишь сам пирог. Возрастает ли угроза? Да. Меняется ли ее характер? Нет.

Повышение уязвимости к угрозам безопасности компьютерных систем объясняется несколькими причинами:

- Новые методы ведения дел: государственный сектор повторяет путь частного сектора, но с опозданием примерно на 5 лет.

- Широкое распространение информационных технологий: компьютеры и компьютерные сети присутствуют повсюду в нашей жизни.

- Снижение затрат: применяемые сегодня технологии перестали быть дорогостоящими. По любым меркам стоимость базовых компьютерных систем сегодня ниже, чем когда-либо. При этом затраты на новые технологии уменьшаются быстрее, чем всего несколько лет назад, в результате колоссального научного прогресса и роста конкуренции.

НОВЫЕ МОДЕЛИ БИЗНЕСА

В процессе перехода от централизованного управления к децентрализованному на смену штаб-квартире, где собирается информация и принимаются решения, приходят местные автономные подразделения, применяющие информационные технологии. В области самих информационных технологий это означает переход от закрытых систем к сетям – как внутренним, так и внешним. Рассредоточение информации означает большие трудности, связанные с защитой ресурсов, контролем над операциями и ответом на возникающие проблемы. Появляется больше уязвимых мест. Положительный аспект, однако, состоит в том, что рассредоточение информационных технологий чрезвычайно повышает производительность, а вложенные средства часто окупаются быстрее, чем за год.

Организации в частном секторе стали делать упор на специализацию вместо того, чтобы делать все для всех. Сейчас в компаниях работает гораздо меньше сотрудников. Это позволяет им избегать проблем, связанных с трудовыми отношениями и изменениями в штатном расписании. Остаются лишь те должности, которые имеют прямое отношение к решению стоящих перед компанией задач. В новых компаниях часто возникает необходимость в привлечении работников со стороны для выполнения вспомогательных и административных функций, в том числе и связанных с инфорационными технологиями. Следственно-судебные и правительственные органы также движутся в направлении упорядочения своей деятельности, снижения затрат и повышения качества предоставляемых услуг.

Кроме того, стало очень трудно удерживать квалифицированный персонал, работающий в области информационных технологий. Уровень заработной платы в государственных организациях не может конкурировать с уровнем оплаты труда в частном секторе, и поэтому уволившимся сотрудникам трудно найти замену. Это обстоятельство также побуждает государственные учреждения нанимать работников со стороны для выполнения определенных задач.

Другим характерным моментом сегодня стала повышенная текучесть руководящих работников и менеджеров. По мере того, как компании сокращают число своих работников или переманивают способных работников друг у друга, возникает угроза того, что руководители или менеджеры среднего звена, уходя из компании, могут прихватить с собой принадлежащую ей интеллектуальную собственность. В одном случае удалось доказать состав такого преступления, когда выяснилось, что конфигурация файловых директорий в компьютере одного из менеджеров полностью идентична той, которой он пользовался на прежнем месте работы в другой компании. Редко признаются или становятся достоянием общественности довольно частые случаи, когда компании, проводящие сокращения своих сотрудников, теряют миллионы долларов в виде похищенного оборудования, программного обеспечения, канцелярских принадлежностей и мебели – если сотрудники, которые подпадают под сокращение, уведомляются об этом заранее.

Несмотря на некоторые преимущества, привлечение внештатных работников к выполнению информационно-технологических функций может создавать дополнительные риски для информационной безопасности. В связи с этим особое значение должно придаваться разработке плана информационной безопасности, особенно когда критически важные для компании информационные функции выполняются работающими по контракту внештатными сотрудниками. Организация может потребовать, чтобы при приеме на работу по контракту человек проходил определенную проверку его предыдущей деятельности.

СТРЕМИТЕЛЬНЫЙ РОСТ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Компьютеры и компьютерные сети стали неотъемлемой частью почти всех сторон нашей жизни. Мошенничество, хищения и распространение нелегальной информации и материалов стали возможными благодаря компьютерам, компьютерным сетям и Интернету, которыми все мы пользуемся. Возникают новые виды правонарушений, а старые обретают новую жизнь.

К счастью, более широкое применение компьютеров привело к появлению более совершенных технологий, стандартов и критериев для оценки качества. Опыт ошибок позволил усовершенствовать технологии, и это принесло пользу всем нам.

Практика в области информационной безопасности также стала более совершенной, поскольку учитывает прошлые ошибки, и был разработан ряд оптимальных методов работы. Дорогу прокладывает частный сектор. Большинство новых продуктов (как оборудование, так и программное обеспечение) выпускается с уже встроенными средствами защиты. Как используются эти средства защиты и используются ли они вообще – это уже другой вопрос.

СНИЖЕНИЕ ЗАТРАТ

По любым критериям, затраты на приобретение базовых информационных технологий сегодня ниже, чем когда бы то ни было. Почти любой человек может позволить себе купить компьютер.

Наряду со снижением стоимости информационных технологий сегодня государственный сектор располагает большими средствами для приобетения компьютеров и программ, чем за последние двадцать лет, то есть с конца 60-х и начала 70-х годов. Так, например, инициативы, связанные с решением компьютерной проблемы 2000 г. и компьютерными преступлениями, предусматривают выделение миллиардов долларов на вполне конкретные цели: модернизацию или замену информационных систем, которыми пользуются государственные организации. Это дает следственно-судебным органам прекрасную возможность для учета информационной безопасности при разработке и внедрении новых методов работы и новых компьютерных систем. Дело в том, что попытки просто перестроить систему информационной безопасности обходятся слишком дорого и обычно не дают результатов.

ПЛАНИРОВАНИЕ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В научно-фантастической книге «Руководство для путешествий автостопом по галактике» можно прочитать такое правило:

НЕ НУЖНО ПАНИКОВАТЬ. Этот совет хорошо подходит и для тех, кто занимается планированием в области информационной безопасности. Многие организации отказываются от вложения средств в информационные технологии, поскольку убеждены в том, что на них немедленно навалятся орды хакеров и лиц, желающих поживиться чужой собственностью.

Несмотря на повышение степени уязвимости и увеличение потенциального числа посягательств, в настоящее время уже имеется опыт и средства, необходимые для приобретения систем электронной защиты и их постоянного совершенствования. При наличии эффективного и заблаговременного планирования можно рассчитывать на то, что большинство посягательств будет быстро и эффективно отражено, а ущерб, нанесенный остальными, будут сведен к минимуму.

При планировании развития информационных технологий очень важно не терять из виду общую картину: план развития должен быть непосредственным продолжением плана деятельности организации. В нем должны содержаться требования, выполнение которых обеспечивало бы реализацию задач организации. Он не должен превращаться в список пожеланий в области информационных технологий. Необходимо концентрировать внимание на цели, а не на методах ее достижения. Обычно существует несколько путей достижения цели, при этом разница в затратах может быть весьма ощутимой. Нужно четкое обоснование того, на что будет потрачен каждый доллар. При этом вопросы информационной безопасности должны быть заложены в план по информационным технологиям с самого начала.

Следует обеспечивать простоту сетевых структур. Это обеспечивает существенные преимущества с точки зрения информационной безопасности. Разветвленные системы, вне зависимости от того, как тесно они связаны друг с другом, подвержены вторжению во многих точках. В связи с этим возникает необходимость увеличения числа средств защиты и вспомогательных систем, что, в свою очередь, ведет к увеличению затрат.

СЕМЬ СТРАТЕГИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1. ПРЕЖДЕ ВСЕГО СИСТЕМА ДОЛЖНА БЫТЬ ПРОСТОЙ. Если система носит слишком сложный характер, пользователи будут избегать ее или пытаться обходить, нанося тем самым ущерб ее безопасности и уменьшая степень ее полезности.

Современные средства информационной безопасности могут быть достаточно скромными и эффективными.

2. НЕОБХОДИМО ЗАРАНЕЕ РАЗРАБАТЫВАТЬ СТРАТЕГИЮ, ПРОЦЕДУРЫ И САНКЦИИ. Они должны отвечать потребностям пользователей, характеру приложений и защищаемой информации. Необходимо самое строгое следование этим принципам. Лучше вообще не иметь никакой стратегии, процедур и санкций, чем иметь такие, какие носят «беззубый» характер.

3. СЛЕДУЕТ ОБУЧАТЬ СОТРУДНИКОВ ПОЛЬЗОВАТЬСЯ СИСТЕМОЙ И ОБРАЩАТЬ ИХ ВНИМАНИЕ НА СТРАТЕГИЮ, ПРОЦЕДУРЫ И САНКЦИИ. Необходимо усиливать такую подготовку за счет обсуждения и распространения новостей, связанных, например, со случаями вторжения в компьютерные системы или другими нарушениями подобного рода.

4. ЛУЧШЕ КАК МОЖНО ШИРЕ ИСПОЛЬЗОВАТЬ ГОТОВЫЕ ПРОДУКТЫ, ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ ЗАЩИТУ, ЧЕМ РАЗРАБАТЫВАТЬ СВОИ СОБСТВЕННЫЕ. На это есть несколько причин, ведь потребности бизнеса четко очерчены. Следственно-судебные органы используют методы сбора и обмена информацией для выявления связей между различными людьми и между людьми и событиями. Готовые продукты, основанные на известных стандартах, проходят испытания и сертификацию, а потребителей, пользующихся этими продуктами, можно опросить и изучить их опыт. Даже когда речь идет о новых продуктах, методы и результаты их испытаний могут быть подвергнуты соответствующей экспертизе. Самое главное состоит в том, что к стандартным коммерческим продуктам обычно прилагается подробная документация, предназначенная для пользователей и технического персонала. Когда же подобные приложения разрабатываются в самой организации, очень часто упускаются из виду такие моменты, как составление документации и проведение испытаний.

5. ИНФОРМАЦИЯ, РЕСУРСЫ И ПОЛЬЗОВАТЕЛИ ДОЛЖНЫ ПОДРАЗДЕЛЯТЬСЯ НА КАТЕГОРИИ. СЛЕДУЕТ ЗАЩИЩАТЬ ИНФОРМАЦИЮ И РЕСУРСЫ В ЗАВИСИМОСТИ ОТ СТЕПЕНИ ИХ ЦЕННОСТИ. Конфиденциальные разведывательные отчеты должны обеспечиваться высокой степенью защиты. С другой стороны, общедоступная и/или легко восстановимая информация не требует изощренной защиты. Объективный анализ информационных ресурсов показывает, что объем общедоступной информации значительно превышает объем информации конфиденциальной.

Аналогичным образом, информационно-технологические ресурсы (персональные компьютеры, серверы, кабели, концентраторы и т.д.), а также средства обеспечения (программы, дискеты и т.д.) должны подвергаться соответствующей инвентаризации и быть надежно защищены. Довольно часто организации получают большие партии компьютерной техники и программного обеспечения (персональные компьютеры, мониторы, сетевые платы, концентраторы, маршрутизаторы и т.д.), но не вносят их в инвентарные ведомости и не проводит тщательной проверки их соответствия заявке, правильности конфигурации и исправности. Как следствие этого, когда оборудование теряется или дает сбой в работе, нет возможности доказать, что оборудование утеряно или неисправно. Поэтому инвентаризация должна быть первым шагом. Второй шаг – это контроль конфигурации оборудования.

Сразу же после получения оборудования необходимо проверить его конфигурацию и осуществить правильную регистрацию прилагаемого к нему программного обеспечения. В инвентарную ведомость следует включить подробное описание компонентов каждой системы, ее аппаратного и программного обеспечения и указать их местонахождение (вплоть до указания номера комнаты и конкретного рабочего стола). Эта информация необходима для защиты информационных ресурсов, позволяя выявлять хищения или несанкционированной доступ к оборудованию и программному обеспечению, а также проводить эффективные расследования при обнаружении подобных нарушений. Имеются компьютерные программы, которые автоматически проверяют конфигурацию оборудования и сообщают об обнаруженных проблемах руководителям, отвечающим за информационную безопасность. Эти программы также позволяют вести учет всех изменений и ремонтных работ, произведенных в системе. По мере осуществления ремонта или модернизации систем очень важно вести учет такого рода мероприятий. Наконец,

хищения и несанкционированный доступ можно предотвращать с помощью замков и специальных винтов для запирания панелей управления на рабочих местах. Необходимо ввести правило о том, что должны расследоваться все проблемы, вызывающие подозрение.

Категоризация оборудования и ресурсов означает классификацию их в зависимости от стоимости или важности для решения конкретных задач. Этот момент очень часто игнорируется. Так, например, организации держат недорогие комплектующие, такие как дискеты, под замком, а важные информационные ресурсы, такие как серверы, остаются незащищенными и находятся в открытых помещениях, или сетевые кабели и концентраторы располагаются на открытых участках стен, а не в защитных коробах или внутри фальш-потолков.

Пользователей также следует подразделять на разные категории. Необходимо контролировать те приложения и информацию, к которым имеют доступ пользователи, а также пути получения такого доступа. (Так, например, пользователю может быть разрешено работать с файлом с ограниченным доступом только с определенного рабочего места и в определенное время). Необходимо контролировать открытие счетов и получение удостоверений пользователя системы. Сами системы следует регулярно проверять на наличие фальшивых удостоверений пользователя и счетов.

Организация должна располагать хорошими возможности для осуществления ревизий.

Один из часто игнорируемых моментов, связанных с информационной безопасностью, касается системной документации. С различного типа документами довольно часто не обращаются должным образом и оставляют их без присмотра в открытых кабинетах. Необходимо обеспечивать защиту подробной технической документации и информации, предназначенной для пользователей. Иногда кажется, что удобнее и дешевле иметь генерализованную документацию, однако, это таит в себе опасность, с точки зрения уязвимости информационной системы. Широко распространяемые инструкции и руководства для конечных пользователей часто содержат в себе много технической информации, которая не нужна конечному пользователю, но весьма привлекательна для хакера. Вооружившись подробной информацией о системе, хакер может вторгнуться в нее с хирургической точностью, оставляя гораздо меньше следов, вместо того, чтобы использовать грубую силу. Поэтому документация должна выдаваться по мере возникновения потребности в ней.

Необходимо обеспечить защиту документации, контроль доступа к ней и обучение пользователей методам ее защиты. В целях снижения затрат рекомендуется публиковать документацию не на бумаге, а с помощью сетевых средств, что также упрощает внесение в нее изменений и дает дополнительные возможности для ее защиты.

6. НУЖЕН РЕАЛИСТИЧНЫЙ ПОДХОД К УПРАВЛЕНИЮ СИСТЕМОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Маловероятно, что следственно-судебные органы способны создать или наладить программу, обеспечивающую 100-процентную безопасность информационных технологий. Необходимо балансировать реальные потребности в защите со стоимостью обеспечения такой безопасности. Для этого можно пригласить специалистов со стороны. Организация должна использовать своих специалистов для выполнения только тех работ, которые они способны произвести с достаточной эффективностью, а для выполнения остальных работ могут привлекаться другие организации или так называемые «общие ресурсы». Главное состоит в том, чтобы добиться результатов, сформулированных в плане информационной безопасности.

Для достижения целей по информационной безопасности существует множество ресурсов. К этой работе можно привлечь частные компании по конкурентоспособным расценкам. По мере того, как организации все шире применяют информационные технологии и вопросы безопасности вызывают растущую обеспокоенность, частные компании расширяют спектр предлагаемых высококачественных услуг в области информационной безопасности.

Привлечение «общих ресурсов» имеет свои преимущества. Под этим понимается процесс, когда следственно-судебные учреждения и специалисты по безопасности помогают друг другу. Совместное пользование ресурсами, объединение финансовых средств для совместных закупок, бесплатные услуги со стороны университетов или местного насе-

ления – все это может пригодиться для закрытия «белых пятен» в реализации плана информационной безопасности.

7. СЛЕДУЕТ ПРОВОДИТЬ ПРОВЕРКИ, РЕВИЗИИ, ИНСПЕКЦИИ НА МЕСТАХ, А ТАКЖЕ РЕГУЛЯРНЫЕ И ВЫБОРОЧНЫЕ РАССЛЕДОВАНИЯ. Применяйте методологию рассмотрения и проверки программ для блокирования путей проникновения в систему «с черного хода». Используйте программы автоматической ревизии и контроля. Используйте программы, позволяющие выявлять внесенные в файлы изменения. Разрабатывайте и применяйте «наводящие» программы, которые способны выявлять реальных или потенциальных нарушителей целостности системы. Предавайте широкой огласке информацию об угрозах и реагировании на них. Всегда принимайте быстрые и последовательные действия при обнаружении нарушений или получении сообщений о них. Широко информируйте сотрудников о дисциплинарных взысканиях, наложенных в связи с нарушениями в области информационной безопасности.

ПОЯВЛЕНИЕ НОВЫХ ТЕХНОЛОГИЙ

Разработки в области безопасности ИТ осуществляются так же быстро, как и в других областях, связанных с информационными технологиями, однако методы защиты не могут быть эффективными без их надлежащего использования. Сегодня почти все имеющиеся в продаже программы оснащены встроенными средствами защиты. Средства блокировки доступа представляют собой наиболее мощные и адаптируемые средства защиты, и продаются по вполне разумным ценам.
В последнее время получают распространение программы шифрования информации, которые становятся все более эффективными и простыми в применении. Постоянно повышаются возможности для контроля и управления распределенными системами из единого центра компьютерной сети. Быстро совершенствуются программы автоматического мониторинга и проверки, предназначенные для контроля использования систем и уведомления сотрудников безопасности о попытках проникновения в нее.

Одной из самых многообещающих областей технических разработок становится биометрия – возможность идентифицировать человека по его уникальным физическим характеристикам (например, отпечаткам пальцев, тембру голоса, геометрии ладони, сетчатке глаза и так далее). Биометрические устройства предоставляют беспрецедентные возможности для идентификации пользователей и способны помешать несанкционированному доступу к системе даже при наличии у нарушителя пароля.

Корпорация IBM в сотрудничестве с банком «Барклэйз» в Европе проводит испытания экспериментальной партии компьютерных клавиатур, в которых встроено устройство для считывания отпечатков пальцев. Прежде, чем пользователь получит доступ к какой-либо части системы, он должен быть идентифицирован биометрическим способом. Технология мгновенного считывания (по алгоритму поиска образов) обеспечивает большую скорость и точность. Она способна осуществить поиск в базе данных, содержащей миллионы образов (в том числе отпечатков пальцев), и проверить их соответствие. Эта технология в сочетании с высокоскоростными сетями имеет большое будущее для применения в банкоматах и других электронных устройствах, осуществляющих операции с денежными средствами. Технология мгновенного считывания используется для подтверждения личности избирателей в Перу, где для их регистрации используются отпечатки пальцев. Этот проект продемонстрировал отличные результаты, а применение такой технологии поможет избежать подтасовок при подсчете голосов.

По мере дальнейшего развития всех этих технологий будет возрастать эффективность и простота мер по обеспечению безопасности информационных технологий.

СПРАВКА: ЗАЩИТА ЖИЗНЕННО ВАЖНЫХ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ США

(Директива Президента США No. 63)

Нижеследующая справка содержит директиву Президента США No. 63, опубликованную Белым домом 22 мая 1998 г.

Настоящая директива Президента США опирается на рекомендации Президентской комиссии по защите жизненно важных объектов инфраструктуры. В октябре 1997 г. Комиссия опубликовала доклад, призывающий к принятию общегосударственных мер для обеспечения безопасности все более уязвимых и взаимосвязанных объектов инфраструктуры США, к которым относятся телекоммуникации, банковско-финансовая система, энергетика, транспорт и основные государственные службы.

Директива Президента США No. 63 представляет собой кульминацию интенсивных межведомственных усилий по оценке этих рекомендаций и созданию эффективной и новаторской базы для защиты жизненно важных объектов инфраструктуры. Намеченная Президентом политика:

- нацелена на создание надежной, взаимосвязанной и безопасной информационно-системной инфраструктуры к 2003 г. и на значительное укрепление безопасности государственных систем к 2000 г. путем:
    - а) незамедлительного создания национального центра по сигнализации о нападениях и реагированию на них;
    - б) создание к 2003 г. потенциала для защиты жизненно важных объектов инфраструктуры от умышленных враждебных действий;
- направлена на снижение уязвимости электронных и физических объектов инфраструктуры, принадлежащих федеральному правительству, требуя от каждого министерства и ведомства принятия мер для уменьшения своей уязвимости перед новыми угрозами;
- требует от федерального правительства служить примером для всей страны в поиске решений проблемы защиты объектов инфраструктуры;
- направлена на обеспечение добровольного участия частного сектора в достижении общих целей по защите жизненно важных систем посредством партнерских отношений между государством и частным сектором;
- защищает право на конфиденциальность и нацелена на использование рыночных механизмов. Она призвана укреплять и защищать экономическое могущество страны, а не подрывать его;
- стремится к обеспечению всестороннего участия и поддержки со стороны Конгресса.

Директива Президента США No. 63 предусматривает создание новой структуры для решения этой важной задачи:

- Национальный координатор будет заниматься не только вопросами защиты жизненно важных объектов инфраструктуры, но и проблемами, связанными с иностранным терроризмом и угрозами применения оружия массового поражения (включая биологическое оружие) внутри страны, поскольку враждебные действия против США могут принимать самые различные формы, что затрудняет определение их «ведомственной принадлежности»;

– Национальный центр по защите объектов инфраструктуры при Федеральном бюро расследований объединит представителей ФБР, Министерства обороны, Секретной службы США, Министерств энергетики и транспорта, развед служб и частного сектора для реализации беспрецедентной программы межведомственного обмена информацией в сотрудничестве с частным сектором. Центр будет также заниматься содействием и координированием деятельности федеральных властей по реагированию на различные инциденты, ослаблению враждебных действий, исследованию угроз и мониторингу усилий по восстановлению;

– Будет поощряться создание частным сектором Центра по распространению и анализу информации, действующего совместно с федеральным правительством;

– Национальный совет по обеспечению защиты объектов инфраструктуры объединит лидеров частного сектора, а также представителей органов власти штатов и местного уровня для руководства разработкой Национального плана;

– Управление по обеспечению защиты жизненно важных объектов инфраструктуры будет оказывать поддержку Национальному координатору в его работе с государственными ведомствами и частным сектором по разработке общенационального плана. Оно будет также участвовать в координации как общенациональной программы обучения и просвещения, так и законодательной и общественной деятельности.

Более подробная информация о настоящее директиве Президента США содержится в рабочих материалах по защите жизненно важных объектов инфраструктуры, копии которых можно получить, обратившись в Управление по обеспечению защиты жизненно важных объектов инфраструктуры по телефону (703) 696-9395.

СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

Инфокибернетическая угроза и защита информационных сетей США

АННОТАЦИИ СТАТЕЙ

Bennett, Robert, et al. THE Y2K CRISIS: A GLOBAL TICKING TIME BOMB? (The Washington Quarterly, vol. 21, no. 4, Autumn 1998, pp. 147–166)

В пяти очерках консультанты по менеджменту, специалисты в области финансового планирования и эксперты по вопросам решения компьютерной проблемы 2000 года предупреждают, что это серьезная проблема, которая требует решения сейчас, пока не стало слишком поздно. Сенатор Беннетт, который возглавляет специальный сенатский комитет по проблеме 2000 года, считает, что «самая сложная задача – это заставить людей мыслить, выходя за рамки их конкретных организаций, за границы нашей страны». По мнению автора, необходимо признать, что «это не проблема информационной технологии, а проблема организации управления, которую необходимо решать немедленно и на самом высоком уровне».

Bowers, Stephen R. INFORMATION WARFARE: THE COMPUTER REVOLUTION IS ALTERING HOW FUTURE WARS WILL BE CONDUCTED (Armed Forces Journal International, August 1998, pp. 38–39)

Утверждая, что сегодня доступ к информации имеет точно такое же решающее значение для благополучия страны, как наличие нефти и боеприпасов, Бауэрс анализирует угрозу, которую практически не заметные компьютерные атаки создают для национальных энергосистем, транспортных сетей, финансовых систем и линий телефонной связи. Автор отмечает, что в ходе проводимых в последнее время в США военных учений отрабатывались действия, которые поднимают информационную войну с тактического уровня на стратегический. Информационная война предполагает поля боя нового типа, потери на котором могут быть так же высоки, как и на традиционном.

Gompert, David C. NATIONAL SECURITY IN THE INFORMATION AGE (Naval War College Review, vol. 51, no. 4, sequence 364, Autumn 1998, pp. 22–41)

Гомперт, возглавляющий Национальный институт оборонных исследований в системе корпорации «Рэнд», утверждает, что те перемены, сопряженные с информационной революцией, хотя и не лишены недостатков, в целом принесли США много пользы. По оценке Гомперта, информационная революция расширила экономическую и политическую свободу, а также раздвинула границы демократического мира. Она вызвала значительные изменения в способах ведения войны, дав Соединенным Штатам, лидирующим в области информационной технологии, значительное преимущество. «В целом информационная технология может помогать тем, кто ею владеет, выигрывать крупные войны на большом расстоянии малыми силами», – пишет Гомперт. При этом вызывает озабоченность тот факт, что государства-изгои «вероятно, смогут применить достижения электроники совершенно в других направлениях: оружие массового поражения, терроризм и информационная война против Соединенных Штатов и их партнеров».

Henry, Ryan; Peartree, C. Edward. MILITARY THEORY AND INFORMATION WARFARE (Parameters, vol. 28, no. 3, Autumn 1998, pp. 121–135)

Авторы исследуют ограниченное влияние, оказываемое различными технологиями на характер войны, и приводят в качестве примера самолет, который, хотя и расширил боевое пространство в результате беспрецедентного технологического прорыва, неоднократно продемонстрировал, что сам по себе он недостаточен для изменения характера войны. Старое оружие не обязательно выходит из моды, «просто к нему добавляются новые инструменты», указывают авторы. Подчеркивая важность овладения технологическими нововведениями, они утверждают, что «столь же важно, чтобы при оценке политических и военных аспектов этих новшеств на первом плане оставались оценки риска и уязвимости, т.е. вопросы стратегии. Самая надежная военная теория уделяет меньше внимания новейшим технологиям и больше – бесконечной сложности того, кто ее применяет».

Selden, Zachary. MICROCHIPS AND THE MILLENNIUM: THE NATIONAL SECURITY IMPLICATIONS OF THE YEAR 2000 PROBLEM (National Security Studies Quarterly, vol. 4, issue 3, Summer 1998, pp. 71–77)

Селден прогнозирует, что к 1 января 2000 г. большинство компьютерных программ, не подготовленных к проблеме 2000 года, будет исправлено или изъято из употребления, а большинство вызывающих опасения встроенных микросхем будет заменено. По его словам, то, что останется, способно вызвать непредсказуемые сбои или породить смятение. Но его будет достаточно, чтобы позволить тем или иным государствам или террористам осуществить скрытые информационные диверсии. Автор предупреждает, что международные террористы могут попытаться воспользоваться ситуацией, когда внимание США отвлечено. И в некоторых горячих точках конфликты могут стремительно углубляться в результате выхода компьютерных систем из строя. В контексте национальной безопасности США переход к 2000 году создает «период повышенной уязвимости», считает автор.

Приведенные выше аннотации – часть более полного обзора публикаций, который можно найти на домашней странице Информационной службы США:
"http://www.usia.gov/admin/001/wwwhapub.html".

БИБЛИОГРАФИЯ

Adams, James. THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE. New York: Simon & Schuster, 1998. 366p.

Arquilla, John; Ronfeldt, David F. (Editors). IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE. Santa Monica, CA: Rand, 1997. 501p.

Barnett, Roger W. INFORMATION OPERATIONS, DETERRENCE, AND THE USE OF FORCE (Naval War College Review, vol. 51, no. 2, Spring 1998, pp. 7–19)

Browne, J.P.R.; Thurbon, M.T. ELECTRONIC WARFARE, Vol. 4 of Brassey's Air Power: Aircraft Weapons Systems and Technology Series. Washington: Brassey's, 1998. 341p.

Cillufo, Frank J.; Tomarchio, Thomas. RESPONDING TO NEW TERRORIST THREATS (Orbis, vol. 42, no. 3, Summer 1998, pp. 439–452)

Clinton, William J. COMMENCEMENT ADDRESS AT THE UNITED STATES NAVAL ACADEMY IN ANNAPOLIS, MARYLAND (Weekly Compilation of Presidential Documents, vol. 34, no. 21, May 22, 1998, pp. 944–948)

Copley, Gregory R. RE-DEFINING PSYCHOLOGICAL STRATEGY IN THE AGE OF INFORMATION WARFARE (Defense & Foreign Affairs Strategic Policy, vol. 26, no. 6, June 1998, pp. 5–8)

Gunther, Christopher. YOU CALL THIS A REVOLUTION? (Foreign Service Journal, vol. 75, no. 9, September 1998, pp. 18–23)

Henry, Ryan; Peartree, C. Edward (Editors). INFORMATION REVOLUTION AND INTERNATIONAL SECURITY (Significant Issues Series, vol. 20, no. 1). Washington: Center for Strategic & International Studies, 1998. 216p.

Libicki, Martin C. INFORMATION WAR, INFORMATION PEACE (Journal of International Affairs, vol. 51, no. 2, Spring 1998, pp. 411–428)

Molander, Roger C.; Riddile, Andrew S.; Wilson, Peter A. STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR. Santa Monica, CA: Rand, 1996. 90p.

Petersen, John L.; Wheatley, Margaret; Kellner-Rogers, Myron. THE YEAR 2000: SOCIAL CHAOS OR SOCIAL TRANSFORMATION? (The Washington Quarterly, vol. 21, no. 4, Autumn 1998, pp. 129–146)

Pfaltzgraff, Robert L.; Schultz, Richard H. (Editors). WAR IN THE INFORMATION AGE: NEW CHALLENGE FOR U.S. SECURITY POLICY. Washington: Brassey's, 1997. 320p.

Rathmell, Andrew. INFORMATION WARFARE: USA TACKLES CYBERTHREAT (Jane's Intelligence Review Pointer, vol. 5, no. 9, September 1, 1998, p. 14)

Ryan, Stephen M. SHOULD U.S. PLEDGE NOT TO MAKE FIRST CYBERSTRIKE? (Government Computer News, vol. 17, no. 24, August 3, 1998, p. 32)

Sanz, Timothy L. INFORMATION-AGE WARFARE: A WORKING BIBLIOGRAPHY (Military Review, vol. 78, no. 2, March–April 1998, pp. 83–90)

U.S. Senate, Select Committee on Intelligence. CURRENT AND PROJECTED NATIONAL SECURITY THREATS TO THE UNITED STATES. Washington: Government Printing Office, 1998. 177p.

Verton, Daniel. DOD PREPS OFFICE FOR CYBERDEFENSE (Federal Computer Week, vol. 12, no. 23, July 13, 1998, pp. 1–2)

ОСНОВНЫЕ САЙТЫ ИНТЕРНЕТА

Просьба иметь в виду, что ЮСИС не берет на себя ответственности за содержание и доступность перечисленных ниже источников; такого рода ответственность несут исключительно владельцы ресурсов.

Центр ВВС по проблемам информационной войны
http://www.afiwc.aia.af.mil/

Центр компьютерных систем высокой надежности Исследовательской лаборатории ВМС
http://www.itd.nrl.navy.mil/ITD/5540/main.html

Центр технологии компьютерной безопасности Национальной лаборатории Лоренса Ливермора Министерства энергетики США
http://ciac.llnl.gov/cstc/

Бюро по обеспечению безопасности критически важных объектов инфраструктуры
http://www/ciao.gov/

Институт стратегий киберпространства при Университете Джорджа Вашингтона
http://www.seas.gwu.edu/seas/institutes/cpi/

Оборонная информационная инфраструктура
http://spider/osfl/disa/mil/dii/

Оборонная политика в области компьютерной проблемы 2000 года
http://www.defenselink.mil/issues/y2k.html

Глоссарий терминов, относящихся к информационной войне
http://www.psycom.net/iwar.2.html

Корпорация ИИМ: безопасный путь
http://www.ibm.com/Security/

Ассоциация по безопасности информационных систем
http://www.issa-intl.org/

Академическая группа по проблемам информационной войны при Аспирантуре ВМС США
http://web.nps.navy.mil/~iwag/

Информационная война и информационная безопасность в Интернете
http://www.fas.org/irp/wwwinfo.html

Информационная война: глоссарий
http://www.informatik.umu.se/%7Erwhit/IWGlossary.html

Центр изучения проблем информационной войны
http://www.terrorism.com/infowar/documents/html

Проблемы информационной войны
http://www.infowar.com/main.html

«Инфрастракчер дифенс, Инк.»
http://206.132.10/154/idmarketsite/

«Майкрософт Корпорейшн» (ключевые инициативы)
http://www.microsoft.com/

Национальный коллоквиум по безопасности информационных систем
http://www.infosec.jmu.edu/ncisse/

Национальный центр защиты инфраструктуры Федерального бюро расследований
http://www.fbi.gov/nipc/home/htm

Национальный институт стандартов и технологии (НИСТ)
http://csrc.nist.gov/

Агентство национальной безопасности
http://www.nsa.gov:8080/

Президентский совет по компьютерной проблеме 2000 года
http://www.Y2K.gov/java/index.htm

Факультет информационной войны и стратегии Национального университета обороны
http://www.ndu.edu/inss/act/iwsvr.html

Новости технологии: правительства побеждают террористов в области сетевого оружия
http://www.techweb.com:80/wire/story/TWB19980922S0018

Юридический комитет Сената США, подкомитет по вопросам технологии, терроризма и правительственной информации
http://www.senate.gov/~judiciary/terrtest.htm

Компьютерная проблема 2000 года: Информационное агентство США
http://www.usia.gov/topical/global/y2k

ВНЕШНЯЯ ПОЛИТИКА США

ТОМ 3 ЭЛЕКТРОННЫЙ ЖУРНАЛ ИНФОРМАЦИОННОГО АГЕНТСТВА США НОМЕР 4

Кибернетическая угроза и защита информационных сетей США

Ноябрь 1998 г.