ПРЕДИСЛОВИЕ

Сетевые технологии – это сложно и довольно запутанно. Тем не менее без хотя бы поверхностного знакомства с принципами работы компьютерной сети никогда не удастся осмысленно применять приложения, работа которых опирается на сетевые технологии, в том числе средства сетевой защиты.

Основа основ сетевых технологий – это протокол. **Компьютерный протокол – это набор правил обмена информацией, реализованных в программном обеспечении, предназначенном для управления связью и передачей данных между двумя компьютерами.** Поэтому разработчики сетевых технологий создали особую классификацию этих протоколов, разделив их по уровням, каждый из которых отвечает за определенный аспект функционирования сети и опирается на классификацию Международной организации по стандартизации (ISO – International Standardsization Organization), модель OSI (Open System Interconnection – взаимодействие открытых систем).

Даже будучи человеком, никак не предрасположенными к доверчивости, окружив себя всеми средствами антивирусной защиты, ничего не загружая и ничего не инсталлируя из предлагаемых в Интернете ресурсов, мы постоянно подвергаем свои компьютеры самой серьезной опасности – вплоть до потери файлов и полной очистки дисков, не говоря уже о «подвешивании» компьютера. Построив определенным образом код HTML, можно создать страничку Web, которая «подвесит» ваш компьютер, а, составив определенным образом также с помощью HTML электронное письмо, можно загрузить и запустить на клиентском компьютере злонамеренную программу, причем без всякого участия пользователя, – достаточно просто открыть письмо в диалоге почтового клиента.

Изучив материал, изложенный в гл. 1, вы сможете оценить уровень опасности, связанной с простым щелчком на ссылке, переносящей на интересующий вас сервер Интернета.

После того как вы убедитесь, что все это очень серьезно, в гл. 2 показано, как настройками IP-безопасности можно значительно снизить уровень угроз, приходящих из Интернета.

Защититься можно, только полностью осознавая сущность угроз, их техническую подоплеку. Поэтому в гл. 3 пособия приводятся конструкции простеньких страничек Web, позволяющих, несмотря на свою простоту, вытворять очень опасные шуточки с компьютерами посетителей сайта Интернета. В этой главе учебного пособия рассмотрены вопросы

безопасности, связанные со службой Интернета, предоставляющей доступ к гипертекстовой информационной базе данных, размещенной в сети Web. Именно после создания этой службы Интернет превратился в то, что мы наблюдаем в настоящее время, – во всемирное информационное сообщество, с которым связываются многие надежды по развитию мировой цивилизации.

Однако возможности Интернета вовсе не исчерпываются сетью Web. Еще до создания Web существовала общемировая компьютерная сеть, предоставляющая доступ к информационным ресурсам на сетевых серверах, а также реализующая почтовые услуги. В гл. 4 учебного пособия, «Практикум по обеспечению «интернет-безопасности», рассматриваются проблемы безопасности, связанные с этими службами Интернета. В этой главе также рассматривается еще одна реальная угроза – клавиатурные шпионы, специальные программы, фиксирующие все ваши действия на компьютере и передающие информацию своему хозяину. Общее представление о возможностях клавиатурного шпиона, например 007 Stealth Activity Recorder&Reporter (*http://www.iopus.com*), и знание общих методов борьбы с такими средствами поможет сохранить не только информацию, но и деньги. Дело в том, что такие программы не реализуются как вирусы – это вполне легальные средства для скрытого контроля доступа к компьютеру. Такие компьютерные наблюдатели ныне стали популярным средством наблюдения за нерадивыми сотрудниками, использующими рабочие компьютеры в личных целях, а также инструментом технического шпионажа.

Операционные системы Windows 2000/XP снабжены развитыми средствами защиты, позволяющими организовать многопользовательский доступ к компьютеру. Начиная с системы Windows 2000 фирма Microsoft преодолела многие недостатки средств защиты, присущие ее предшественнице – системе Windows NT 4.0. Система защиты Windows 2000 выдержала серьезную проверку. Достаточно сказать, что перед выпуском операционной системы Windows 2000 компания Microsoft создала на основе системы Windows 2000 Server узел Web по адресу *Windows2000test.com* и предложила хакерам всего мира взломать защиту системы [7]. Многочисленные попытки взлома к полному успеху не привели – к средствам уровня операционной системы доступ не смог получить никто. Тем самым была доказана эффективность защиты Windows 2000, если она корректно настроена и введена в действие.

В гл. 5 и 6 учебного пособия рассмотрены основные компоненты, из которых состоит система защиты Windows 2000/XP при многопользовательском режиме работы, и правила настройки этой системы защиты исходя из выбранной политики безопасности. Изучение системы защиты

начинается с описания основополагающих средств администрирования системы – добавления учетных записей, настройки разрешений доступа к ресурсам компьютера и аудита. Далее рассматривается работа встроенных средств анализа и настройки безопасности системы защиты Windows 2000/XP. В завершение приводится описание практических шагов по настройке разрешений доступа к системному реестру Windows 2000/XP, а также способы запуска приложений под другой учетной записью. Последняя процедура очень эффективно защищает ресурсы компьютера при путешествиях по Интернету или при просмотре электронной почты с внедренным активным содержанием. Это особенно важно в нынешнее время, когда подобные вторжения из Web принимают тотальный характер.