ВМЕСТО ПРЕДИСЛОВИЯ

В конце 1980-х гг. произошло знаменательное событие. Стартовал процесс перехода человечества к новой фазе развития, которая получила название «информационное общество».

Сегодня мы можем отметить, что основы этого общества сформированы. В данное время уже сложно представить нашу жизнь без персональных компьютеров, мобильных телефонов и Интернета. А ведь всего 10—15 лет назад все это только начиналось. Отсюда следует, что продолжение процесса развития будет еще более захватывающим. Не за горами то время, когда все мы и шагу ступить не сможем, чтобы не использовать те или иные, как сейчас принято говорить, сервисы, предоставляемые современными информационно-коммуникационными технологиями (ИКТ). И не только в частной жизни. Производство, энергетика, транспорт, связь, финансы — все окажется замкнутым на ИКТ, практически вся жизнь общества станет в сильнейшей степени зависеть от этих технологий.

В таких условиях надежность и безотказность работы ИКТ, качество информации, которой мы пользуемся, сохранение секретов приобретают первостепенное значение. Мы должны доверять всем этим сервисам. Иначе последствия для общества и каждого отдельного человека могут быть просто катастрофическими.

Таким образом, одной из самых главных проблем развития информационного общества становится обеспечение информационной безопасности личности, общества и государства.

Мы являемся свидетелями того, как в последние годы обостряется проблема безопасности компьютеров, являющимися объектами, наиболее часто подвергающимися нападению.

Нарастают симптомы развивающейся информационной войны. И это не случайно. Интенсивное расширение числа абонентов глобальной сети Интернет несет с собой увеличение уязвимости различного рода информационных и управляющих систем, а использование современного персонального компьютера дает в руки злоумышленникам уникальный по своим возможностям инструмент разведки и различного рода деструктивной деятельности, в том числе подготовки и реализации террористических актов. Довольно широко в этих целях используется и распространение в сети программ-вирусов, разрушающих данные, носители информации и даже оборудование. В настоящее время появились новые, связанные с этим термины: «киберпреступность», «кибертерроризм», «кибербезопасность».

Чтобы успешно противостоять всему этому потоку вызовов и угроз, каждому члену информационного общества необходимо обладать определенным минимумом знаний, соответствующей информационной культурой и быть готовым к активной борьбе за чистоту ИКТ от различного рода кибермошенников, киберпреступников, кибертеррористов и просто киберхулиганов.

Данное учебное пособие развивает и в концептуальном, и в содержательном плане материал книги, изданной автором в содружестве с С.В. Пазизиным и Н.С. Погожиным в 2001 г.[1] Ставится цель познакомить читателей с основными проблемами защиты информации в компьютерных сетях, информационно-вычислительных системах и отдельных компьютерах, дать представление о возможных угрозах их безопасности. При этом главное внимание уделяется безопасности критических систем, обеспечивающих национальную безопасность (государственное управление, инфраструктура страны, кредитно-финансовая сфера). Исходя из накопленного на сегодняшний день опыта проектирования и эксплуатации компьютерных сетей, в пособии рассмотрены основные подходы к защите данных и программ, а также выделены апробированные методы и средства ее обеспечения.

[1] *Малюк А.А.*, *Пазизин С.В.*, *Погожин Н.С.* Введение в защиту информации в автоматизированных системах. — М.: Горячая линия — Телеком, 2001.