программа пришла от знакомого, следует это перепроверить. Разумеется, следует опасаться программ, скачанных из ненадежных (непроверенных) источников, например p2p-сетей. Также необходимо использовать шифрование особо важных данных: номеров кредитных карт, паролей и т.д. И наконец, рекомендуется использовать соответствующие антивирусные программы.

Очевидно, что с развитием технологий и программных средств под мобильные устройства вирусы для них станут такими же развитыми, как их PC-варианты. Ожидается появление полиморфных вирусов, новых методов их маскировки и противодействия антивирусам.

Таким образом складывается новое научно-техническое направление – безопасность мобильных устройств, требующее как исследования непосредственно самих вирусов, так и развития аппаратных и программных средств антивирусной защиты.

Литература

1. М.Букин. Секреты сотовых телефонов. М., «Питер», 2005, 206 с.
2. P.Wang, M.González, C.Hidalgo. Understanding the Spreading Patterns of Mobile Phone Viruses. // Science, 2009, Vol. 324 No. 5930 pp. 1071-1076.

МОЛДОВА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

А. К. РУСНАК,
Молдавская Экономическая Академия,
Кишинев, Республика Молдова

Статься рассматривает некоторые проблемы информационной безопасности в Республике и предлагает пути их решения.

Ключевые слова: *информация, информационная безопасность.*

Под информационной безопасностью понимается состояние защищённости информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера.

Цель информационной безопасности – обезопасить главные ценности информационной системы, защитить и гарантировать доступность и целостность информации, не допустить утечку информации, свести к минимуму ущерб от событий несущих угрозу информационной безопасности.

Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм.

Существующая в настоящий момент в мелком, среднем и даже крупном бизнесе и государственном секторе практика обработки важной (в том числе секретной) информации на компьютерах, подключенных к сети Интернет, а так же исполь-

зование для деловой переписки и передачи конфиденциальной информации бесплатных почтовых сервисов представляет реальную угрозу ее утечки или несанкционированного уничтожения.

Также в большинстве случаев предприятия, компании и органы публичной власти при построении собственных информационных систем практически не уделяют внимания вопросам информационной безопасности, не обращают внимания на существующие угрозы информационной безопасности, а также не проводят анализ рисков.

В настоящее время в Республики Молдова существуют следующие проблемы обеспечения информационной безопасности:

1. Несовершенство действующей нормативно-правовой базы в области обеспечения информационной безопасности.
2. Отсутствие во многих средних и крупных компаниях и органах публичного управления единой комплексной системы защиты информации.
3. Нехватка квалифицированного персонала в области информационной безопасности.
4. Недостаточное внимание к проблеме обеспечения безопасности информационных систем, отсутствие таких регламентирующих документов как политика безопасности, инструкции и планы по обеспечению информационной безопасности и бесперебойной работе информационных систем. При этом большинство пользователей информационных систем зачастую не владеют элементарными понятиями и навыками в области информационной безопасности.
5. Недостаточное финансирование сектора информационной безопасности.

Кроме того существуют реальные угрозы информационной безопасности:

- Поражение отдельных компьютеров или всей информационной системы компьютерными вирусами, что может привести как к уничтожению информации, так и к утечке.
- Несанкционированный доступ заинтересованных лиц (в том числе и пользователей информационных систем) к информационным ресурсам, что может привести к незаконной модификации обрабатываемой информации, ее уничтожению или хищению.
- Блокирование работы информационных систем, что может привести к серьезным сбоям в функционировании.
- Передача конфиденциальной информации с помощью электронной почты, что может привести к утечке информации.
- Нецелевое использование компьютерных систем, Интернета, государственных и корпоративных баз данных.

Заключение. Исходя из сложившейся ситуации, можно предложить следующие для обеспечения защиты информационных систем и ресурсов:

1. Дальнейшее совершенствование нормативно-правовой базы в области обеспечения информационной безопасности и специальных телекоммуникационных систем Республики Молдова.

2. Создание и внедрение комплексной системы защиты информации и информационных ресурсов, включающую в себя криптографическую и антивирусную защиту, систему межсетевого экранирования, подсистему аутентификации и идентификации при доступе, подсистему управления, доступом, подсистему защиты информационных систем при их интеграции между собой, а так же при подключении к внешним телекоммуникационным системам.
3. Создание системы аттестации объектов информатизации на предмет соответствия требованиям информационной безопасности.
4. Распределение полномочий между компетентными ведомствами в области организации и обеспечения информационной безопасности и создание реальных механизмов для реализации концепций и политик.

THE LEGAL BASIS OF INFORMATIONAL SECURITY IN FACE OF MODERN WORLD REALITY OR ONLY A MYTH

Michał MAZUR,
Institute of Political Studies and International Relations
(Cracow, Poland)

The article examines contemporary issues combined with the problem of legal basis of informational security. In this brief text author tries to underline some of the most important questions which arise from many attempts to create the sufficient legal model of information protection. The task seems obviously to be very hard but in the end it's not impossible.

1. Introduction

In modern world almost all critical aspects of people activity are supported by legal regulations. This matter has fundamental meaning for their stability and continuity. Generally when something is obvious it is much easier to obey, to comply with regulations.

Informational security, both real and legal, seems to be the first rate factor for the functioning of individuals, institutions and, in the first place, for political organisms which are independent states. For centuries one can point many examples where the effective information handling was essential for the final result of each scuffle.

Real informational security, mentioned above, must have, in every case, foundation. This foundation is legal regulation which is able to sanction effective security of identified data. Symptomatic, in this field, is statement that to keep a secret, silent is not sufficient [1].

2. Contemporary patterns and issues

Most of contemporary states rest their legislation, as regards informational security, on regulations focused around information defined as classified or secret. The other area, which is thought to be crucial, are the issues of state security, fundamental for every political authority. These are usually gathered by legislator in constitution or in the legal acts of the highest rank. Exceptions in certain states are capital planning practices within the government or agency-specific policies [2].