циально незащищенных слоев населения. В данном аспекте на это же должно быть направлено ценовое регулирование экономики, которое является одним из главных видов государственного воздействия на экономику. Цены как основной инструмент уровновешивания спроса и предложения увязывают возможности потребителя с денежным запросом производителя, выполняя в тоже время и очень важную социальную функцию: влияют на структуру и объем потребления благ и услуг, расходы, уровень жизни, прожиточный минимум, потребительский бюджет семьи.

М. Н. Гриневич, И. А. Веремеева

Могилевский машиностроительный институт

Защита экономической информации фирмы в условиях электронной обработки данных

В своей работе предприниматель сталкивается с большими объемами информационных потоков. Информированность для предпринимательской деятельности имеет огромное значение, поскольку превосходство в конкурентной борьбе достигается принятием эффективных и своевременных решений на основе накопленной и обработанной информации, поступающей от различных источников.

Неадекватная защита данных может подвергнуть фирму риску серьезных убытков, вызванных случайным или преднамеренным разрушением, искажением или использованием данных. Поэтому весьма актуальным является вопрос обеспечения надежной защиты компьютерных данных.

В решении вопроса безопасности компьютерных данных в фирме необходим логистический системный подход, который должен состоять из следующих последовательных шагов:

1. Обеспечение приоритетности проблемы защиты информации. Для этого следует разработать стратегию защиты информации, которая включает в себя разделение обязанностей по управлению и контролю за защитой данных; выявление информации, не подлежащей разглашению (например, торговые секреты, производственные планы, списки клиентов и т. п.).

2. Уточнение источников информации, а также степени уязвимости фирмы и размера возможного ущерба в случае несанкционированного доступа пользователей к файлам данных.

3. Выбор и внедрение методов и средств защиты компьютерной системы. Отметим основные пять из них. Во-первых, это организационный контроль. Его цель — точное и эффективное выполнение каждым из сотрудников своих обязанностей. В частности, он призван обеспечить защиту компьютерной системы и содержащуюся в ней информацию от слу-

чайного либо преднамеренного искажения, снизить риск различного рода денежных махинаций. Во-вторых, это технические средства защиты информации в виде устройств и приспособлений, призванные предотвратить возможность утраты важной информации в случае возгорания, перебоев с подачей электроэнергии, перепадов температуры, кражи и т. д. В-третьих, это аппаратные, программные и криптографические методы и средства защиты информации от несанкционированного доступа. Они представляют собой систему мер, позволяющих ограничить доступ и использование вычислительной системы неуполномоченными на то лицами. К таким мерам относятся: аутентификация (опознание) пользователя с помощью специальных предметов (жетонов, карточек и т. д.) и паролей для регистрации пользователя в вычислительной системе, контроль действий пользователей (фиксация всех произведенных ими операций), а также защита данных методами кодирования и шифрования информации. В-четвертых, это контроль за разработкой и качеством приобретаемого программного обеспечения. Разработанное собственными силами программное обеспечение (ПО) должно выполнять функции планирования и организации вычислительного процесса и быть надежно защищено от несанкционированного доступа. Приобретая готовое ПО, необходимо убедиться в том, что оно является лицензионной копией, защищено от копирования, имеет высокую степень надежности в эксплуатации. В-пятых, это контроль за созданием резервных копий. Для этой цели необходимо составление персоналом резервных копий информации и основных компьютерных программ, а также перекрестное обучение сотрудников выполнению наиболее важных операций в условиях обеспечения их взаимозаменяемости.

4. Результаты ревизий и проверок. После выбора и внедрения методов контроля необходимо периодически уточнять и проверять их в действии для оценки эффективности и соответствия изменяющимся условиям деятельности фирмы. Одно из мероприятий по снижению вероятности потерь экономической информации заключается в проведении периодического тестирования сотрудников по вопросам возможности осуществления ими действий, направленных против интересов фирмы.

Таким образом, проблема защиты экономической информации фирмы существует и для ее решения следует применять комплексный подход, включающий ряд мероприятий и учитывающий специфику работы предприятия.

Учет предлагаемых мероприятий по защите экономической информации фирмы позволит предпринимателю значительно снизить риск потери конфиденциальных данных, находящихся на магнитных носителях, и сократить возможные убытки.