ВВЕДЕНИЕ

Государственный стандарт Р 51275–2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» описывает весьма внушительное пространство угроз, которые существуют объективно и, реализовавшись, могут нанести ущерб информации, обрабатываемой в компьютерной системе. Кроме несанкционированного доступа злоумышленников, технических разведок извечных конкурентов, злого умысла обиженных сотрудников, сюда присоединяются и вполне «обыденные» угрозы, связанные с разлитым на системный блок кофе, засыпанием на «back space», чисто человеческим любопытством, граничащим с некомпетентностью.

От большого пространства разнообразных опасностей можно уберечься только соответствующим множеством рубежей защиты, разнообразных по физическому принципу действия, по объекту, субъекту, способу и степени противодействия угрозам. Большинство опытных пользователей ПЭВМ хорошо знакомы с мерами по защите информации. Отдельные мероприятия сами по себе могут быть очень хороши, но особенно они действенны при соблюдении основных принципов защиты информации, среди которых важнейшими являются системность, комплексность, непрерывность в пространстве и во времени. Системному администратору или администратору безопасности организовать одному надежный заслон ущербу компьютерной информации не только очень сложно — практически невозможно, хотя бы потому, что информационная безопасность подразумевает в том числе и целый ряд административно-организационных, технических, кадровых мероприятий. Более того, обилие необходимых и возможных мер защиты компьютерной информации затрудняет их комплексирование, планирование и контроль. В этой ситуации на помощь специалистам по защите автоматизированных информационных систем (АИС) приходят специализированные аппаратно-программные средства защиты информации (СЗИ).

Предлагаемое пособие предназначено для специалистов, отвечающих за безопасность информационных объектов, может быть полезным руководителям предприятий, преподавателям и студентам вузов, изучающим современные информационные технологии.

Цель пособия — предоставить читателям возможность изучить методы и средства защиты информации на примере имеющихся на российском рынке специализированных программно-аппаратных систем. Основной акцент в пособии делается на практическое изучение материала. Известные авторам многочисленные учебные пособия (например, [27, 29]) содержат подробное теоретически обоснованное описание методов защиты информации, однако редко рассматривают конкретные специализированные программно-аппаратные средства. Практическая реализация защитных механизмов в этих книгах рассмотрена на уровне операционных систем. С другой стороны, техническая документация, поставляемая с системами защиты, подробно описывая особенности реализации методов защиты в каждой конкретной системе, не всегда дает методику применения этих средств.

В настоящем пособии сделана попытка сформировать общую методику применения готовых программно-аппаратных СЗИ для решения наиболее важных проблем, неизбежно возникающих в процессе защиты информации на предприятиях и в организациях. Вместе с тем пособие не следует воспринимать как руководящий документ по защите информации, в особенности составляющей государственную тайну.

По мере изложения теоретического материала читателям предлагаются практические задания, обозначенные абзацем «**ВЫПОЛНИТЬ!**». Выполнение заданий, а также ответы на содержащиеся в них вопросы являются необходимым условием освоения учебного материала.

Предполагаем, что, ознакомившись с теоретической частью пособия и выполнив практические задания, читатели смогут, во-первых, обоснованно подойти к выбору того или иного средства защиты и, во-вторых, грамотно использовать выбранное средство в процессе своей творческой деятельности.

Пособие состоит из четырех глав, библиографического списка и приложений.

Глава 1 «Методы и средства криптографической защиты информации». В главе приведено описание основных методов и средств защиты информации, основанных на криптографии, вво-

дятся принципы и этапы проектирования средств защиты информации.

В главе 2 обсуждаются вопросы стандартизации, лицензирования и сертификации в области проектирования средств защиты информации.

Глава 3 «Применение средств криптографической защиты информации (СКЗИ)» содержит основные теоретические сведения и практические задания для изучения СКЗИ StrongDisk, Secret Disk, «Верба», «КриптоПро CSP», StrongNet, «Игла-П» и VipNet.

Глава 4 «Проектирование средств криптографической защиты информации» содержит основные теоретические сведения и практические задания для построения средств криптографической защиты информации на базе библиотек СКЗИ «КриптоПро CSP» и «Верба-OW». По результатам изучения осуществляется разработка четырех программ в средах программирования Borland Delphi, Microsoft Visual Studio и Microsoft .Net Framework. Предполагается возможность интеграции разрабатываемых приложений в крупные программные проекты, разрабатываемые с учетом требований к криптографической защите информации.

Библиографический список содержит 33 наименования нормативных документов, технической документации и учебных пособий, требующихся для углубленного изучения отдельных тем.

В приложениях приводятся рекомендации для преподавателей по проведению практических занятий с использованием технологии виртуальных машин, технические характеристики распространенных электронных идентификаторов, перечень терминов и фонд оценочных средств.

В условиях постоянного совершенствования разработчиками программных средств авторы не стремились включить в пособие самые современные средства защиты информации, предполагая, что главным является изучение методов и технологий криптографической защиты информации, а не интерфейса программных средств.

Практические задания при изучении пособия выполняются на ПЭВМ в системе виртуальных машин VirtualBox или VMware. При выполнении работы слушатели формируют отчет в электронном виде, состоящий из экранных копий. По каждому выполненному заданию с помощью, например, комбинации клавиш Alt+PrtScr выполняется снимок экрана, который помещается в

документ, например, формата Microsoft Word. Файл со снимками экранов является, таким образом, отчетом о выполненной работе. В связи со значительным объемом отчетов преподавателям рекомендуется их прием осуществлять в электронном виде.

Отчет должен включать:

- наименование практического задания;
- фамилию, инициалы слушателя, номер учебной группы;
- описание структуры виртуального стенда, использованного для выполнения практического задания;
- результаты экспериментов, проведенных при выполнении практического задания;
- выводы по результатам выполнения практического задания.

Обратим внимание, что для обеспечения уникальности отчетов и сохранения авторства их составителей (слушателей) обязательным условием приема отчетов является наличие в экранных копиях указания на фамилию слушателя или его порядковый номер в списке группы. Для решения этой задачи предполагается, что при выполнении заданий, связанных, например, с созданием каталогов, файлов, учетных записей и иных объектов, слушатели будут использовать в качестве составной части имени объекта, например, свой номер в списке учебной группы, или свою фамилию, или инициалы по указанию преподавателя.