

## **СЕКЦИЯ 4. ПРОБЛЕМЫ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ КАДРОВ**

### **ЗАЩИТА ИНФОРМАЦИИ В ФАЙЛОВОЙ СИСТЕМЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ**

В.Т. ПЕРШИН

В связи с расширением практики дистанционного обучения возникают проблемы, связанные с организацией защиты от несанкционированного доступа к файлам, содержащим информацию о результатах экспертных оценок успеваемости студентов. Это наиболее уязвимая часть всей системы дистанционного обучения, так как именно она представляет наибольший интерес для опытного программиста, который может сломать защиту и изменить содержащуюся в файле информацию.

На примере создания электронного учебника по курсу "*Основы радиоэлектроники*" рассмотрены возможности надежного перекрытия доступа к файлам о результатах тестирования. Осуществлена защита памяти с помощью кода, находящегося внутри программы. Этот код ограничивает доступ к областям памяти, выделенным управляющей программой для хранения информации об успеваемости студентов.

Рассмотрен также способ размещения информации о результатах тестирования на сервере с защитой его от несанкционированного доступа системными средствами сервера.

Отмечаются преимущества предложенного способа защиты информации, заключающиеся в простоте используемых средств для его реализации, упрощении протокола взаимодействия программ, обеспечивающих размещение защищаемой информации и организацию доступа к ней нескольких пользователей разного уровня.

### **ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ДИСТАНЦИОННОМ ОБУЧЕНИИ**

Д.А. МЕЛЬНИЧЕНКО, А.П. МОРОЗОВ

В настоящий момент все большее распространение получает дистанционное обучение — новая форма образования, которая сочетает в себе открытость с его интенсификацией за счет применения электронных учебников, компьютерных обучающих программ, информационных баз знаний и данных. Такой вид обучения не представляется возможным без активного использования WEB-технологий. Системы, в которых информация передается по глобальной сети особенно уязвимы: компьютерные вирусы могут распространяться моментально от системы к системе, засоряя память или разрушая программы и данные. Для систем дистанционного образования очень важно, что часть данных (личные сведения о студентах, результаты контроля знаний и т.д.) являются конфиденциальными и подлежат защите. Поэтому, создание системы информационной безопасности — необходимое условие надежного и эффективного функционирования технологии дистанционного обучения.

Обеспечение безопасности системы в целом достигается за счет обеспечения безопасности на каждом ее уровне: внешнем, сетевом, системном и на уровне приложений.

Для обеспечения надежной работы системы на каждом уровне должен быть разработан комплекс организационно-административных, технических и технологических мер по предотвращению угроз разрушения и уничтожения информации, а также устранению их последствий.

Соблюдение всех этих принципов позволит обеспечить безопасную среду для бесперебойной работы всей системы дистанционного обучения.

### **ОСОБЕННОСТИ ПОДГОТОВКИ ИНЖЕНЕРОВ СВЯЗИ ПО ВОПРОСАМ ПОЧТОВОЙ БЕЗОПАСНОСТИ**

В.М. БУРАЧЕНКО, Л.М. ЛЫНЬКОВ, В.В. СОЛОВЬЕВ, Н.Д. ЮШКЕВИЧ

В последнее время отрасль почтовой связи осваивает большое количество новых нетрадиционных услуг, современные технологии, в том числе и в финансово-кредитной сфере. Поэтому наряду с проблемами физической безопасности персонала и объектов почтовых учреждений появляется необходимость дальнейшего совершенствования и расширения преподавания дисциплины "Почтовая безопасность" учащимся и студентам Высшего государственного колледжа связи и системы переподготовки почтовых служащих.

Для этого в рабочую программу по данной дисциплине включены новые направления, такие как, элементы банковских услуг (правоотношения, операции, инкассация, кризисные ситуации), обеспечение финансовой безопасности, включая систему международных финансовых телекоммуникаций SWIFT и электронную пересылку посредством POST \* Net, новые аспекты информационной безопасности, обеспечение коммерческой тайны и некоторые другие.