

МОДЕРНИЗАЦИЯ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА КЛАДОВЩИКА НА РУПП «БРЕСТХЛЕБПРОМ» ФИЛИАЛА БАРАНОВИЧСКОГО ХЛЕБОЗАВОДА

Введение. Хранение информации в памяти ЭВМ придает этой информации принципиально новое качество динамичности, т.е. способности к быстрой перестройке и непосредственному ее использованию в решаемых на ЭВМ задачах. По мере своего дальнейшего развития административные системы обработки данных переросли в автоматизированные системы управления (АСУ) соответствующими объектами, в которых, как правило, не ограничиваются одной ЭВМ, а в составе двух и более ЭВМ объединяют в вычислительный комплекс (ВК) [1].

Автоматизированная система управления (АСУ) — это человек-машинная система, в которой с помощью технических средств обеспечивается сбор, накопление, обработка информации, формулирование оптимальной стратегии управления определенными компонентами и выдача результатов [2].

С целью обеспечения возможности взаимодействия человека с ЭВМ в интерактивном режиме появляется необходимость реализовать в рамках АСУ так называемое АРМ — автоматизированное рабочее место. АРМ представляет собой совокупность программно-аппаратных средств, обеспечивающих взаимодействие человека с ЭВМ, т.е. такие функции как: возможность ввода информации в ЭВМ; возможность вывода информации из ЭВМ на экран монитора, принтер или другие устройства вывода (в настоящее время этот перечень достаточно широк).

АРМ должно отвечать следующим требованиям: минимальное время ответа на запросы пользователя; адаптация к уровню подготовки пользователя и его профессиональным запросам; простота освоения приемов работы на АРМ и легкость общения, надежность и простота обслуживания; терпимость по отношению к пользователю; возможность быстрого обучения пользователя; возможность работы в составе вычислительной сети [1].

Объектом научной работы является материальный склад РУПП «Брестхлебпром» Филиала Барановичского хлебозавода.

Предмет проектирования: автоматизация рабочего места кладовщика.

Целью данной исследовательской работы является разработка системы модернизации автоматизированного рабочего места кладовщика. В рамках выполнения научной работы необходимо разработать программу, которая должна отвечать следующим требованиям: организация удобного диалога ЭВМ и пользователя, открытость для модификаций и дополнений последующими версиями и разработками, работа в ОС MS Windows, возможность перенесения данных из предыдущей версии программы, организовать защиту системы введением пароля, простота освоения программы и простота работы с ней.

Актуальность проекта заключалась в том, что на предприятии имеется устаревшая программа учета с минимальным набором функций, работающая под ОС MS DOS. Новое программное обеспечение, разработано под ОС Windows.

Результаты исследования. В процессе работы проведены следующие исследования и разработки: разработали предметную область, выделили сущности и атрибуты в ней. На основе предметной области построили логическую и физическую модели данных в ERWin. Сгенерировали область из среды ERWin в среду MS Access и заполнили полученные таблицы в MS Access. Далее создали программный интерфейс в среде программирования Delphi, с помощью компонента ADOConnection подключились к БД. Заключительным этапом провели тестирование данного проекта.

В ходе выполнения научной работы была разработана программа, предназначенная для модернизации автоматизированного рабочего места кладовщика на РУПП «Брестхлебпром» Филиале Барановичском хлебозаводе.

Новая программа использует один файл (.mdb), в котором хранится вся информация. Этот файл можно хранить не только на сервере, но и на компьютере кладовщика, что позволит уменьшить нагрузку на локальную сеть.

Данный проект работает в ОС Windows. Он позволяет выполнять следующие операции: сортировать данные по возрастанию или убыванию, производить поиск необходимой информации, фильтровать данные.

Кроме этого можно просмотреть информацию о поступивших на склад ТМЦ, сведения о работниках, приход для бухгалтерии, акт списания или акт переоценки ТМЦ и другие. Всю эту информацию можно вывести на печать с помощью созданного отчета в проекте.

Выводы. Созданный проект для модернизации автоматизированного рабочего места кладовщика требует минимальное время ответа на запросы пользователя, прост в освоении и «общении» с пользователем, что отвечает требованиям для созданных АРМ специалистов. Годовые текущие затраты, связанные с решением задачи в проектном варианте в 2,4 раза меньше чем в базовом варианте. Это свидетельствует о том, что данный проект можно реализовывать на предприятии. Проект экономически эффективен, срок окупаемости проекта составит 1 год и 6 месяцев.

Программное приложение «Модернизация автоматизированного рабочего места кладовщика» используется на РУПП «Брестхлебпром» филиале Барановичского хлебозавода.

Список источников

1. Автоматизированные рабочие места и их оснащение информационными средствами [Электронный ресурс]. — Режим доступа : <http://www.foragoza.ru>
2. Белогорцев, Е. В. Автоматизированные системы управления (Сложные системы) [Электронный ресурс] : учеб. пособие. — Электрон. текст. дан. (715 кб). — Минск : Электронная книга БГУ, 2004.
3. Кандзюба, С. П. Delphi. Базы данных и приложения. Лекции и упражнения / С. П. Кандзюба, В. Н. Громов. — СПб. : ДиаСофтЮП, 2005. — 576 с.
4. Фараонов, В. В. Программирование Баз данных в Delphi 7 : учеб. курс / В. В. Фараонов. — СПб. : Питер, 2006. — 459 с.

Е. В. Климко

Научный руководитель — В. Н. Ярмолик

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь.

ПРОБЛЕМА ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. АНАЛИЗ. ПУТИ РЕШЕНИЯ

В области разработки программного обеспечения (ПО) существуют достаточно серьёзные проблемы, связанные с нарушением прав интеллектуальной собственности разработчиков. Это связано с наличием таких угроз для программных продуктов как: несанкционированное использование и несанкционированная модификация, а также обратное проектирование. Как показывает мировая практика, уязвимость ПО к перечисленным угрозам является причиной существенных экономических потерь для компаний-производителей. Так, по данным Business Software Alliance количество нелегальных копий программных продуктов ведущих фирм достигает от 20% (США) до 95% (Грузия) в зависимости от региона и страны. В среднем в мире более чем одна из трех установленных копий программного обеспечения является нелегальной [1].

В связи с этим разработка новых подходов, методов, алгоритмов защиты программного обеспечения и реализация на их основе эффективных технических средств защиты является весьма актуальной.

Достаточно существенным представляется вопрос о том, защитой какого именно программного обеспечения следует заниматься в первую очередь, так как атакам подвергается разнообразное ПО, от распространяемого свободно до коммерческого, более того, несущего в себе информацию о личных данных пользователей. Целесообразно осуществлять меры по защите от несанкционированного использования, обратного проектирования и несанкционированной модификации коммерческих программных продуктов следующих типов:

- ПО, легко подвергаемое декомпиляции (получению исходного кода из исполняемого);
- ПО, поставляемое пользователю в виде исходных кодов на языке высокого уровня;
- ПО, из которого легко извлекаются интересующие атакующего функционально законченные модули (компоненты).

Данные проблемы частично решаются за счёт применения ряда традиционных юридических и технических мер по предотвращению нарушений прав интеллектуальной собственности разработчиков ПО. К ним относятся: патентование и заключение лицензионных соглашений; программно-аппаратные методы защиты; методы, основанные на криптографическом преобразовании кода программного обеспечения; методы, основанные на привязке программного обеспечения к носителю; организация выполнения ПО на удалённом сервере (“server-side execution”). Однако, перечисленные подходы не являются достаточно эффективными. Перечислим наиболее очевидные трудности, с которыми могут столкнуться производители при попытке использовать данные методы защиты:

- использование юридических мер затруднено несоответствием законодательства в различных государствах и ограниченной территорией действия патентов;
- программно-аппаратная защита, основанная на использовании аппаратных ключей, уязвима к эмуляции работы ключа либо модификации защищаемой программы с целью полного отключения защиты;
- методы, основанные на дешифровании кода программы «на лету» (“on-the-fly”), не являются защищенными от возможности считывания из оперативного запоминающего устройства вычислительной машины значений ключей дешифрования либо кода программы в открытом виде;
- привязка ПО к носителю создаёт неудобства его использования и неприменима при доставке программного продукта конечному пользователю путём загрузки с web-сайта разработчика;
- выполнение ПО на удалённом сервере связано с существенной потерей производительности приложений.

Недостаточная эффективность традиционных методов защиты ПО послужила причиной происходящего в последние годы интенсивного развития принципиально новых подходов к защите ПО, основанных на использовании цифровых водяных знаков (ВЗ) и, как их модификации, цифровых отпечатков пальцев. На сегодняшний день предложено множество алгоритмов внедрения водяных знаков в ПО. Однако, такие вопросы как обеспечение защиты, минимально влияющей на качество ПО и удобство его использования, а также создание