Заключение. Использование информационных технологий даёт толчок развитию новых форм и содержания традиционных видов деятельности учащихся, что ведёт к их осуществлению на более высоком уровне. Работа с компьютером должна быть организована так, чтобы с первых же уроков начальной ступени обучения она стала мощным психолого-педагогическим средством формирования потребностно-мотивационного плана деятельности школьников, средством поддержания и дальнейшего развития их интереса к изучаемому предмету. Правильно организованная работа учащихся с компьютером может способствовать, в частности, росту их познавательного и коммуникативного интереса, что, в свою очередь, будет содействовать активизации и расширению возможностей самостоятельной работы обучаемых по овладению английским языком как на уроке, так и во внеурочное время.

Список цитируемых источников

1. *Биболетова, М. З.* Мультимедийные средства как помощник УМК “Enjoy English” для средней школы / М. З. Биболетова. — ИЯШ. — 1999. — № 3.

2. *Владимирова, Л. П.* Интернет на уроках иностранного языка / Л. П. Владимирова. — ИЯШ. — 2011. — № 3. — С. 33—41.

3. *Донцов, Д.* Английский на компьютере. Изучаем, переводим, говорим / Д. Донцов. — М. : [б. и.], 2007.

Материал поступил в редакцию 08.09.2014 г.

УДК 004.65(476)

А. А. Бердникова, А. Ю. Бузук
Учреждение образования «Барановичский государственный университет», Барановичи

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ НА ТЕРРИТОРИИ РЕСПУБЛИКИ БЕЛАРУСЬ

Рассматриваются некоторые вопросы информационной безопасности, целостности и конфиденциальности информации, и в первую очередь безопасности систем управления базами данных (далее — СУБД). Даётся определение информационной безопасности и основные цели её защиты, рассмотрены аспекты понятия надёжности информационных систем. Определены основные направления борьбы с потенциальными угрозами безопасности информации, и, в частности, СУБД, с учётом их специфики и в соответствии с законодательством Республики Беларусь. Опираясь на статистические данные, авторы приходят к выводам о необходимости разработки новых алгоритмов и поиска способов решения этих задач.

Ключевые слова: информация, информационная безопасность, криптология, СУБД, средства защиты СУБД.

This article discusses some of the issues of information security, integrity and privacy of information and especially the security of the database management system. There are definition of the information security, the main aims of its security, examined aspects of the concept of the reliability of information systems. The main areas for intervention with potential threats of the information security and especially of the database management system, taking into account their specificities and in accordance with the laws of the Republic of Belarus are determined there. Based on the statistical data, the findings are necessary to develop new algorithms and search methods of solving these problems.

Key words: information, information security, cryptology, database management system, protection means of database management system.

Введение. Развитие вычислительных систем обусловило необходимость организации обработки, хранения и предоставления доступа к данным больших объёмов в электронном виде, которые имеют тенденцию увеличивать свои объёмы достаточно регулярно. Актуальность вопросов целостности и конфиденциальности информации, содержащейся в системах баз данных, поднимают вопросы проблемы информационной безопасности.

Основная часть. В современном обществе под термином «информационная безопасность» принято понимать защищённость информации и её структурных компонентов от случайных или преднамеренных воздействий естественного либо искусственного характера, которые могут нанести какой-либо ущерб субъектам информационных отношений. В понятие «защита данных» включаются вопросы сохранения их целостности и санкционированной доступности в результате деятельности как посторонних лиц, так и специальных программ-вирусов. Абсолютно безопасных систем нет, и это очевидно. Система будет считаться надёжной, если с помощью определённых аппаратных и программных средств будет обеспечиваться одновременная обработка информации различной степени секретности группой пользователей без нарушения каких-либо прав доступа.

Защита информации — это комплекс мероприятий, направленных на обеспечение целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных, т. е. важнейших аспектов информационной безопасности.

Репозиторий БарГУ

Основные цели защиты информации: обеспечение физической и логической целостности, предупреждение несанкционированных получения, модификации и копирования.

Одной из наук, занимающейся методами шифрования и дешифрования, является криптология — самостоятельное научное направление, изучающее и разрабатывающее научно-методологические основы, способы, методы и средства криптографического преобразования информации.

Главные направления использования криптографических методов — передача конфиденциальной информации по каналам связи, установление подлинности передаваемых сообщений, хранение информации на носителях в зашифрованном виде. Криптографические методы защиты информации в автоматизированных системах могут применяться как для защиты информации, обрабатываемой в ЭВМ или хранящейся в различного типа запоминающих устройствах, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи.

В Республике Беларусь существует закон об информации, информатизации и защите информации, в главе 7 которого рассмотрены основные вопросы защиты информации. В ней выделены основные цели, требования, методы организации мер по защите информации: 1) правовые меры защиты информации — заключаемые между обладателем информации и пользователем информации договоры, в которых установлены условия использования информации, а также законодательная ответственность сторон по договору за нарушение, прописанных в договоре условий; 2) организационные — обеспечение режима особого допуска на территорию предприятия или организации, где осуществляется доступ к информации, хранящейся на различного вида носителях, а также приоритетность доступа к информации круга лиц и характера информации; 3) программно-технические — различные меры использования средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации.

На государственные органы и юридические лица, осуществляющие обработку и распространение информации, предоставление которой ограничено, возлагается ответственность за обеспечение защиты информации путём назначения соответствующих подразделений или должностных лиц.

Выделим основные направления борьбы с потенциальными угрозами конфиденциальности и целостности информации: идентификация и подлинность пользователей; разграничение приоритета доступа к данным; учёт и анализ всех действий, влияющих на безопасность данных; защита зарегистрированной информации от преобразований и её анализ; защита информации, передаваемой по каналам связи.

Обозначенные направления применимы как к информации в целом, так и к СУБД в частности. Следует отметить, что специфика СУБД делает потенциально возможными новые угрозы и, соответственно, требует особых мер защиты. Так как СУБД имеют особую внутреннюю структуру, которую даже можно назвать строгой и капризной, значит, и операции над их элементами определены чётко и конкретно. Как правило, на производстве эти операции включают в себя четыре основных действия: поиск, вставка, удаление, замена элемента. Остальные являются вспомогательными и применяются достаточно редко.

Как показывает статистика, злоумышленники не уделяют особого внимания СУБД, и предпочитают взламывать защиту сети на уровне операционной системы и получают доступ к файлам СУБД средствами операционной системы. Иногда злоумышленники без труда преодолевают защиту, установленную непосредственно в самой СУБД, но лишь тогда, когда используется СУБД с низким уровнем защитных механизмов, плохо протестированная версия СУБД, или администратор-программист СУБД при определении политики безопасности допустил ошибки.

Существуют два наиболее распространённых сценария попыток взлома СУБД: в первом случае округляются в меньшую сторону результаты арифметических операций над числовыми полями СУБД, а в некоторой другой записи СУБД суммируется разница; во втором — злоумышленники получают доступ к полям записей СУБД, содержащим только накапливаемую статистическую информацию.

Главный источник угроз для СУБД, лежит в самой природе баз данных, хранящей информацию. Задача взломщика — сформулировать запрос таким образом, чтобы множество записей, для которого собирается статистика, состояло только из одной записи.

Основным средством взаимодействия с СУБД является язык SQL — формальный непроцедурный язык программирования, применяемый для создания, модификации и управления данными в произвольной реляционной базе данных, управляемой соответствующей СУБД. SQL основывается на исчислении кортежей. Механизм правил даёт возможность выстраивать сложные, трудные для анализа цепочки действий, позволяя попутно неявным образом передавать право на выполнение процедур, даже не имея, строго говоря, полномочий на это. В результате потенциальный злоумышленник получает под свой контроль мощный и удобный инструментарий, а, как известно, развитие СУБД направлено на то, чтобы сделать этот инструментарий еще более мощным и удобным[1].

Заключение. Вопросы, связанные с решением проблем по защите информации в целом, и СУБД в частности, остаются довольно актуальными. На текущий момент эффективны следующие средства защиты данных в СУБД: разграничение прав доступа к объектам базы данных, защита паролем, шифрование данных и программ. В результате исследования проблем информационной безопасности можно отметить, что существуют такие виды атак, которые преодолевают данные средства защиты, и в связи с этим необходимы разработка новых алгоритмов и поиск способов решений задач информационной безопасности.

Репозиторий БарГУ

Список цитируемых источников

1. *Вьюкова, Н.* Информационная безопасность систем управления базами данных [Электронный ресурс] / Н. Вьюкова, В. Галатенко // Citforum. — Mode of access: http//www.citforum.ru/database/kbd96/49.shtml. — Date of access: 25.08.2014. — Screen heading.

Материал поступил в редакцию 08.09.2014 г.

УДК 004.652.5

М. А. Вареник
Учреждение образования «Барановичский государственный университет», Барановичи

ОСНОВНЫЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫХ МОДЕЛЕЙ ДАННЫХ

Объектные базы данных появились на свет, поскольку появилась насущная необходимость решать задачи, связанные с обработкой и хранением сложных многосвязных данных, а также слабоструктурированной и неструктурированной информации: текст, изображение, музыка и любые другие данные, требующие специфической обработки. Объектная система управления базами данных (далее — СУБД) идеально подходит для интерпретации такого рода данных. Этим она отличается от реляционных СУБД, где добавление нового типа данных достигается или ценой потери производительности, или за счёт резкого увеличения сроков и стоимости разработки приложений.

Ключевые слова: модель данных, объектно-ориентированное программирование, объект, класс, наследование, полиморфизм.

Object databases were born because there was an urgent need to solve the problems connected with processing and storage of difficult multicoherent data, and also semistructured and unstructured information: the text, the image, music and any data demanding specific processing. Object DBMS is ideally suited for interpretation of such data. Unlike relational DBMS where addition of new type of data is reached at the price of loss of productivity or at the expense of sharp increase in terms and the cost of applications programming.

Key words: model of data, object-oriented programming, object, class, inheritance, polymorphism.

Репозиторий БарГУ

Введение. Появление объектно-ориентированного подхода в программировании внесло фундаментальные изменения во взгляды на данные и процедуры их обработки. Данные и процедуры традиционно хранились отдельно: данные и связи между ними — в базах данных, процедуры обработки — в прикладной программе. Объектно-ориентированный подход позволяет хранить процедуры обработки вместе с данными, т. е. понятие сущности может быть расширено процедурами её поведения в рамках предметной области [1].

Целью данного исследования является рассмотрение основных принципов организации объектно-ориентированных моделей данных и использование данных моделей в современных СУБД.

Основная часть. Первой формализованной и общепризнанной моделью данных была реляционная модель Кодда. В этой модели, как и во всех следующих, выделялись три аспекта — структурный, целостный и манипуляционный. Структуры данных в реляционной модели основываются на плоских нормализованных отношениях, ограничения целостности выражаются с помощью средств логики первого порядка и, наконец, манипулирование данными осуществляется на основе реляционной алгебры или равносильного ей реляционного исчисления. Своим успехом реляционная модель данных во многом обязана тому, что опиралась на строгий математический аппарат теории множеств, отношений и логики первого порядка. Разработчики любой конкретной реляционной системы считали своим долгом показать соответствие своей конкретной модели данных общей реляционной модели, которая выступала в качестве меры «реляционности» системы [2].

Разработка систем объектно-ориентированных баз данных началась в середине 80-х годов XX века в связи с необходимостью удовлетворения требований приложений, отличных от характерных для систем реляционных баз данных. Попытки использования технологий реляционных баз данных в таких сложных приложениях, как автоматизированное проектирование (CAD); автоматизированное производство (CAM); технология программирования; системы, основанные на знаниях, и мультимедийные системы, проявили ограничение систем реляционных баз данных. В условиях, когда появилось новое поколение приложений баз данных, возникли потребности, которые лучшим образом удовлетворялись при применении объектно-ориентированных баз данных.

Объектно-ориентированные базы данных — базы данных, в которых информация представлена в виде объектов, как в объектно-ориентированных языках программирования. Между записями базы данных и функциями их обработки устанавливаются связи с помощью механизмов, подобных тем, которые имеются в объектно-ориентированных языках программирования. Такая модель позволяет идентифицировать