Защита экономических баз данных

Вишневская Д. Д., Шкопец Т. Ю., студ. I к. БГЭУ,
науч. рук. Акинфина М. А., канд. физ.-мат. наук, доц.

Ни для кого не секрет, что в эпоху массовой компьютеризации, в которой пребывает современное общество, IT-технологии все больше вытесняют человека, выполняя за него все больше задач, на которые еще в недавнем прошлом они способны не были. Основным предметом труда стала информация, а компьютеры — новым орудием.

Информационные системы проникают во все новые сферы жизни общества. В таких, как финансы и банковское дело, работа с обращениями граждан сохранность информации — важнейшее условие. В настоящее время, вследствие интенсивности использования электронных баз данных в экономической сфере, возникает проблема эффективной защиты хранимой информации. Хакеры зачастую используют такие методы взлома, как несанкционированный доступ, подбор пароля, вирусы, трояны и так называемые SQL-инъекции. Хищение и нарушение информации наносит существенный вред экономике в целом и физическим лицам в частности. Каждый сбой работы базы данных может парализовать работу целых корпораций, банков, что приведет к ощутимым материальным потерям [1]. Защита паролем, шифрование данных и проблем, разграничение прав доступа к объектам базы данных, защита полей и записей таблиц баз данных используются для усиления безопасности баз данных, т. е. для предотвращения экономических потерь.

Один из простейших и привычных способов защиты баз данных от несанкционированного доступа — защита паролем. В зашифрованном виде пароли хранятся в определенных системных файлах СУБД. Такая защита не является самым сильным и эффективным средством, особенно если пароли не шифруются. Вычислительная система не может различать пользователей, использующих одинаковые пароли, — вот основной недостаток парольной защиты.

Более мощным и надежным средством является шифрование данных, т. е. их преобразование из читаемого текста в нечитаемый, при помощи определенного алгоритма.

В целях контроля использования основных ресурсов СУБД во многих системах имеются средства установления прав доступа к объектам баз данных. Они определяют возможные действия над объектами. Владелец объекта (пользователь, создававший объект), а также администратор БД, имеют все права. Остальные пользователи к разным объектам могут иметь различные уровни доступа. Разрешение на доступ к конкретным объектам базы данных сохраняется в файле рабочей группы. Например, в БД Oracle защита

информации реализуется следующим образом. Стандартный пакет СУБД компании включает функцию виртуального надзора за приложением (Virtual Private Database); с помощью этой функции можно установить контроль доступа для каждого отдельного поля БД, что позволяет обеспечить одновременную работу различных пользователей, причем каждый из них не будет иметь доступ к информации других. Для дополнительной защиты БД Oracle предлагает опцию Oracle Label Security, благодаря которой можно произвести более четкое разграничение доступа, например, определив временной интервал, в течение которого может быть открыт доступ к той или иной информации [2]. Основными характеристиками продуктов Oracle является надежность, безопасность, высокая производительность и удобство в работе. Данные характеристики безусловно важны для СУБД, ставшей на сегодняшний день практически обязательной частью любой серьезной информационной системы. Но не только эти характеристики позволяют продуктам Oracle удерживать лидерство на рынке СУБД. Стремительно развивающиеся информационные технологии требуют от современных СУБД расширения классической функциональности по хранению и обработке данных.

Следует отметить, что средства защиты, предоставляемые базой данных — это только один уровень, защита должна быть многоуровневой. Для того, чтобы предоставить полную защиту информации, необходимо реализовать в сети, серверах и на всех компьютерах весь комплекс безопасности, а именно — антивирусы, антишпионы, сетевые экраны VPN, IDS и т. д. Чем больше уровней защиты, тем сложнее будет их преодолеть. Должна быть четкая политика безопасности и контроль. Хорошая политика безопасности позволяет предотвратить случаи несанкционированного взлома и утечки информации.

Литература

1. Корнеев, В. В., Гареев А. Ф., Васютин С. В., Райх В. В. Базы данных. Интеллектуальная обработка информации. — М.: Нолидж, 2000. — 352 с.

2. Защита баз данных [Электронный ресурс]. — Режим доступа: http://www.studfiles.ru. — Дата доступа: 19.02.2013.

Внешний долг Республики Беларусь: динамика и современное состояние

Гатилло А. С., студ. II к. БГУ,
науч. рук. Гаврилко Г. Н., канд. эк. наук, доц.

В настоящее время проблема внешнего долга является одной из наиболее острых проблем для белорусской экономики: пик платежей по внешнему долгу приходится на 2013–2014 годы. Объем ресурсов, необходимых для