2. Официальная статистика. Оперативные данные // Национальный статистический комитет Республики Беларусь [Электронный ресурс]. – 2013. – Режим доступа: http://belstat.gov.by/ homep/ru/indicators/main1.php. – Дата доступа: 16.09.2013.

3. Платежный баланс Республики Беларусь // Национальный банк Республики Беларусь [Электронный ресурс]. – 2013. – Режим доступа: http://www.nbrb.by/statistics/BalPay/. – Дата доступа: 18.09.2013.

А. В. Войтова, О. В. Лапицкая

Научный руководитель – кандидат технических наук Ю. В. Климов

ЗАЩИТА БАЗЫ ДАННЫХ

В самом общем смысле база данных – это набор записей и файлов, организованных особым образом. В широком смысле, один из типов баз данных – это документы, набранные с помощью текстовых редакторов и сгруппированные по темам. Другой тип – файлы электронных таблиц, объединяемые в группы по характеру использования. Вряд ли существует абсолютно надежная компьютерная система защиты. Хотя средства защиты Microsoft Access считаются одними из лучших для персональных компьютеров.

Проблема обеспечения защиты информации является одной из важнейших при построении надежной информационной структуры учреждения на базе ЭВМ. Эта проблема охватывает как физическую защиту данных и системных программ, так и защиту от несанкционированного доступа к данным. Таким образом, в понятие защиты данных включаются вопросы сохранения целостности данных и управления доступа к данным (санкционированность). Растущие масштабы краж критически важных данных делают все более актуальной необходимость в непосредственной защите баз данных и приложений.

Защита баз данных является одной из самых сложных задач, стоящих перед подразделениями, отвечающими за обеспечение информационной безопасности. При этом четкой и ясной методики комплексного решения задачи защиты баз данных, которую можно было бы применять во всех случаях, не существует, в каждой конкретной ситуации приходится находить индивидуальный подход.

Долгое время защита баз данных ассоциировалась с защитой локальной сети предприятия от внешних атак хакеров, борьбой с вирусами и т. п. Последние аналитические отчеты консалтинговых компаний выявили другие, более важные направления защиты информационных ресурсов компаний. Исследования убедительно показали, что от утечки информации со стороны персонала и злонамеренных действий «всесильных» администраторов баз данных не спасают ни межсетевые экраны, ни VPN, ни даже проверенные системы обнаружения атак и анализа защищенности.

Неавторизованный доступ к данным и кража конфиденциальной информации являются главными составляющими потерь предприятий после ущерба, наносимого вирусами [1].

Защита базы данных включает в себя стандартные и нестандартные способы защиты СУБД.

Стандартными способами являются:

- защита от несанкционированного доступа;
- защита с использованием пароля БД;
- шифрование/Дешифрование базы средствами Access. Кодирование/раскодирование баз данных Access в книге Access 2002;
- защита от Shift;
- запуск приложения через форму авторизации;
- использование защиты на уровне пользователя;
- использование параметров запуска;
- защита страниц доступа к данным.

Нестандартными способами являются:

- изменение расширения файла;
- защита с использованием пароля БД, содержащего непечатные символы;
- защита с модификацией файла;
- защита изменением версии БД;
- защита с использованием электронного ключа.

Защита с использованием пароля БД – данный способ защиты позволяет установить пароль на открытие БД для всех пользователей. Многие разработчики пользуются исключительно английским языком. Узнать или изменить пароль БД можно не прибегая к помощи специальных программ [2].

Шифрование/дешифрование базы средствами Access. Кодирование/раскодирование баз данных Access в книге Access 2002 – само по себе шифрование базы данных еще не гарантирует ее надежной защиты, но все же препятствует ее просмотру средствами, внешними по отношению к Access и Jet. При шифровании базы данных ее файл сжимается и становится недоступным для чтения с помощью служебных программ или текстовых редакторов.

Защиту от Shift можно применять только при условии, что база преобразована в .mde. В противном случае ее легко обойти, сделав простой импорт всех объектов в новую базу. Обычно защиту от Shift применяют в комплексе с другими методами: привязка к компьютеру, вход по паролю, шифрование данных и т. д. [3].

Запуск приложения через форму авторизации – в Access предусмотрена возможность задать пароль на базу данных. Однако сам пароль хранится в системном реестре в незашифрованном виде. Можно создать аналогичный интерфейс, но уже с зашифрованным паролем, чтобы при попытке открыть форму, если пользователю удалось войти в базу, она аварийно закрывалась.

Использование защиты на уровне пользователя позволяет установить различные уровни доступа к важным данным и объектам в базе данных. Чтобы воспользоваться базой данных, необходимо ввести пароль при запуске Microsoft Access. После этого анализируется файл рабочей группы, в котором каждый пользователь идентифицируется уникальным кодом [4].

Защита страниц доступа к данным – страницы доступа к данным фактически сохраняются не в файле Microsoft Access, а в виде файла HTML в локальной файловой системе, в папке на общем сетевом ресурсе или на HTTP-сервере. Чтобы защитить страницу доступа к данным, необходимо защитить ссылку и файл HTML с помощью средств защиты файловой системы компьютера, на котором эти файлы хранятся.

Защита с модификацией файла – этот способ защиты основан на модификации первых байт файла. Таким образом, перед открытием БД в ее файл записывается правильный заголовок, хранимый в программе, а после закрытия возвращается неправильный.

Защита с использованием электронного ключа – со стартом операционной системы запускается некий процесс, который отслеживает все обращения к защищенному файлу БД. Если это обращение исходит от обычного приложения, то файл читается и выводится сообщение о «нераспознаваемом формате базы данных». Но если с файлом работает указанное при шифровании приложение, то данные передаются ему в дешифрованном виде.

Информационная безопасность относится к числу дисциплин, развивающихся чрезвычайно быстрыми темпами. Этому способствуют как общий прогресс информационных технологий, так и постоянное противоборство нападающих и защищающихся. Обеспечение информационной безопасности современных информационных систем требует комплексного подхода. Реальная безопасность нуждается в каждодневной работе всех заинтересованных сторон.

Список источников

1. http://securit.lv/archives/1653.
2. http://msvb.narod.ru/doc_access.htm.
3. http://www.studfiles.ru/dir/cat32/subj1166/file9304/view98440/page2.html.
4. http://www.bibliofond.ru/view.aspx?id=66106.
5. http://www.accessoft.ru/Text/Text10_12.html.