Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра сетей и устройств телекоммуникаций

ЗАЩИТА БАЗ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ НА ПРИМЕРЕ СУБД MICROSOFT ACCESS

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к лабораторной работе
по дисциплине «Защита программного обеспечения
и баз данных в сетях телекоммуникаций»
для студентов специальностей I-45 01 03 «Сети телекоммуникаций»
и I-45 01 05 «Защита информации» всех форм обучения

Минск 2007

УДК 681.3.06 (075.8)
ББК 32.973.202-018.2 я73
З-40

Составители:
М. Н. Бобов, П. М. Буй

З-40 **Защита** баз данных в телекоммуникационных сетях на примере СУБД Microsoft Access : метод. указания к лаб. работе по дисц. «Защита программного обеспечения и баз данных в сетях телекоммуникаций» для студ. спец. I-45 01 03 «Сети телекоммуникаций» и I-45 01 05 «Защита информации» всех форм обуч. / сост. М. Н. Бобов, П. М. Буй. – Минск : БГУИР, 2007. – 28 с. : ил.

Исследуются методы защиты программного обеспечения и баз данных на примере защиты СУБД Microsoft Access. Рассматривается методика применения мастера защиты Microsoft Access.

Лабораторная работа может быть использована при изучении других курсов, связанных с защитой программного обеспечения и баз данных в сетях телекоммуникаций.

УДК 681.3.06 (075.8)
ББК 32.973.202-018.2я 73

ЦЕЛЬ ЛАБОРАТОРНОЙ РАБОТЫ

Изучение защиты системы управления базами данных Microsoft Access.

1. ОСНОВЫ РАБОТЫ В СУБД MICROSOFT ACCESS

База данных – это набор записей и файлов, организованных особым образом.

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.

Специальная структура папок и подпапок помогает справиться с несколькими сотнями электронных таблиц или ярлыков. В этом случае человек является диспетчером базы данных. Но если решаемая задача становится слишком сложной (к примеру, необходимо собрать информацию обо всех клиентах и заказах, а данные разбросаны по отдельным текстовым файлам и электронным таблицам; сохранить связи между файлами при вводе новой информации и т.д.), то необходима система управления базами данных.

Microsoft Access – это полнофункциональная реляционная СУБД. В ней предусмотрены все необходимые средства для определения и обработки данных, а также для управления ими при работе с большими объемами информации.

Прежде чем приступать к созданию базы данных, необходимо потратить некоторое время на ее проектирование. Разработка базы данных включает следующие этапы:

– определение назначения базы данных;

– принятие решения о том, какие исходные данные (таблицы) база данных должна содержать;

– определение полей, которые будут входить в таблицы, и выбор полей, содержащих уникальные значения;

– назначение связей между таблицами и окончательный просмотр получившейся структуры;

– создание таблиц, связывание их между собой и экспериментальное наполнение базы пробными данными;

– создание форм, отчетов и запросов для операций с введенными данными.

Разработка базы данных начинается с изучения проблемы, которую она должна разрешить, или потребности, которую она должна удовлетворить. Для решения каждой из этих задач можно создать отдельную базу данных.

Определив набор таблиц, входящих в базу, надо продумать, какая информация о каждом субъекте (или объекте) будет вводиться в каждую из таблиц. Каждое поле БД должно принадлежать отдельной таблице. Информация в каждом поле должна быть структурно-элементарной, т.е. она должна храниться в виде наименьших логических компонентов.

В реляционной базе данных таблицы могут быть связаны друг с другом. Эта связь устанавливается с помощью уникальных полей. Уникальные поля – это поля, в которых значения не могут повторяться. Такое поле (или комбинация полей), которое однозначно идентифицирует запись в таблице, называется первичным ключом.

На заключительном этапе создают формы для ввода информации в базу, отчеты для вывода информации и запросы, с помощью которых производится выборка информации из нескольких таблиц.

Для того чтобы создать новую таблицу, необходимо нажать на кнопку **Таблицы** (**Table**) на левой навигационной панели, а после этого – на кнопку **Создать** (**New**). В результате этого откроется диалоговое окно, в котором приведено пять возможных способов создания таблицы:

– режим таблицы (Datasheet View) – таблица создается путем ввода имен полей в заголовок каждого столбца;

– конструктор (Design View) – таблица создается путем составления списка имен полей и задания свойств каждого поля;

– мастер таблиц (Table Wizard) – таблица создается автоматически с помощью программы-мастера, которая предлагает выбрать поля из списка и содержит заготовки для различных видов таблиц;

– импорт таблиц (Import Table) – таблица создается путем импорта данных из другой базы или из другой электронной таблицы;

– связь с таблицами (Link Table) – таблица создается путем установления связи с таблицей, существующей в другой базе данных.

Формы обеспечивают пользователям возможность ввода данных без необходимости знать, как устроена таблица. Одна форма может содержать данные из нескольких таблиц, благодаря чему обеспечивается возможность ввода данных в разные таблицы из одной формы. Если форма, используемая для ввода записей в базу, полностью соответствует документу-источнику, вероятность ошибок при вводе данных снижается. Как и в случае с таблицами, существует несколько способов создания форм:

- автоформа (AutoForm) – автоматическое создание форм;
- мастер форм (Form Wizard) – создание формы с помощью мастера;
- конструктор (Form Design View) – создание формы вручную в режиме конструктора.

Запросы служат для отбора записей из одной или нескольких таблиц на основе условия, заданного пользователем. В Microsoft Access можно применять пять различных типов запросов: на выборку, с параметрами, перекрестный, на изменение и специфические запросы SQL (Structured Query Language). Большинство запросов, используемых в базах данных, являются запросами на выборку. Запрос на выборку отображает данные из одной или нескольких таблиц.

Отчет – это итоговый документ, создаваемый на основе базы данных. Microsoft Access дает возможность выбора различных способов подготовки отчетов. В отчет могут входить как все данные, так и отдельные избранные данные, содержащиеся в записях. Отчеты можно создавать как на основе таблиц, так и на основе запросов. Гибкость настройки отчетов в соответствии с собственными требованиями, т.е. возможность организации легкого доступа к данным, хранящимся в базе, и определяет название программы Microsoft Access – «доступ». При сохранении отчета сохраняется только его структура. Данные, отображаемые в режиме предварительного просмотра отчета, не сохраняются вместе с отчетом. Данные, выдаваемые отчетом, всегда соответствуют текущему состоянию записей базы данных.

2. АРХИТЕКТУРА ЗАЩИТЫ В СУБД MICROSOFT ACCESS

Информация, имеющая ценность, нуждается в защите как от непреднамеренного, так и от преднамеренного несанкционированного доступа.

Защита паролем, сохранение базы данных в виде MDE-файла (в этом случае базу данных можно открывать для просмотра, но не для изменения) могут скрыть от случайного пользователя возможности, которые не разрешается использовать. Но опытный пользователь Microsoft Access может открыть базу данных при нажатой клавише **Shift** (чтобы не запустить приложение), изучить исходные тексты процедур и определить, как обойти защиту. Чтобы действительно предотвратить несанкционированный доступ к объектам базы, необходимо использовать средства защиты, встроенные в Microsoft Access.

В системе защиты Microsoft Access есть возможность указывать пользователей, которым предоставляется или, наоборот, запрещается доступ к объектам базы данных. Кроме того, есть возможность определять группы пользователей и назначать разрешения на уровне группы, чтобы облегчить построение защиты при большом числе пользователей. Пользователю достаточно быть членом группы, чтобы получить права доступа, установленные для неё.

Microsoft Access хранит информацию о защите в двух местах. Во время установки программа Setup создаст в папке \Program Files\Microsoft Ofice\Office стандартный файл рабочей группы (System.mdw), который впоследствии используется по умолчанию при запуске Microsoft Access. Этот файл содержит информацию обо всех пользователях и группах. При создании базы данных Microsoft Access сохраняет сведения о правах, предоставляемых конкретным пользователям и группам, в файле базы данных.

Общая структура защиты Microsoft Access отображена на рис. 1. Учётные записи пользователей и групп хранятся в файле рабочей группы. Разрешение на доступ к конкретным объектам сохраняется в файле базы данных.

Расположение текущего файла рабочей группы хранится в реестре Windows. Можно использовать служебную программу Wrkadm.exe (администратор рабочих групп) для изменения текущего или определения нового файла рабочей группы. Кроме того, существует возможность выбора

нужного файла рабочей группы во время выполнения приложения, если задать соответствующий параметр командной строки в ярлыке запуска.

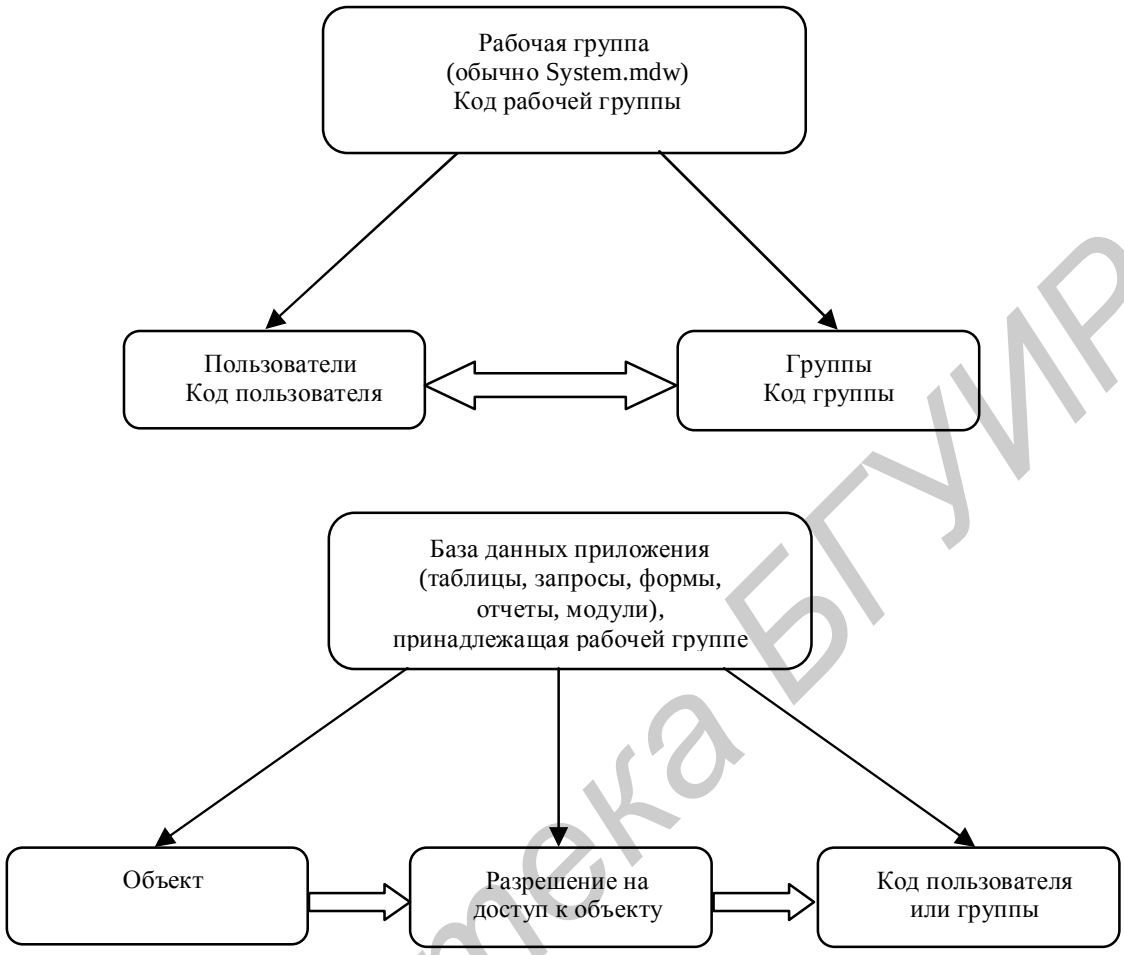

Рис. 1. Общая структура защиты СУБД Microsoft Access

Каждая рабочая группа имеет уникальный внутренний идентификатор, генерируемый Microsoft Access при определении файла рабочих групп. Любая база данных, созданная пользователем рабочей группы, «принадлежит» как этому пользователю, так и рабочей группе. Каждый пользователь и группа также имеют уникальный внутренний идентификатор, но можно дублировать один и тот же код пользователя и группы в нескольких рабочих группах. Когда назначается право доступа к объекту базы данных, Microsoft Access сохраняет в ней внутренний идентификатор пользователя или группы вместе с информацией о доступе. Таким образом, предоставленные права перемещаются вместе с файлом базы данных при копировании его в другую папку или на другой компьютер.

Компьютерная система защиты может быть открытой или закрытой. В открытой системе доступ, если только он не запрещен специально,

предоставляется всем пользователям (даже если они не известны системе). В закрытой системе доступ предоставляется только тем, кому он был разрешен. На первый взгляд, система защиты Microsoft Access кажется открытой, поскольку есть возможность запускать ее без регистрации, создавать базы данных, передавать их другим пользователям, которые могут открывать и изменять их по своему усмотрению. Но на самом деле система защиты Microsoft Access является закрытой и кажется открытой только потому, что в стандартной рабочей группе, используемой по умолчанию, всегда имеются определенные встроенные коды пользователей и групп, общие для всех устанавливаемых копий Microsoft Access.

При установке Microsoft Access всегда создается стандартная рабочая группа, содержащая один встроенный код пользователя и два встроенных кода групп. Код пользователя называется Admin, и для него не определен пароль. Microsoft Access автоматически загружается с этим кодом и предоставляет пользователю все права и привилегии этого пользователя. При создании базы данных или нового объекта в базе данных текущий код пользователя становится владельцем объекта и получает полные права на доступ к этому объекту. Поскольку большинство пользователей Microsoft Access никогда не используют защиту и загружаются как пользователи Admin, владельцем всего, что они создают, является универсальный код Admin.

Первой встроенной группой является группа Users. Все пользователи, в том числе и новые, становятся ее членами и не могут быть удалены из нее. Кроме того, внутренний идентификатор группы Users всегда один и тот же во всех устанавливаемых в мире копиях Microsoft Access. Группе Users автоматически предоставляются полные права доступа к любому новому объекту или базе данных, которые вы создаете. Это означает, что даже если пользователь зарегистрировался с иным кодом, чем Admin, он все равно имеет полный доступ к вашим базам данных и объектам в них, поскольку пользователь всегда является членом универсальной группы Users.

Вторая встроенная группа называется Admins. Ее внутренний идентификатор уникален для каждого файла рабочей группы и определяется на основе информации, которую пользователь предоставляет программе администратора рабочих групп при создании файла. По умолчанию в эту группу включен только пользователь Admin, но пользователь может определить другого пользователя, включить его в группу Admins и удалить

пользователя Admin. Эта группа должна содержать по крайней мере одного пользователя.

Группа Admins обладает двумя основными привилегиями. Во-первых, члены группы Admins могут определять и изменять учетные записи пользователей и групп, а также устанавливать и менять пароли. Во-вторых, члены группы Admins имеют полный доступ к любым базам данных, созданным при использовании этого файла рабочей группы. Члены этой группы могут первоначально не иметь никаких разрешений на доступ к объектам, но могут назначить себе нужные права. Для понимания этого свойства важно иметь в виду, что любая база данных, созданная при использовании конкретного файла рабочей группы, наследует код этой рабочей группы. Некий пользователь может быть членом группы Admins в другом файле рабочей группы, но если коды рабочих групп не совпадают, этот пользователь не получит прав доступа к текущей базе данных.

В таблице приведены разрешения, которые можно назначать базе данных или ее объектам. У владельца объекта может и не быть никаких конкретных разрешений, но, пользуясь своим статусом владельца, он имеет право предоставлять любые или все разрешения любому пользователю или группе, включая себя самого.

Пользователь может получить доступ к объекту, благодаря разрешению, назначенному его коду пользователя, или через разрешения, предоставленные любой группе, к которой он принадлежит. Microsoft Access использует модель «наименее ограничительных» разрешений. Это подразумевает, что пользователь обладает наибольшими правами доступа, предоставленными его коду пользователя и любой из групп, в которые он включен. На рис. 2 показано гипотетическое множество пользователей и групп вместе с разрешениями доступа к объекту «Таблица», явно назначенными каждому пользователю и группе. Отдельные пользователи могут неявно наследовать дополнительные разрешения или права благодаря их членству в одной или нескольких группах. К примеру, Денис имеет по крайней мере разрешения на чтение, обновление, вставку и удаление данных, так как он является членом группы «Маркетинг». Будучи владельцем объекта «Таблица» (как его создатель), Денис также получает права администратора и разрешение на изменение макета, так как Microsoft Access назначает эти разрешения при создании объекта. А если кто-то

другой создал этот объект и позднее передал права владельца Денису, то Денис может предоставить самому себе любые отсутствующие разрешения.

Таблица

Разрешение	Объект	Разрешённые действия
Открытие/запуск (Open/Run)	База данных, форма, отчет, макрос	Открытие базы данных, формы или отчета, запуск макроса. (Любой пользователь может выполнять процедуры в модулях)
Монопольный доступ (Open Exclusive)	База данных	Открытие базы данных для монопольного доступа. Без этого разрешения пользователь не может открыть базу данных и отключить других пользователей
Чтение макета (Read Design)	Таблица, запрос, форма, отчет, макрос, модуль	Просмотр объектов в режиме конструктора. Если для таблицы или запроса предоставлен любой тип доступа к данным, автоматически дается разрешение на чтение макета, поскольку оно необходимо для корректного открытия набора записей
Изменение макета (Modify Design)	Таблица, запрос, форма, отчет, макрос, модуль	Просмотр и изменение макета объектов. Если в приложении используется программа Visual Basic, изменяющая макеты запросов во время выполнения, пользователь должен предоставить разрешение на изменение макета всем пользователям этих запросов
Администратора (Administer)	База данных, таблица, запрос, форма, отчет, макрос, модуль	Предоставление разрешений на доступ к объекту, даже если пользователь или группа не является владельцем объекта
Чтение данных (Read Data)	Таблица, запрос	Просмотр данных таблицы. Дает разрешение на чтение макета. В случае запроса пользователь должен иметь разрешение также на чтение данных для всех используемых в нем таблиц или запросов
Обновление данных (Update Data)	Таблица, запрос	Обновление данных таблицы или запроса. Предоставляет разрешения на чтение данных и макета. В случае запроса пользователь должен иметь также разрешение на обновление данных для всех таблиц, изменяемых с его помощью
Вставка данных (Insert Data)	Таблица, запрос	Вставка данных в таблицу или запрос. Предоставляет разрешения на чтение данных и макета. В случае запроса пользователь должен дополнительно иметь разрешение на вставку данных для всех таблиц или запросов, изменяемых с его помощью
Удаление данных (Delete Data)	Таблица, запрос	Удаление данных из таблицы или запроса. Предоставляет разрешения на чтение данных и макета. В случае запроса пользователь должен дополнительно иметь разрешение на удаление данных для всех таблиц, изменяемых с его помощью

Поскольку пользователи всегда являются членами группы Users, которой по умолчанию предоставляются все права доступа к любому новому объекту, любой другой пользователь, а не только Admin, может получить полный доступ ко всем объектам базы данных.

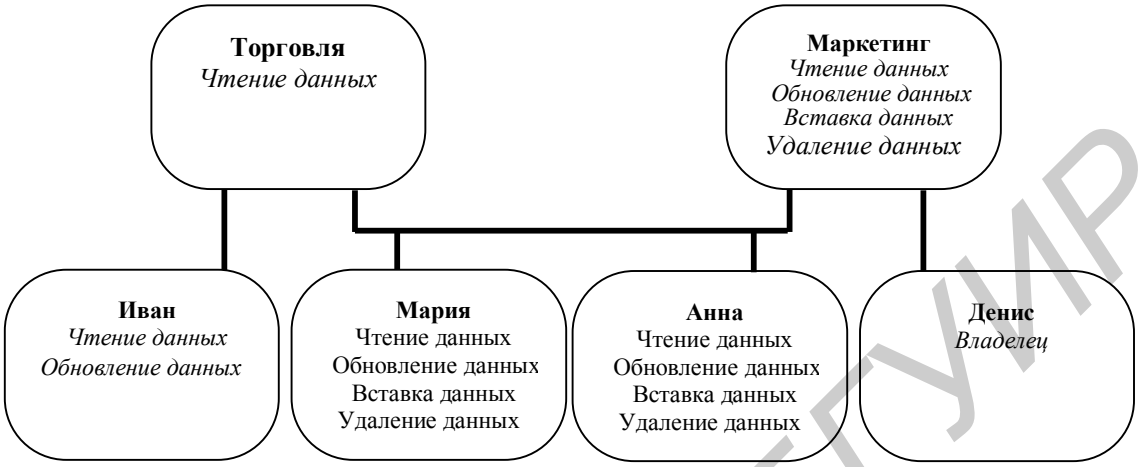

Рис. 2. Явно и неявно назначенные разрешения (явные разрешения напечатаны обычным шрифтом, а неявные – курсивом)

3. ИСПОЛЬЗОВАНИЕ МАСТЕРА ЗАЩИТЫ В СУБД MICROSOFT ACCESS

При обычной установке Microsoft Access стандартная рабочая группа создается на основе информации о пользователе Windows и названии организации. Поэтому любому человеку, имеющему доступ к компьютеру, не составляет особого труда выяснить эти сведения и продублировать их. Поэтому нужна уникальная рабочая группа, чтобы было трудно воспроизвести ее идентификатор, дающий всем членам группы Admins право изменять разрешения. Затем потребуется код пользователя, отличный от Admin, в качестве владельца базы данных и всех ее объектов. Кроме этого, для всех объектов необходимо удалить разрешения из группы Users. Чтобы никто не мог изучить данные и тексты процедур с помощью служебных программ для просмотра дисков, вы должны зашифровать базу данных.

Можно проделать все эти этапы «вручную», но Microsoft предоставляет мастера, помогающего установить защиту на уровне пользователя. Он выполнит за пользователя перечисленные выше шаги, включая шифрование базы данных.

Для того чтобы мастер защиты успешно выполнил работу по установке защиты базы данных, пользователь должен зарегистрироваться под именем владельца защищаемой базы данных или в том же файле рабочей группы, который использовался им при создании базы данных, и при этом быть в нем членом группы Admins. Одним из важнейших шагов является создание новой рабочей группы с уникальным кодом, которая, скорее всего, будет отличаться от рабочей группы, использовавшейся при создании базы данных. Кроме того, при создании базы данных пользователь, вероятнее всего, был зарегистрирован как пользователь Admin, а для базы данных, владельцем которой является Admin, нельзя установить защиту. В этом случае придется назначить нового владельца.

Мастер защиты в Microsoft Access позволяет защитить базу данных, даже если пользователь зарегистрировался как пользователь Admin в первоначальной рабочей группе. В этой ситуации мастер заставит его создать новую рабочую группу. В новой рабочей группе мастер сделает владельцем базы данных новый код пользователя. Но это возможно только в том случае, если пользователь является владельцем базы данных. Пользователь также может перед запуском мастера создать новую рабочую группу и в ней новый код пользователя (не Admin) в группе Admins, но этот пользователь должен быть владельцем базы данных, в противном случае попытка мастера переназначить владельца окажется безуспешной.

Для того чтобы лучше понять систему защиты Microsoft Access, необходимо сначала создать новую рабочую группу, определить по крайней мере один код пользователя и создать пользователя Admin из группы Admins. Далее, найти программу Wrkgadm.exe – администратора рабочих групп на компьютере. При установке Microsoft Access она обычно помещается в папку, в которой установлен пакет Microsoft Office.

Начальное окно диалога администратора рабочих групп для Microsoft Access не отображает имя пользователя и название организации. Но эту важную для защиты информацию все равно можно легко найти, открыв любое приложение Microsoft Office на компьютере и выбрав команду **Справка → О программе** (**Help → About**). Здесь приведен полный путь к текущему файлу рабочей группы. Как показано на рис. 3, стандартный файл рабочей группы называется System.mdw и находится в папке Office. Если был создан другой

файл рабочей группы, то в окне диалога, которое открывается щелчком на кнопке **Связь** (**Join**), появляется возможность ввести путь к этому файлу или воспользоваться кнопкой **Обзор** (**Browse**) для указания его местонахождения.

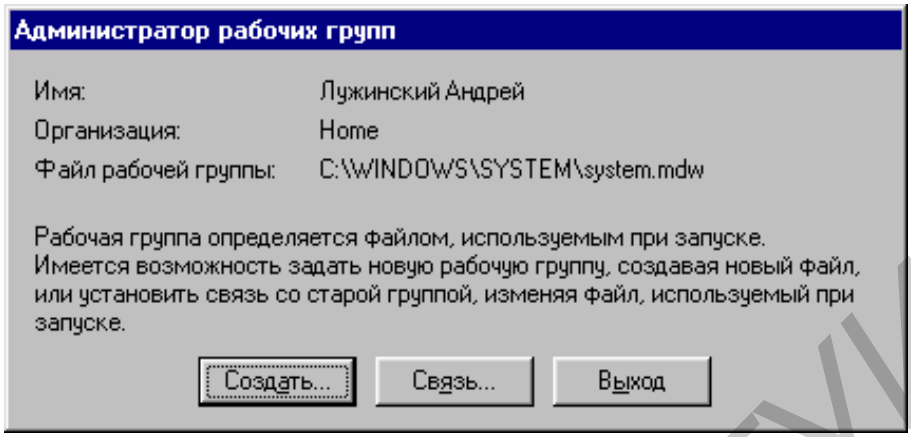

Рис. 3. Начальное окно диалога администратора рабочих групп

Чтобы создать и подключить новую рабочую группу, необходимо нажать на кнопку **Создать** (**Create**). В результате откроется второе окно диалога администратора рабочих групп, представленное на рис. 4. Здесь необходимо заполнить поля **Имя** (**Name**) и **Организация** (**Organization**), а в качестве кода группы ввести комбинацию из букв и цифр длиной до 20 символов. Администратор рабочих групп использует содержимое трех полей для генерации уникального 64-разрядного внутреннего идентификатора. Чтобы создать другой файл рабочей группы с идентичным идентификатором, нужно ввести ту же информацию в эти три поля, причем код группы должен совпадать с точностью до регистра. Эта информация должна храниться в безопасном месте, чтобы можно было воссоздать файл рабочей группы, если он будет удален или испорчен.

Нажатие на кнопку **ОК** позволит перейти в окно диалога, в котором можно задать имя и местонахождение нового файла рабочей группы. Для завершения создания файла рабочей группы необходимо нажать на кнопку **ОК** в этом окне диалога. Администратор изменит параметры в системном реестре, чтобы «связать» пользователя с только что созданной рабочей группой. Последовательное нажатие кнопки **ОК** в окне подтверждения и затем кнопки **Выход** (**Exit**) в начальном окне диалога закроет окно администратора рабочих групп. Если на компьютере запущено приложение Microsoft Access, необходимо закрыть его и снова запустить в новой рабочей группе.

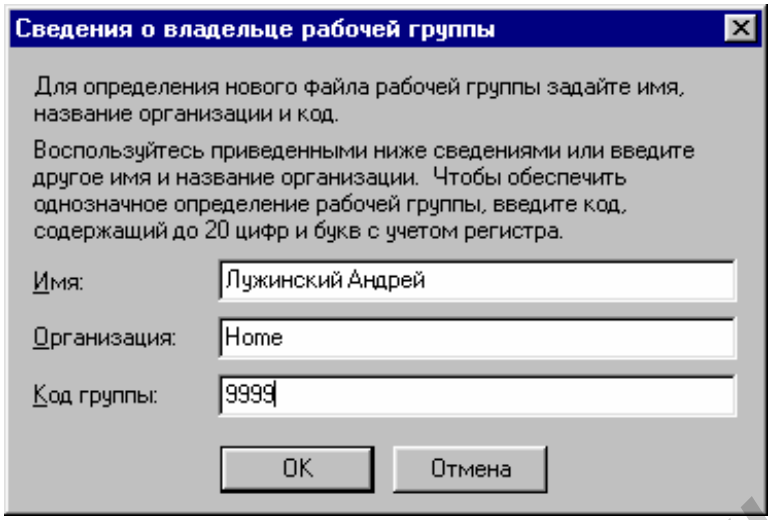

Рис. 4. Второе окно диалога администратора рабочих групп

После запуска Microsoft Access в новой рабочей группе нужно добавить нового пользователя, включить его в группу Admins, определить пароль для пользователя Admin и удалить его из группы Admins. Для этого не требуется открывать базу данных. После открытия Microsoft Access необходимо выбрать команду **Сервис → Защита → Пользователи и группы** (**Tools → Security → → User And Group Accounts**), и на экране появится окно диалога **Пользователи и группы** (**User And Group Accounts**), изображенное на рис. 5.

Если на вкладке **Пользователи** (**Users**) раскрыть список **Имя** (**User**), то появится единственный пользователь, определенный в этой рабочей группе, – Admin. По спискам, расположенным в нижней части вкладки, можно судить, что пользователь Admin включен в обе встроенные группы. В верхней части вкладки **Пользователи** находится три кнопки:

– **Создать…** – предназначена для определения нового пользователя;

– **Удалить** – предназначена для удаления пользователя, выбранного в списке (Microsoft Access не позволит удалить пользователя Admin);

– **Снять пароль** – предназначена для снятия пароля выбранного пользователя.

Следующим шагом нужно определить нового пользователя, который станет владельцем всех объектов, являясь при этом членом группы Admins. Для этого необходимо нажать на кнопку **Создать** (**New**). В результате откроется окно диалога **Новый пользователь или группа** (**New User/Group**), также показанное на рис. 5. Например, в файле рабочей группы Secured.mdw был создан пользователь с именем Andrey и личным кодом 9999. Личный код

должен содержать не менее четырех, но не более 20 букв и цифр. Комбинация прописных и строчных букв имеет большое значение. Так, в случае ввода ANDREY вместо Andrey будет создан пользователь, имеющий совершенно другой внутренний идентификатор.

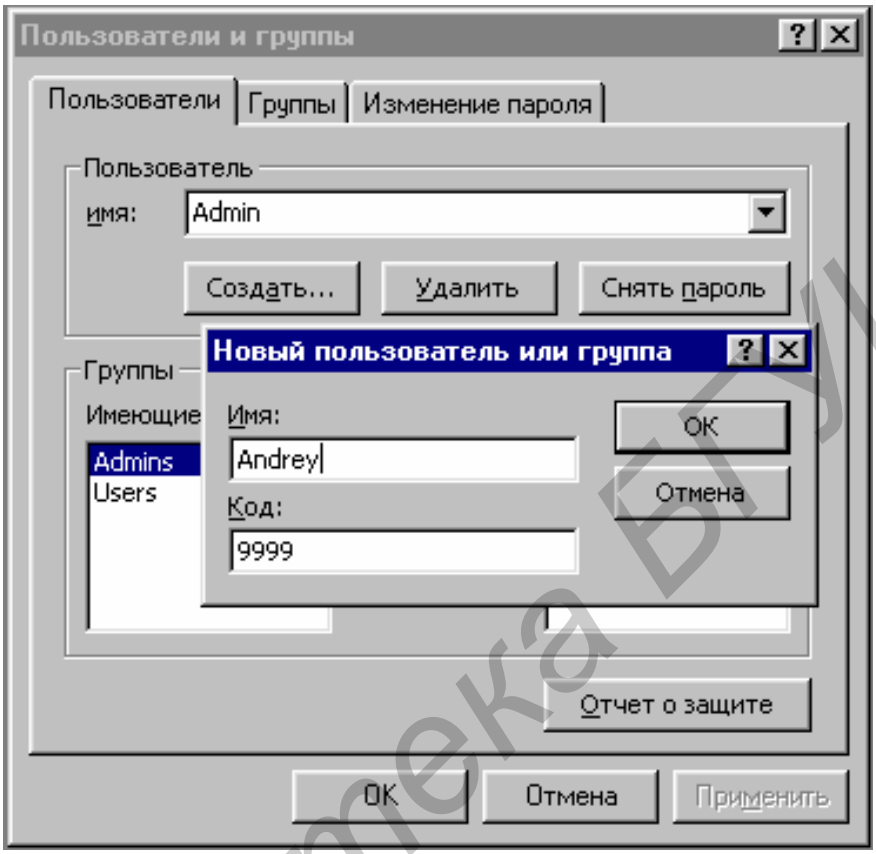

Рис. 5. Создание нового пользователя в окне диалога **Пользователи и группы**

Чтобы добавить пользователя, необходимо нажать на кнопку **ОК**. Он появится в списке **Имя** (**Name**). В списке **Имеющиеся группы** (**Available Groups**) необходимо выделить группу Admins и нажать на кнопку **Добавить** (**Add**), чтобы сделать нового пользователя членом этой группы. Новый пользователь уже включен в группу Users, что дает ему полные права доступа ко всем объектам в любой незащищенной базе данных. Из группы Users нельзя удалить никакого пользователя.

Чтобы исключить пользователя Admin из группы Admins, необходимо выбрать текущее имя пользователя (Admin) в раскрывающемся списке **Имя**, выделить группу Admins в списке **Участие в группе** (**Member Of**) и нажать на кнопку **Удалить** (**Remove**). Microsoft Access не позволит пользователю это сделать до тех пор, пока новый пользователь не будет создан и не добавлен в группу Admins. Для того чтобы изменить пароль, необходимо перейти на

вкладку **Изменение пароля** (**Change Logon Password**), как показано на рис. 6, и ввести пароль в поля **Новый пароль** (**New Password**) и **Подтверждение** (**Verify**).

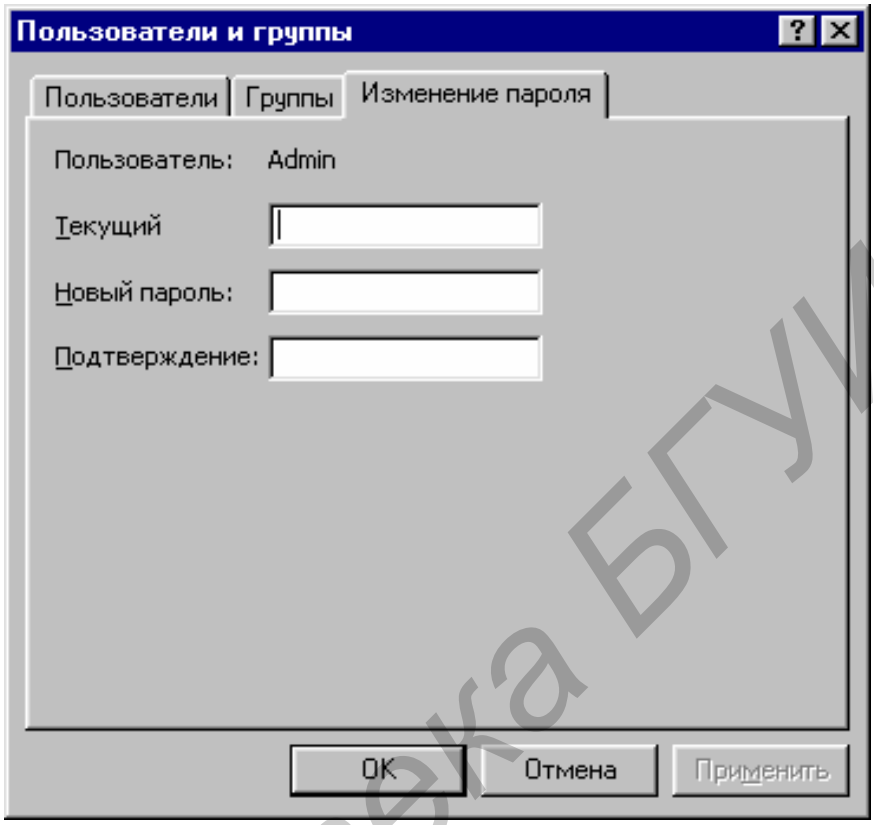

Рис. 6. Изменение пароля в окне диалога **Пользователи и группы**

Для подтверждения смены пароля необходимо нажать на кнопку **Применить** (**Apply**), назначив тем самым пароль для пользователя Admin. После задания пароля для Admin при последующих запусках Access в этой рабочей группе программа будет запрашивать имя пользователя и пароль.

После создания нового пользователя необходимо закрыть и снова запустить Access. Теперь при открытии любой базы данных Access будет запрашивать имя пользователя и пароль, поскольку пользователь по умолчанию (Admin) уже защищен паролем.

4. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

А) Создайте базу данных, содержащую две таблицы, три запроса, одну форму и один отчет, с использованием СУБД Microsoft Access.

Б) Создайте несколько новых групп.

В) Создайте пользователей и включите их в только что созданные группы.

Чтобы определить пользователя как члена группы, выберите команду **Сервис → Защита → Пользователи и группы**. На вкладке **Пользователи** (**Users**) выберите пользователя, которого вы хотите включить в одну или несколько групп. В левом списке окна диалога отображаются имеющиеся группы, а в правом списке – группы, в которые входит этот пользователь. На рис. 7 показано добавление в группу NotAdmin пользователя Buchanan_Nike.

Г) Проверьте разрешения пользователей и групп. Для этого сначала откройте нужную базу данных. Вы должны быть владельцем базы данных и всех объектов, которые хотите проверить, или иметь разрешение администратора на доступ к базе данных и объектам. После выбора команды **Сервис → Защита → Разрешения** (**Tools → Security → User And Group Permissions**) Microsoft Access откроет окно диалога, показанное на рис. 8.

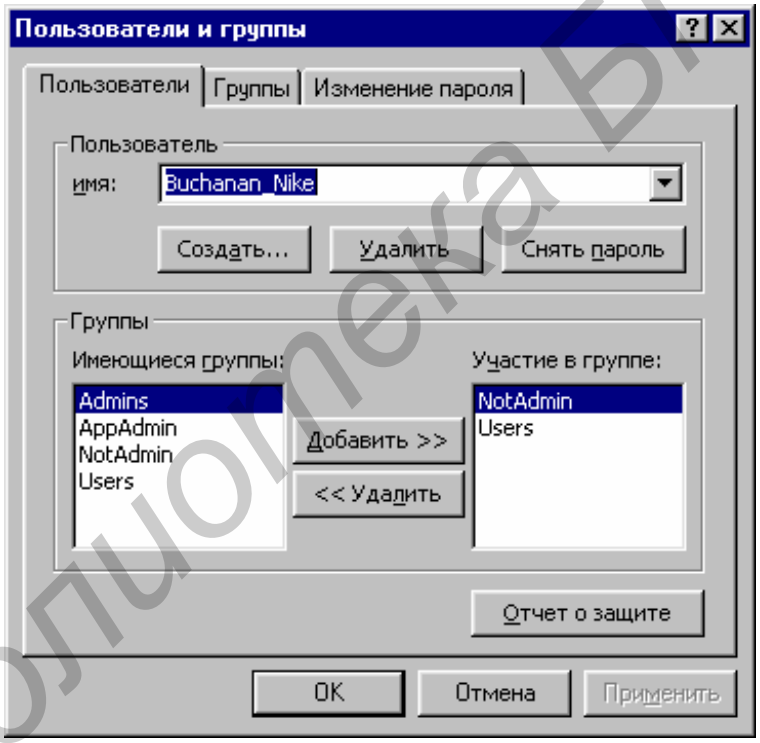

Рис. 7. Включение пользователя в группу

В списке в левой верхней части окна отображаются пользователи или группы, определенные в базе данных. Установите переключатель **Пользователи** (**Users**) или **Группы** (**Groups**) в зависимости от того, что вы хотите увидеть. В списке **Имя объекта** (**Object Name**) выводятся объекты базы данных. Пользуясь расположенным ниже раскрывающимся списком, можно изменить тип отображаемых объектов. После выбора нужного объекта флажки в нижней части окна отобразят явно назначенные разрешения. Если вы

выберете группу Users и просмотрите объекты, то убедитесь, что она имеет полные права доступа ко всем объектам. Кроме того, имея права администратора на доступ к объектам, можно выбирать любые из этих объектов и изменять разрешения, предоставляемые пользователю или группе.

Не пробуйте изменять разрешения или владельца объекта до тех пор, пока полностью не поймете все возможные последствия такого действия.

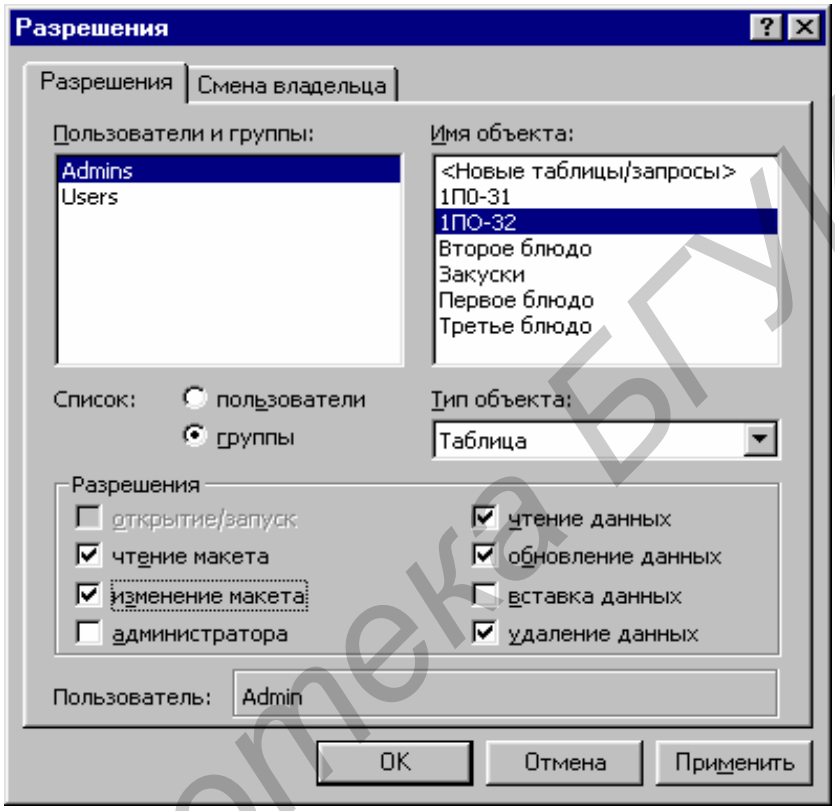

Рис. 8. Некоторые разрешения, предоставленные группе Users

На вкладке **Смена владельца** (**Change Owner**) для любого объекта определите, кто (пользователь или группа) является его текущим владельцем. В большинстве случаев всеми объектами владеет пользователь Admin. Выделите один или несколько объектов и выберите другого пользователя или группу, нажав на кнопку **Сменить владельца** (**Change Owner**). Никогда не передавайте объект другому владельцу, если вы полностью не понимаете возможные последствия такого действия. Прежде чем назначить объекту нового владельца, вы должны твердо знать, как зарегистрироваться в качестве такого владельца. Если вы владеете объектом, то всегда можете передать права владельца другому коду пользователя или группы или отобрать их.

Д) Зарегистрируйтесь как новый (не Admin) пользователь. При задании пароля пользователю Admin используйте пароль, выданный преподавателем.

Е) Создайте новую пустую базу данных.

Ж) Импортируйте все объекты из базы данных, которую вы хотели защитить, с помощью команды **Файл → Внешние данные → Импорт** (**File → → Get External Data → Import**). Укажите исходную базу данных и затем в окне диалога **Импорт** (**Import**) обязательно выделите все объекты.

З) Запустите мастер защиты базы данных. Для этого выберите команду **Сервис → Защита → Мастер** (**Tools → Security → User-Level Security Wizard**). Откроется окно диалога, представленное на рис. 9.

Первое окно диалога содержит краткое описание работы мастера и предоставляет две возможности. Установите верхний переключатель, мастер создаст новый файл рабочей группы, создаст новый код пользователя (не Admin) в этой рабочей группе и затем установит защиту для базы данных, используя эту рабочую группу и нового пользователя. При установке нижнего переключателя Microsoft Access защитит базу данных, используя текущую рабочую группу и текущий код пользователя.

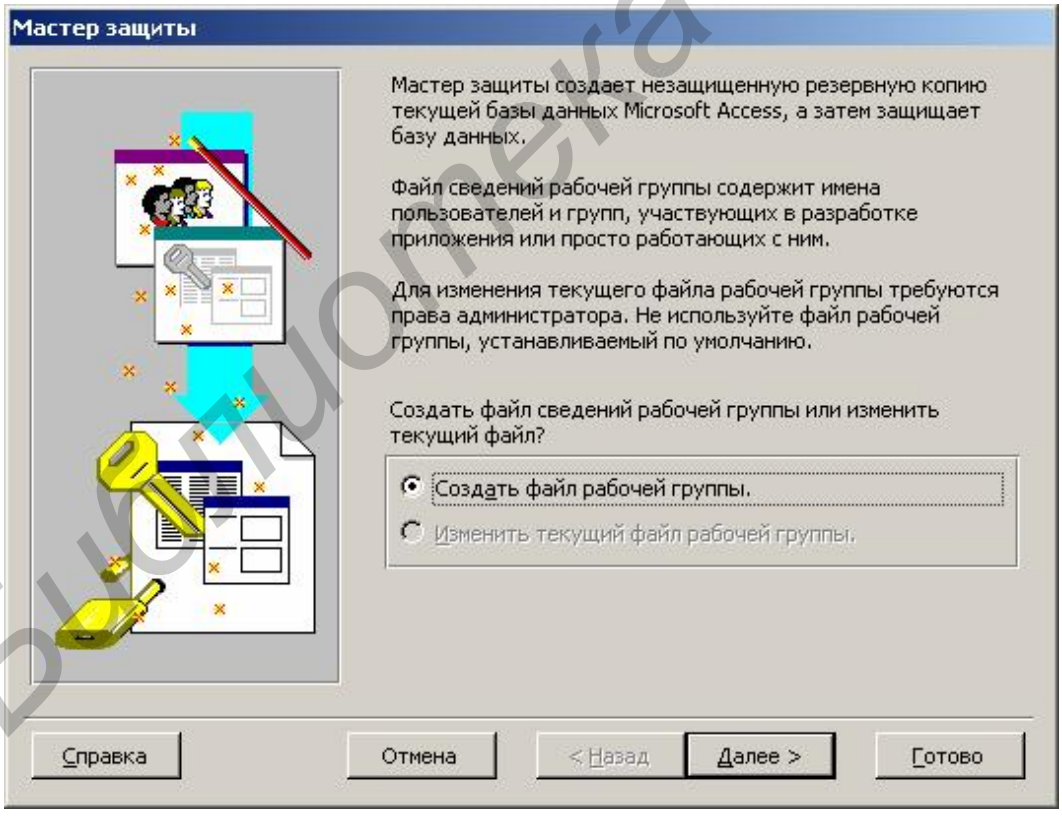

Рис. 9. Начальное окно диалога мастера защиты

Нажмите кнопку **Далее** (**Next**), чтобы перейти в следующее окно мастера, показанное на рис. 10.

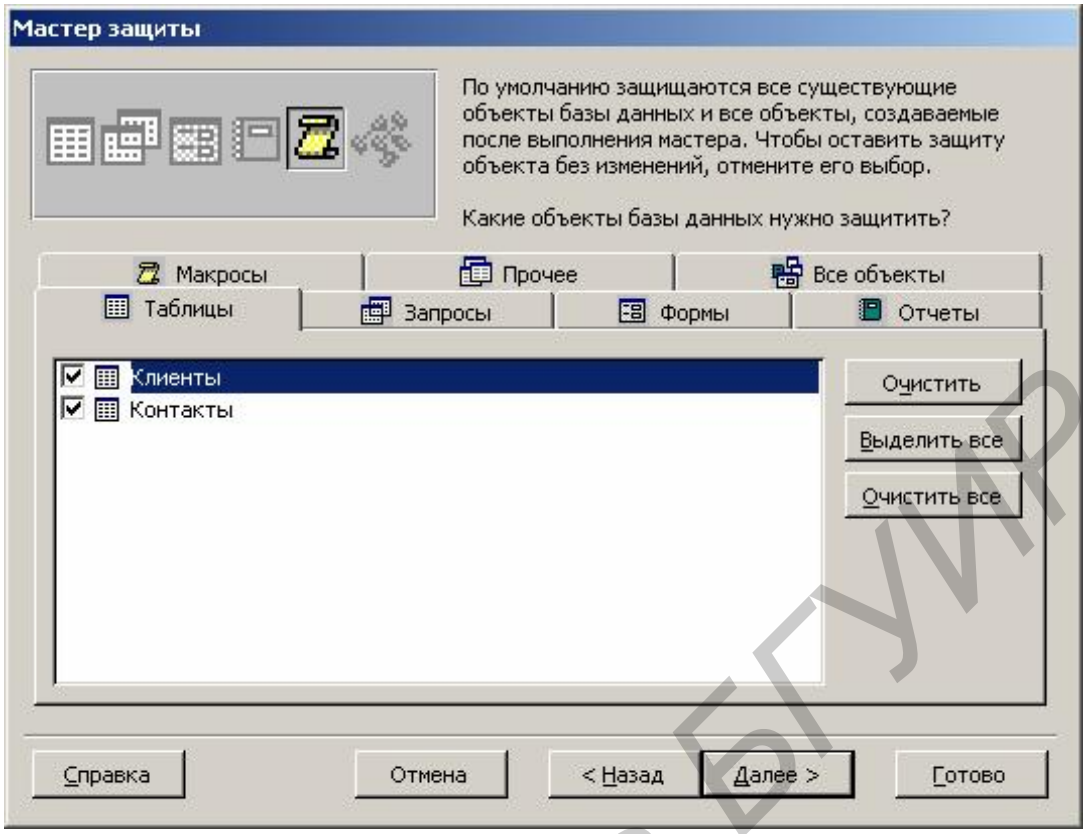

Рис. 10. Выбор объектов, которые нужно защитить

По умолчанию мастер защищает все объекты базы данных. Отмените выбор определенных объектов, сняв флажки рядом с их именами. Нажмите кнопку **Далее**.

В следующем окне диалога, показанном на рис. 11, мастер предложит создать одну или несколько дополнительных групп. После их создания нажмите на имя группы в левом списке, чтобы увидеть разрешения, которые будут предоставлены этой группе. Поставьте созданным группам разрешения только на чтение и запуск, установив флажок **Только чтение** (**Read-Only Users**).

Примите генерируемый случайным образом код группы, отображаемый в этом окне мастера, или введите свой собственный код. Мастер предоставляет возможность определить пользователей и включить их в выбранные группы. Нажмите на кнопку **Далее**, чтобы перейти в следующее окно диалога, представленное на рис. 12.

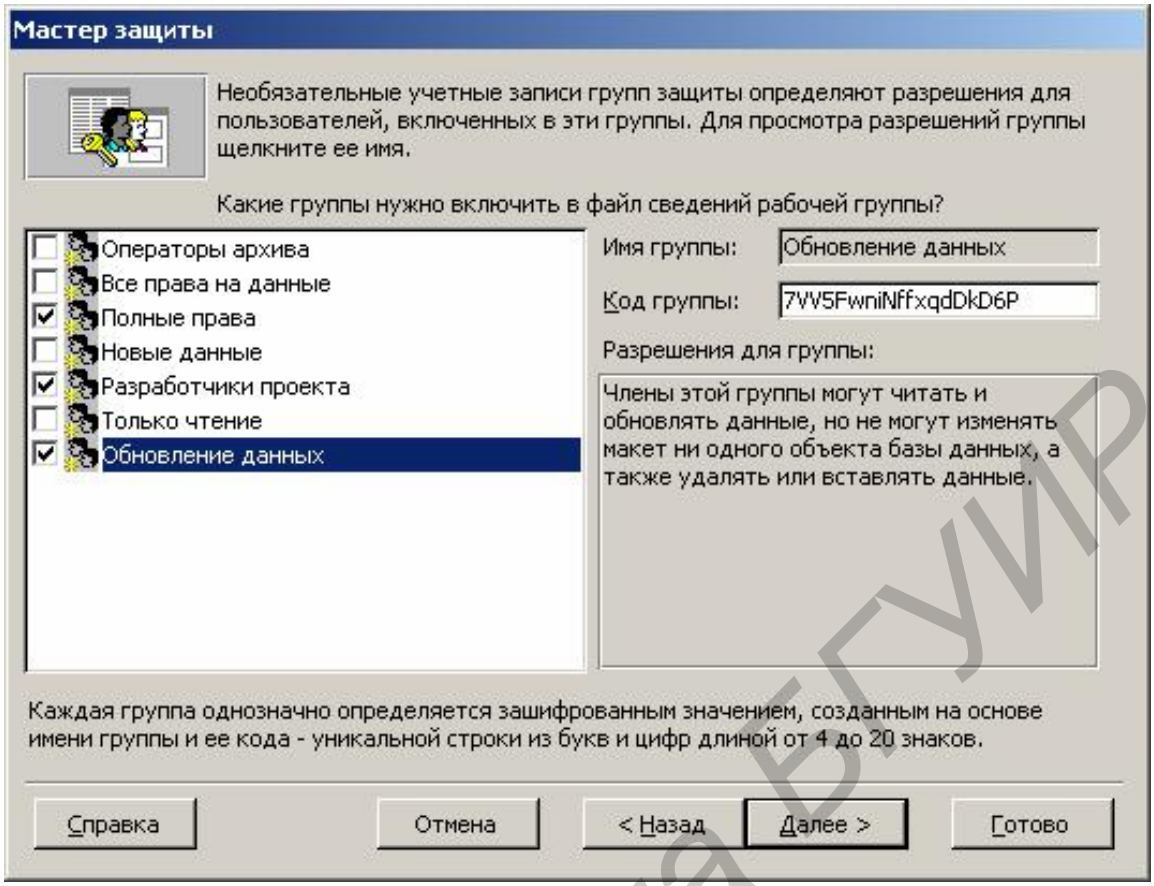

Рис. 11. Выбор дополнительных групп, создаваемых мастером

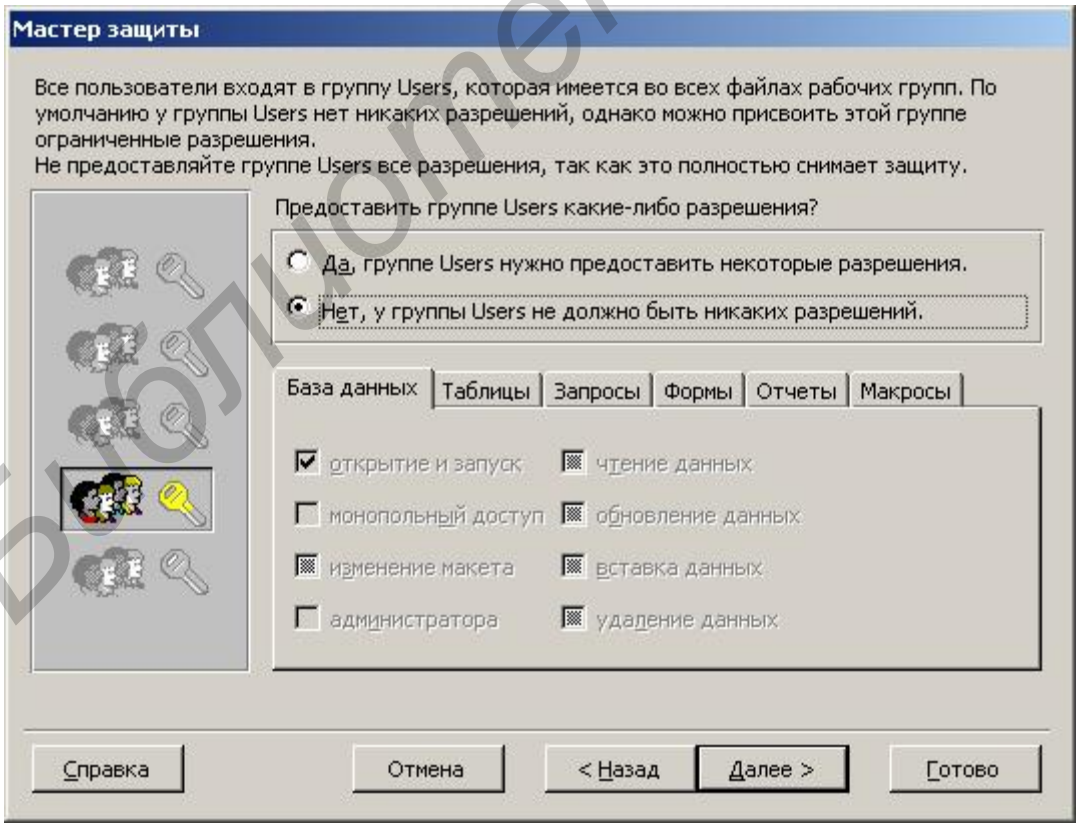

Рис. 12. Предоставление некоторых разрешений группе Users

Это окно мастера позволяет предоставить некоторые разрешения универсальной группе Users. По умолчанию для полной защиты базы данных мастер не оставляет этой группе каких-либо разрешений. Если вы откроете защищенную базу данных, то обнаружите, что вы можете просматривать любые данные и макеты всех объектов, но вам не удастся внести какие-либо изменения. Это было достигнуто путем предоставления группе Users разрешения **Открытие/запуск** (**Open/Run**) для базы данных, а для всех других объектов – разрешения **Чтение макета** (**Read Disign**) или **Чтение данных** (**Read Data**). Нажмите на кнопку **Далее**, чтобы перейти в следующее окно диалога, показанное на рис. 13.

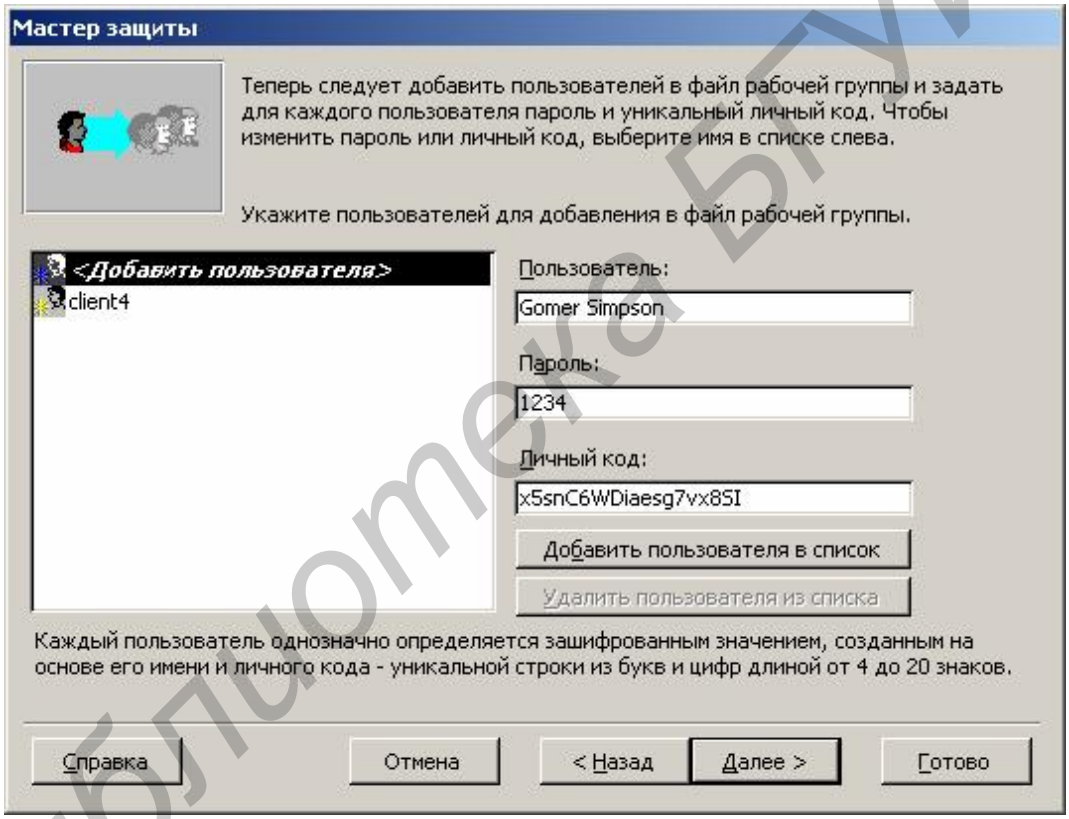

Рис. 13. Определение новых пользователей в рабочей группе

Добавьте несколько пользователей в рабочую группу. Для этого нажмите на элементе **Добавить пользователя** (**Add NewUser**) в начале списка, заполните поля **Пользователь** (**UserName**), **Личный код** (**PID**) и (необязательно) **Пароль** (**Password**) и затем нажмите на кнопку **Добавить пользователя в список** (**Add This User To The List**).

Новые пользователи, добавленные в этом окне, помечаются звездочкой, отображаемой рядом со значком. Просмотрите информацию о новом

пользователе, выделив его имя в списке, и в случае ошибки удалите его, нажав на кнопку **Удалить пользователя из списка** (**Delete User From List**).

Нажмите на кнопку **Далее**, чтобы перейти в следующее окно диалога, показанное на рис. 14, в котором вы включите пользователей в нужные группы.

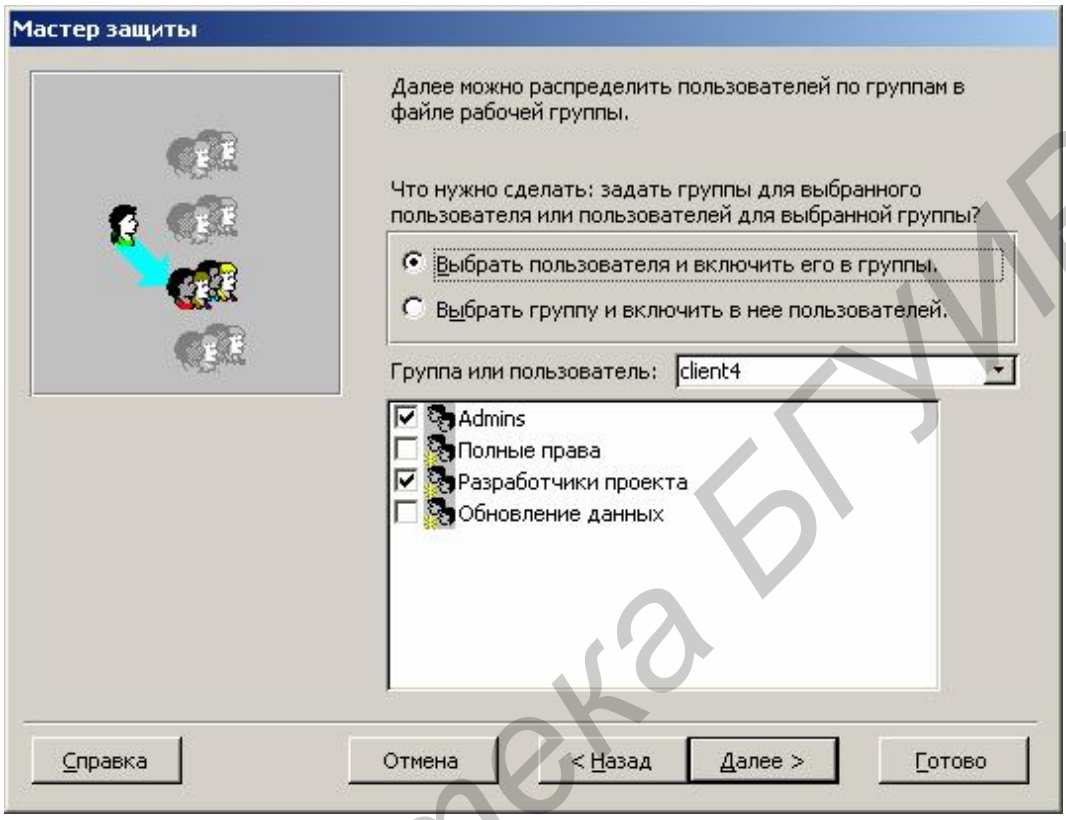

Рис. 14. Определение вхождения пользователя в группу

Нажмите на кнопку **Далее**, чтобы перейти в последнее окно мастера, представленное на рис. 15.

Последнее окно диалога позволяет задать имя резервной копии файла базы данных. В предложенном мастером варианте используется исходное имя базы данных с расширением .bak. Нажмите на кнопку **Готово** (**Finish**), чтобы позволить мастеру закончить работу.

После установки защиты для объектов базы данных мастер выведет отчет со сведениями о новой рабочей группе (если она создавалась) и информацией, которая потребуется при переопределении пользователей и групп, созданных мастером. При закрытии окна отчета мастер предложит сохранить отчет в файле снимка (с расширением .snp). Данным предложением мастера следует воспользоваться, чтобы не потерять эту очень важную информацию. Затем мастер закроет защищенную базу данных, зашифрует все данные и снова ее откроет.

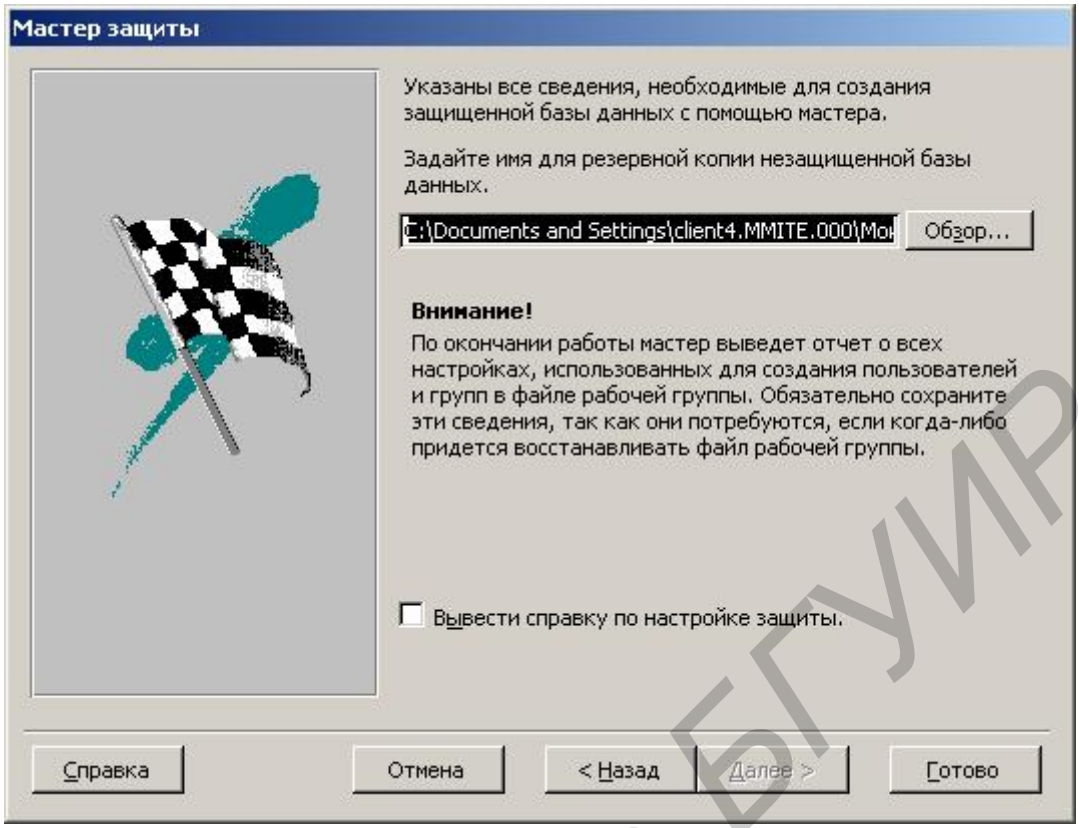

Рис.15. Последнее окно мастера защиты

И) Определите новые группы и пользователей. Это необходимо сделать для того, чтобы облегчить предоставление нужных вам разрешений. Определите группы для каждого уровня доступа, который вы намерены предоставить. Выберите пользователей для включения их в соответствующие группы.

Откройте защищенную базу данных (удерживайте нажатой клавишу Shift, если вы открываете защищенную копию базы данных). Выберите команду **Сервис → Защита → Пользователи и группы** (**Tools → Security → User And Group Accounts**), чтобы вывести на экран окно диалога **Пользователи и группы** (**User And Group Accounts**). На вкладке **Группы** (**Groups**) нажмите на кнопку **Создать** (**New**), чтобы открыть окно диалога **Новый пользователь или группа** (**New User/Group**), показанное на рис. 16. Создание новой группы совершенно аналогично определению нового пользователя – генерация внутреннего идентификатора группы производится с учетом регистра символов в имени и коде. Нажмите на кнопку **ОК**, чтобы добавить новую группу.

Создайте пользователей и включите их в только что созданные группы.

Чтобы определить пользователя как члена группы, выберите команду **Сервис → Защита → Пользователи и группы**. На вкладке **Пользователи**

(**Users**) выберите пользователя, которого вы хотите включить в одну или несколько групп. В левом списке окна диалога отображаются имеющиеся группы, а правом списке – группы, в которые входит этот пользователь. На рис. 17 показано добавление в группу NotAdmin пользователя Buchanan_Nike.

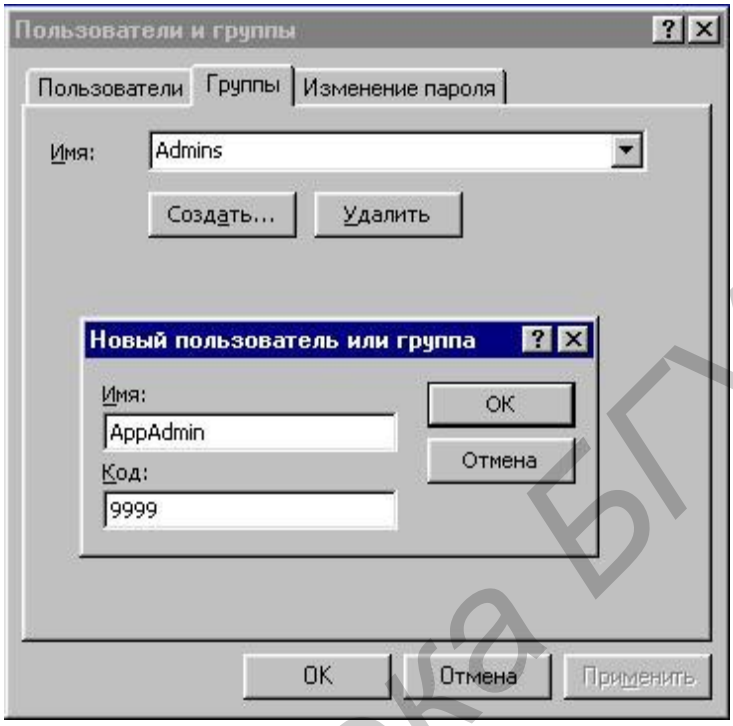

Рис.16. Создание новой группы защиты

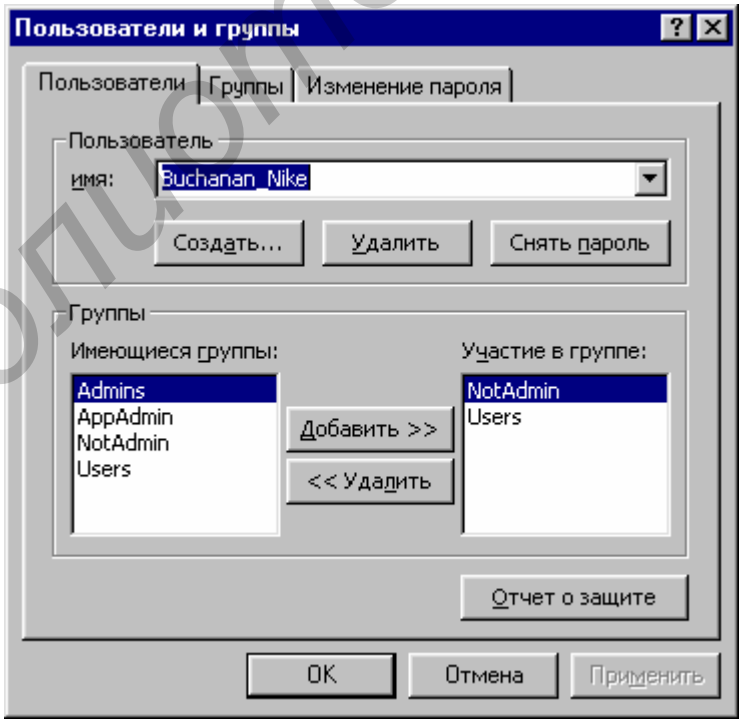

Рис. 17. Включение пользователя в группу

Назначьте разрешения для каждой группы. Закройте окно диалога **Пользователи и группы**. Выберите команду **Сервис → Защита → → Разрешения** (**Tools → Security → User And Group Permissions**), чтобы открыть окно диалога, показанное на рис. 18.

Установите переключатель **Список** (**List**) в положение **Группы** (**Groups**), чтобы увидеть список групп. Выделите необходимую группу в списке **Пользователи и группы** (**User/Group Name**) и затем последовательно выбирайте каждый тип объекта в раскрывающемся списке **Тип объекта** (**Object Type**). Перед выбором каждого нового типа нажимайте на кнопку **Применить** (**Apply**).

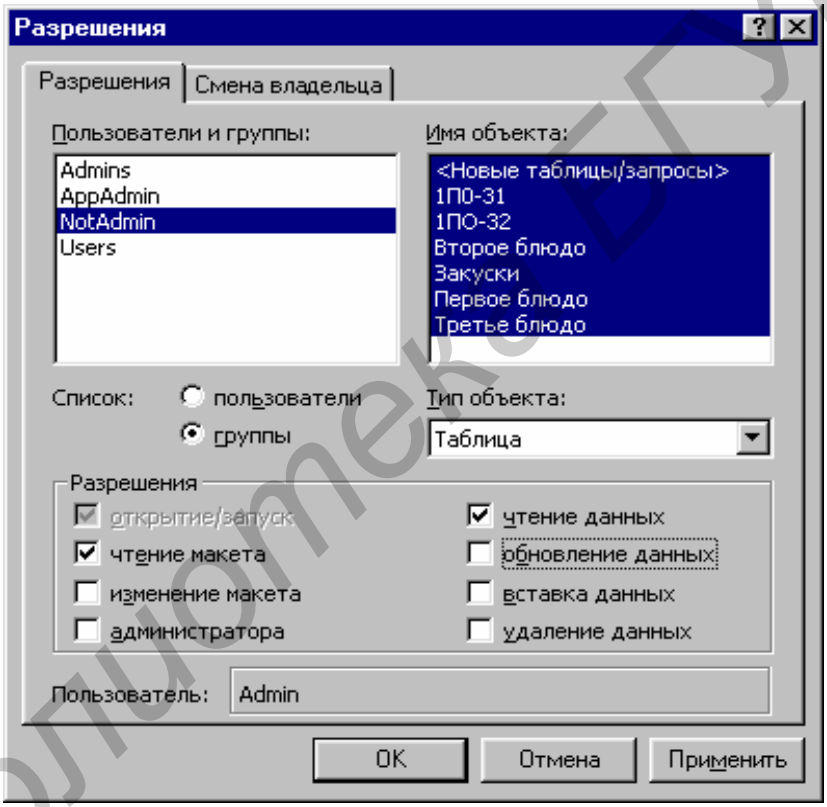

Рис.18. Назначение ограничений разрешений группе NotAdmin

Выделите одну из созданных вами групп в левом списке. Для базы данных предоставьте только разрешение **Открытие/запуск** (**Open/Run**). Для всех таблиц и запросов предоставьте разрешение **Чтение данных** (**Read Data**), а для всех форм и отчетов – разрешение **Открытие/запуск**.

5. СОДЕРЖАНИЕ ОТЧЕТА

- Краткие сведения из теории.
- Описание хода выполнения работы.
- Файл базы данных Microsoft Access.
- Отчет работы мастера защиты.
- Выводы.

ЛИТЕРАТУРА

1. Вейскас, Д. Эффективная работа с Microsoft Access 2000 / Д. Вейскас. – СПб. : Питер, 2001.

2. Робинсон, С. Microsoft Access 2000 : учебный курс / С. Робинсон. – СПб. : Питер, 2000.

3. Куртер, Дж. Microsoft Office 2000 : учебный курс / Дж. Куртер, А. Маркви. – СПб. : Питер, 2000.

Св. план 2007, поз.117

ЗАЩИТА БАЗ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ НА ПРИМЕРЕ СУБД MICROSOFT ACCESS

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к лабораторной работе
по дисциплине «Защита программного обеспечения
и баз данных в сетях телекоммуникаций»
для студентов специальностей I-45 01 03 «Сети телекоммуникаций»
и I-45 01 05 «Защита информации» всех форм обучения

Составители:
Бобов Михаил Никитич
Буй Павел Михайлович

Редактор М. В. Тезина
Корректор Е. Н. Батурчик

Подписано в печать 06.08.2007.	Формат 60x84 1/16.	Бумага офсетная.
Гарнитура «Таймс».	Печать ризографическая.	Усл. печ. л. 1,74.
Уч. изд. л. 1,7.	Тираж 100 экз.	Заказ 8.

Издатель и полиграфическое оформление: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ № 02330/0056964 от 01.04.2004. ЛП №02330/0131666 от 30.04.2004.
220013, Минск, П.Бровки,6