Тема занятия

Защита базы данных

Преподаватель: Карев Н.А.

Защита данных

Защита данных - **это комплекс мероприятий, предназначенных для обеспечения *целостности, непротиворечивости, секретности и безопасности данных.***

Целостность - **это свойство данных, которое заключается в нахождении значений данных в установленных диапазонах.**

Непротиворечивость – **это свойство данных, которое заключается в отсутствии копии данных находящихся на разных стадиях обновления.**

Безопасность - **это свойство данных, которое заключается в невозможности их физического уничтожения.**

Секретность - **это свойство данных, которое заключается в невозможности несанкционированного доступа и использования (т.е. без ведома их владельца).**

Классификация причин нарушения работы БД

Случайные **(неумышленные):**

- **сбои в работе оборудования**
- **ошибки в работе программных средств**
- **ошибки ввода/вывода**
- **действия физических полей**
- **стихийные бедствия**
- **халатность работников**

Неслучайные **(умышленные):**

- **корыстные и некорыстные**

Защита целостности и непротиворечивости

1. **Минимальная избыточность данных.**
2. **Ограничение доступа**
3. **Ограничение обработки**
4. **Ведение системного журнала**
   - **Регистрация пользователей**
   - **Регистрация действий**
5. **Копирование данных и контрольные точки**

Минимальная избыточность данных означает отсутствие или минимальное присутствие дублирования данных

Ограничение доступа:

1. На уровне пользователей
2. На уровне данных

Пользователи БД

Пользователи классифицируются по категориям, и каждая категория получает право работы с определенной областью доступа

В системе обычно имеется 4 группы пользователей:

1. ***Администраторы*** **(системные) – полные права доступа к данным**
2. ***Общая*** **(пользователи) – минимальный доступ**
3. ***Владелец*** **(собственник данных) – полное право доступа к данным**
4. ***Группа*** **- т.е. часть пользователей, которым владелец передал часть прав.**

Ограничение доступа на уровне пользователей

При входе выделяют две процедуры:

1. Процедура идентификации - проверка имени пользователя.

2. Процедура верификации - проверка пароля, т.е. правильности ввода имени.

Ограничение доступа на уровне данных

Данные подразделяются на следующие категории:

1. **системные (прозрачные или невидимые) - никто не должен иметь к ним доступ;**

2. **пользовательские.**

Ограничение обработки на уровне пользователей

Ограничения, как правило, устанавливаются на следующие виды действий:

- **администрирование (как правило, изменение структуры);**
- **чтение (просмотр);**
- **запись;**
- **модификация (изменение);**
- **удаление;**
- **добавление;**
- **передача прав.**

Ведение системного журнала

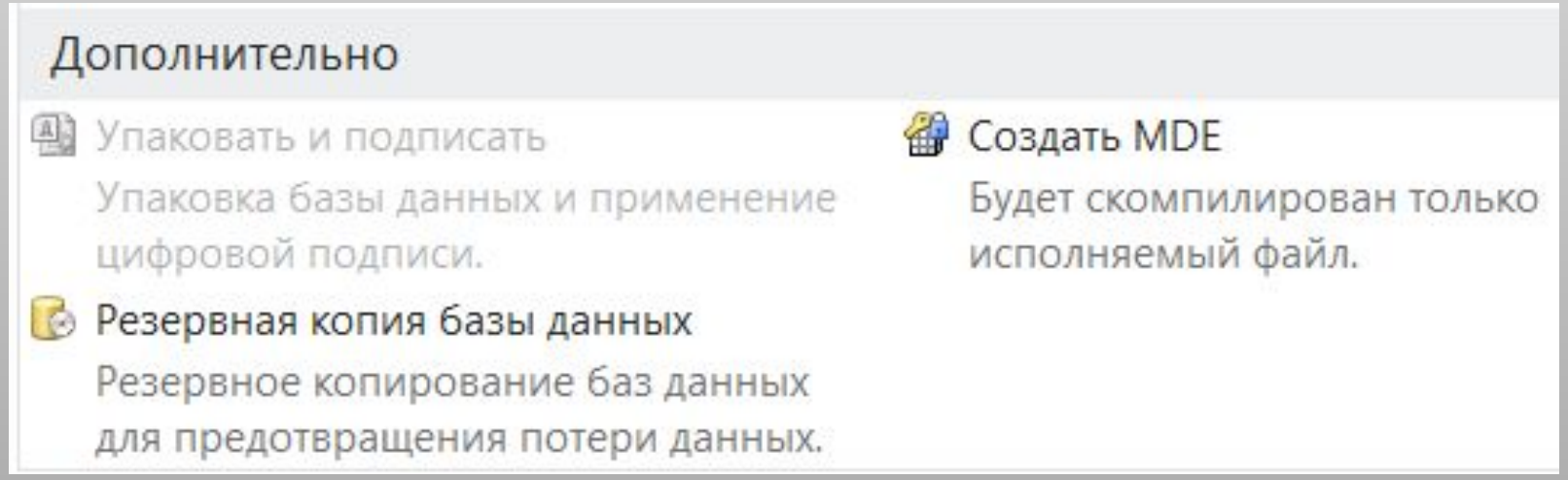
Ведение системного журнала предполагает:

1. Регистрацию каждого входа пользователя

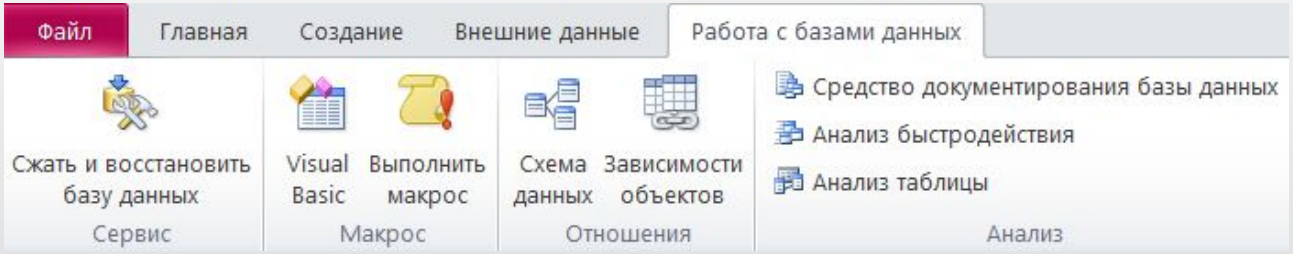
2. Регистрация всех действий, которые совершил пользователь

Архивирование, сжатие и восстановление баз данных

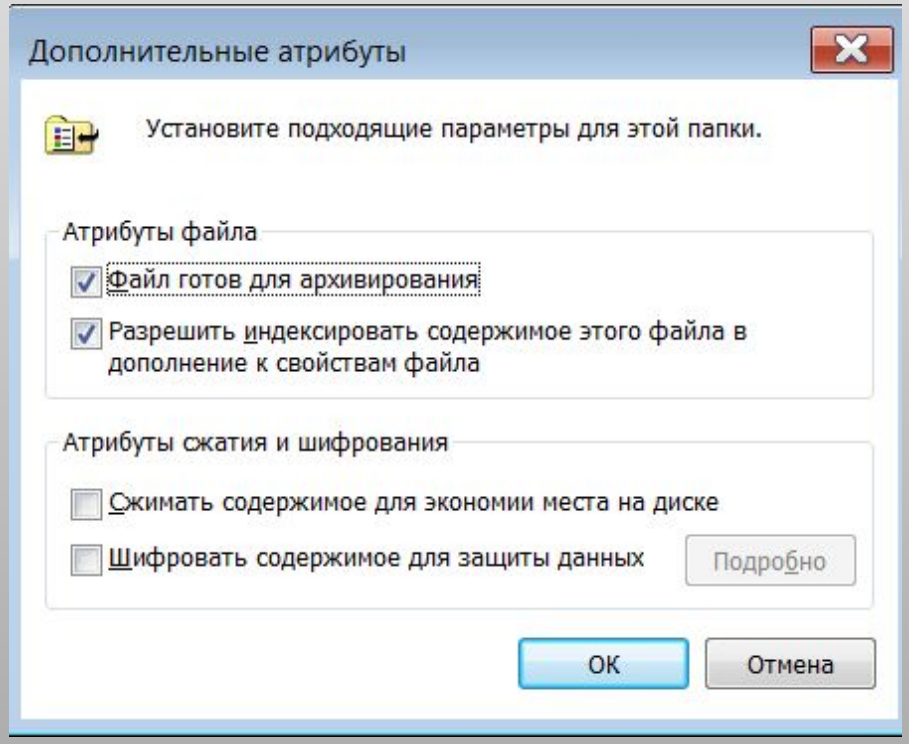
1. При наличии достаточного объёма свободного места на диске можно создать резервную копию обычным копированием файла или используя средства Access



2. Для сжатия можно использовать средства MS Access



или дополнительные атрибуты файла



Защита информации с помощью шифрования

Защита информации в базе данных может производится с помощью операции шифрования.

Операция шифрования в Access приводит к кодированию файла базы данных.

После выполнения операции шифрования просмотр данных становится невозможен.

Операция дешифрования отменяет результаты операции шифрования.

Операция шифрования или дешифрования неприменима к открытой базе данных.

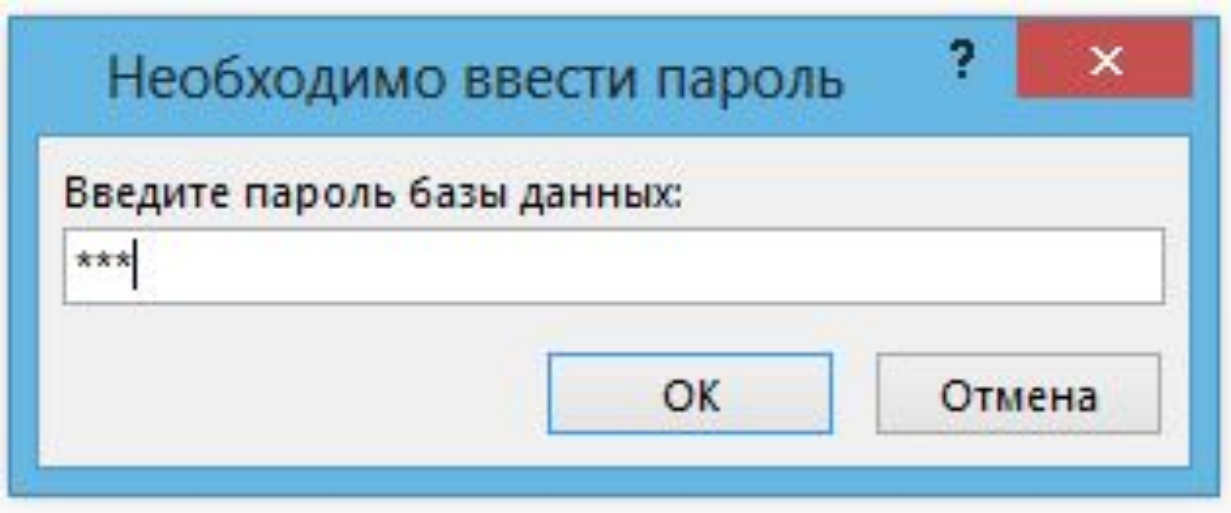
Защита БД от несанкционированного доступа

Существует несколько способов защиты базы данных Access от несанкционированного доступа:

1. **База данных может быть защищена паролём;**
2. **Для базы данных Access может быть установлена система защиты на уровне пользователей;**
3. **База данных может быть скомпилирована в исполнительный файл (расширение** .mde **или** .accde**).**

Защита базы данных Access с помощью пароля

Самый простой способ защиты базы данных — с помощью пароля. Можно назначить пароль базе данных Access, который будет требоваться всякий раз при её открытии.



Домашнее задание

Найти и выписать в тетрадь законы РФ, которые регламентируют работу с информацией и защищают её.

Сделать вывод:
Какое наказание (административное и уголовное) за создание вредоносных программ существует в РФ.

Установка и снятие пароля защиты базы данных

Чтобы установить пароль для защиты базы данных:

1. **Закройте базу данных. Если база данных совместно используется в сети, убедитесь, что остальные пользователи её закрыли.**
2. **Сделайте резервную копию базы данных и сохраните её в надёжном месте.**
3. **В меню Access выберите команду Файл, Открыть.**
4. **Выделите файл базы данных.**
5. **Щелкните по стрелке, расположенной справа от кнопки Открыть. В раскрывающемся списке режимов открытия базы данных выделите элемент Монопольно. База данных откроется в режиме монопольного доступа.**
6. **Выберите команду Файл – Сведения – Зашифровать паролм.**
7. **В появившемся диалоговом окне введите в поле Пароль пароль для защиты базы данных с учетом регистра символов.**
8. **Введите пароль ещё раз в поле Подтверждение.**
9. **Нажмите кнопку ОК.**