

Муниципальное общеобразовательное учреждение «Новгородская
средняя общеобразовательная школа им. В.Н. Лесина»

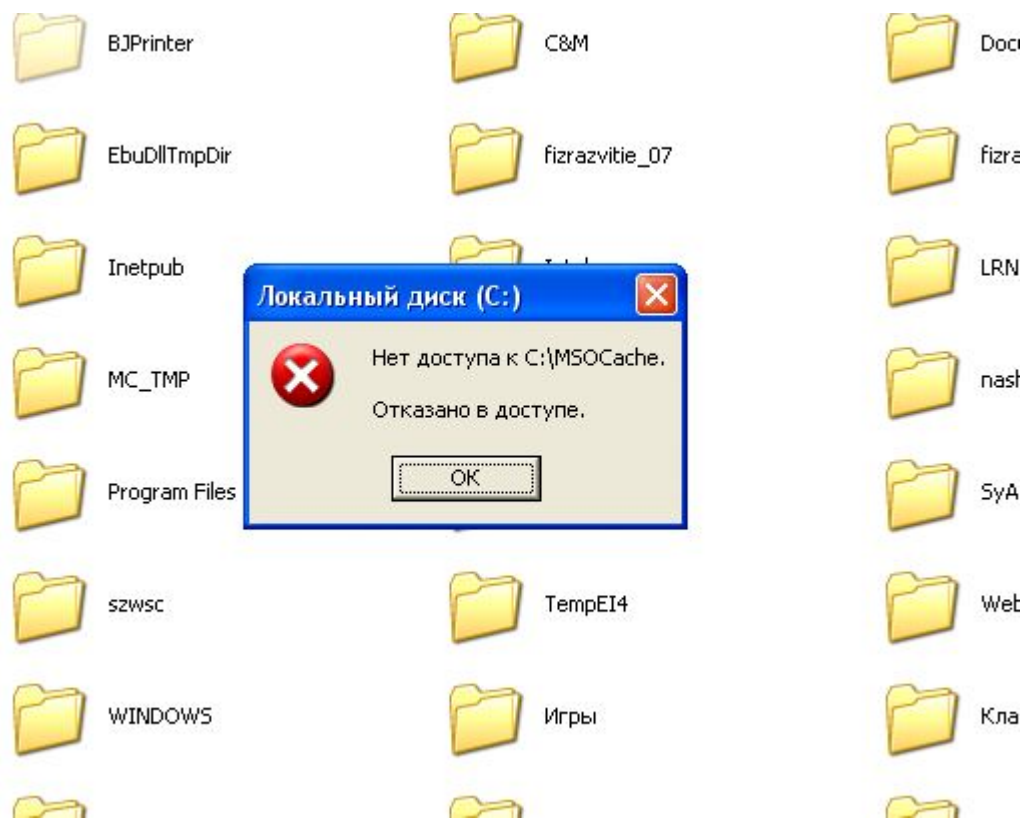
Меры по обеспечению безопасности на прикладном уровне

учитель технологии и физкультуры

I категории

Середин Е.Н.

ОС может запретить пользователю во время работы изменять или даже находить некоторые системные файлы



2 способа разграничения прав доступа

```
graph TD; A[2 способа разграничения прав доступа] --> B[на основе каких-либо данных, известных только уполномоченным на такой доступ (например, пароля)]; A --> C[доступ на основе учетных записей];
```

на основе каких-либо
данных, известных
только уполномоченным
на такой доступ
(например, пароля)

доступ на основе учетных
записей

Аутентификация

— установление соответствия между пользователем и его учетной записью



«ЛОГИН» — от англ. «log in» —
«отметить начало»

подтвердить паролем

Методы двухфакторной аутентификации

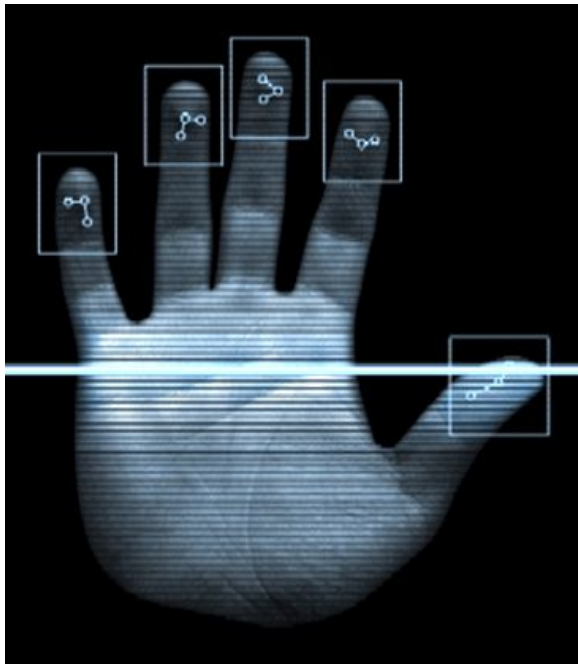
Логин + пароль + носитель



магнитная карта, смарт-карта, USB-ключ

Биометрическая идентификация

доступ предоставляется на основе анализа
некоторых биологических показателей,
уникальных для каждого человека
(отпечатка его пальцев или рисунка сосудов сетчатки



ГЛ



Авторизация

— проверка, имеет ли этот пользователь право выполнять такую операцию

Пароль

по-прежнему наиболее часто
используемое средство для выполнения
аутентификации

Подбор пароля

руководствуясь имеющимися сведениями,
злоумышленник начинает перебирать все
возможные варианты строк на соответствие
паролю

Меры защиты

- никогда и нигде *не разглашать пароль*
- Не следует использовать простые пароли
- Нельзя использовать предсказуемые пароли
- Нежелательно использовать в качестве пароля какие-либо осмысленные слова.
- Время от времени пароли нужно менять
- Использовать системы, которые ограничивают число попыток неправильного набора пароля за определенный промежуток времени
- Не желательно сохранять пароль на локальной машине и/или вообще передавать его через сеть, в которой вы работаете.

Генераторы паролей

— программы, которые порождают случайные пароли заданной длины.



Учетные записи пользователей

Учетные записи пользователей

Назад Домой

Обучение

- Учетные записи
- Типы учетных записей пользователей
- Переключение пользователей

Учетные записи пользователей

Выберите задание...

- Изменение учетной записи
- Создание учетной записи
- Изменение входа пользователей в систему

или выберите изменяемую учетную запись

учитель
Администратор компьютера
Защита паролен

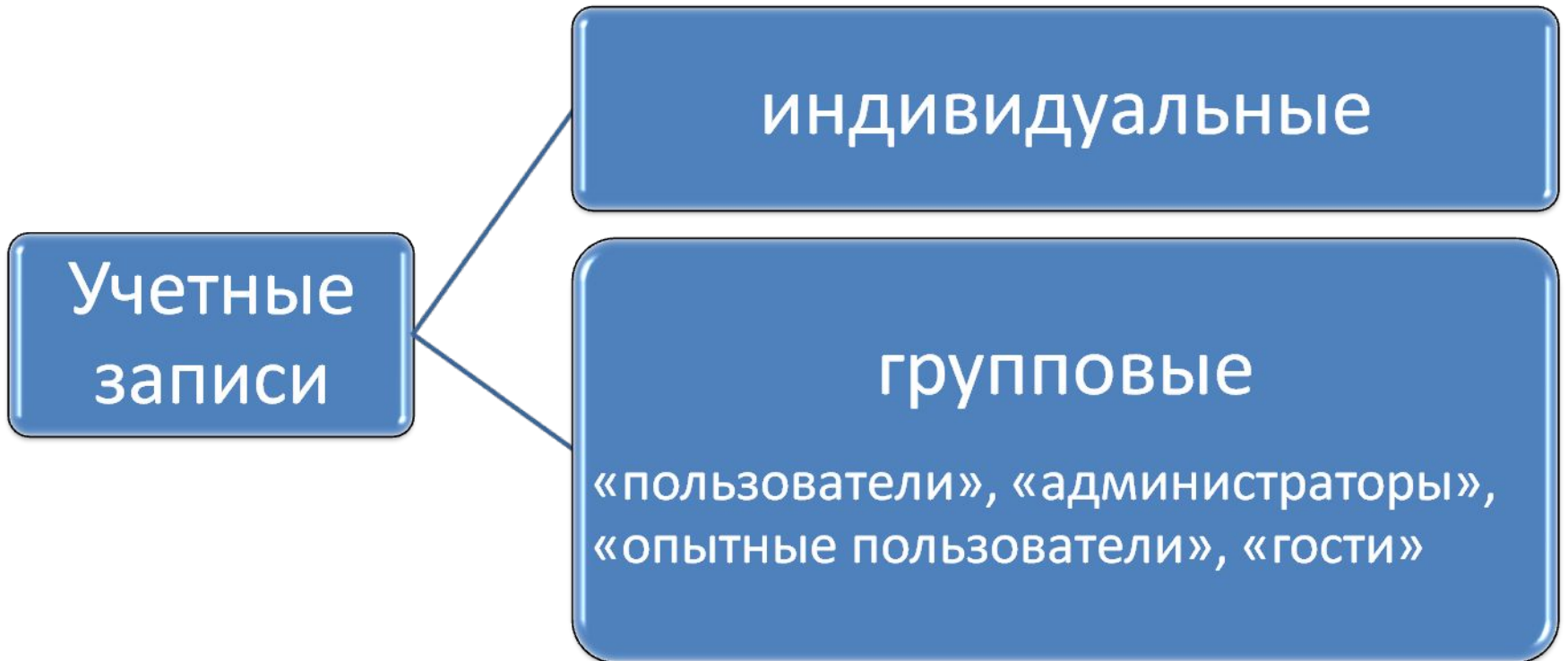
ученик
Ограниченная учетная запись

Гость
Учетная запись гостя
отключена

Изменение учетной записи

Создание учетной записи

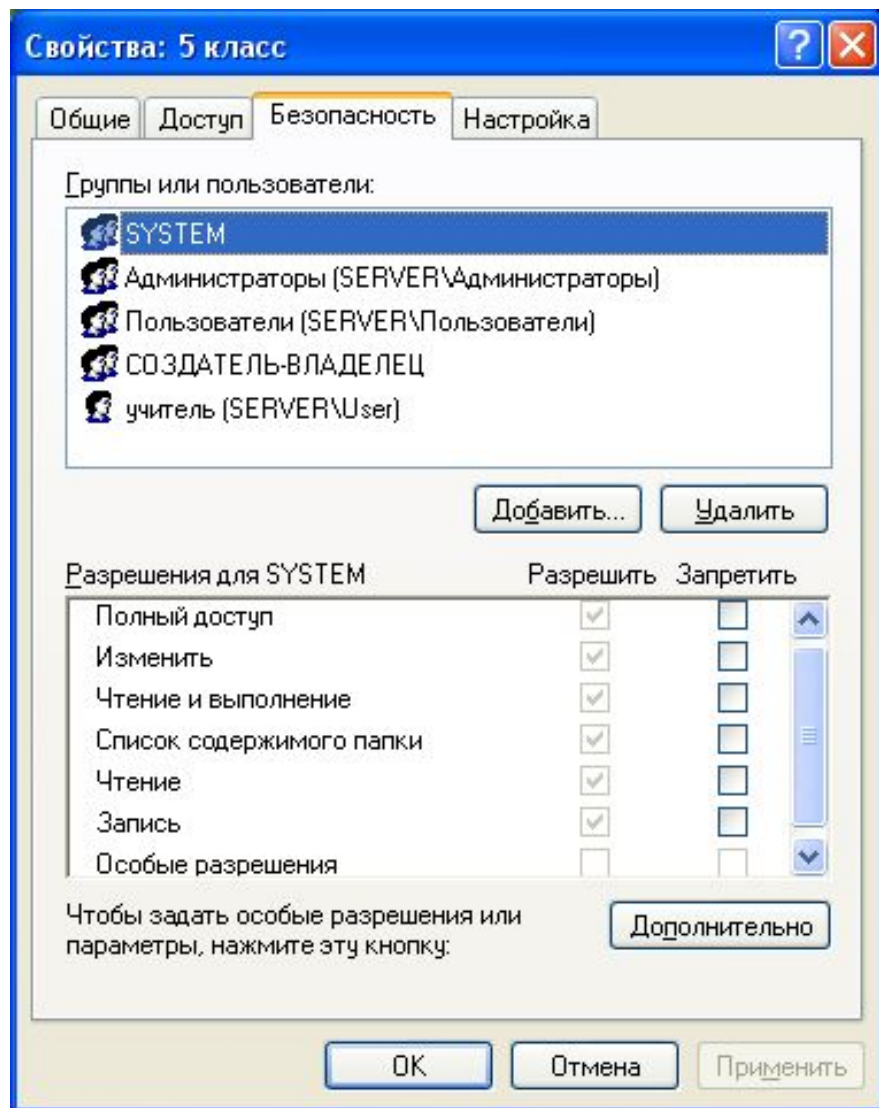
Изменение входа пользователей в систему



Основные положения:

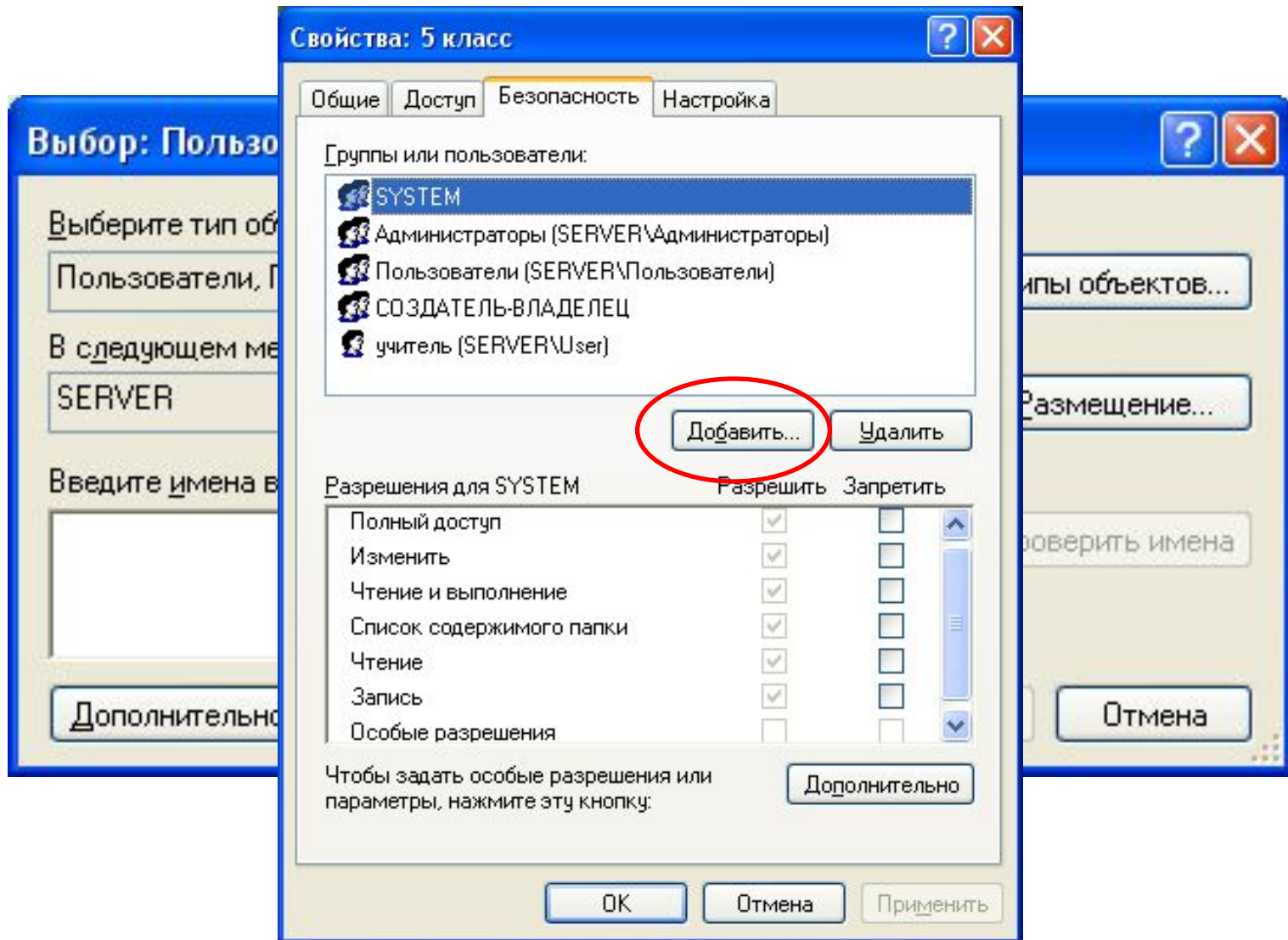
- работа пользователя с ОС начинается с процедуры аутентификации;
- ОС создает *маркер безопасности сеанса*;
- каждый объект или операция сопровождаются *списком доступа*;
- при попытке выполнения того или иного действия система безопасности проверяет:
 - а) нет ли в списке доступа идентификаторов, которым эта операция запрещена? Если есть, то в доступе будет отказано;
 - б) есть ли в списке идентификаторы, которым это действие разрешено? Если есть, ОС разрешает выполнить операцию.

Управление списками (на примере файлов)



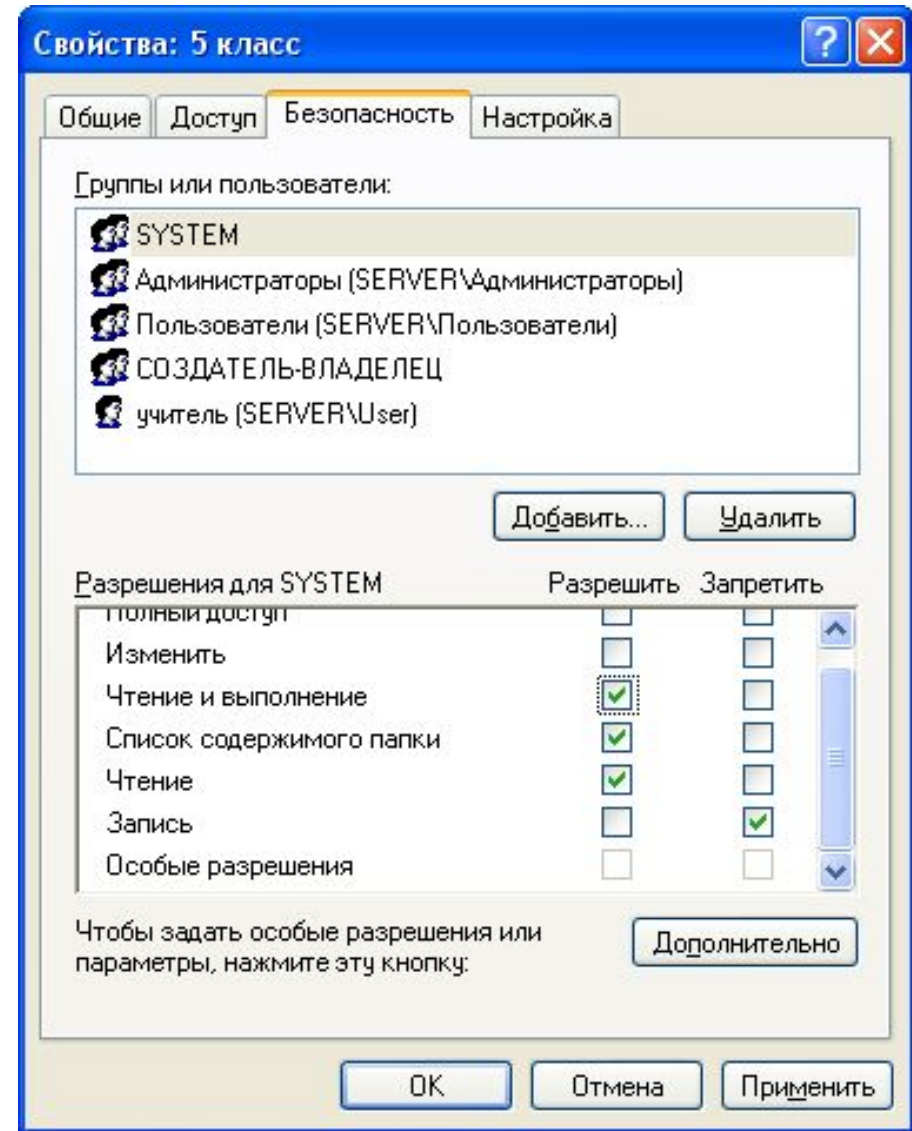
Вызвать список контроля доступа к файловому объекту можно из контекстного меню в разделе **Свойства** на вкладке **Безопасность**.

Для добавления к списку новой учетной записи нужно щелкнуть мышью на кнопке **Добавить...**



Значение пунктов списка :

- Чтение;
- Запись;
- Список содержимого;
- Чтение и выполнение;
- Изменить;
- Полный доступ;
- Особые разрешения.



**Спасибо за
внимание**