Отчет по лаборатной работе №2

по предмету Информационная безопасность

Алхимова Дарья Сергеевна

Содержание

[Цель работы 1](#__RefHeading___Toc5323_550107995)

[Задание 1](#__RefHeading___Toc5325_550107995)

[Теоретическое введение 2](#__RefHeading___Toc5327_550107995)

[Выполнение лабораторной работы 3](#__RefHeading___Toc5329_550107995)

[Выводы 20](#__RefHeading___Toc5331_550107995)

[Список литературы 20](#__RefHeading___Toc5333_550107995)

# Цель работы

Целью данной работы является получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

# Задание

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (использую учётную запись администратора): useradd guest.
2. Задайте пароль для пользователя guest (использую учётную запись администратора): passwd guest.
3. Войдите в систему от имени пользователя guest.
4. Определите директорию, в которой вы находитесь, командой pwd. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию.
5. Уточните имя вашего пользователя командой whoami.
6. Уточните имя вашего пользователя, его группу, а так же группы, куда входит пользователь, командой id. Выведенные значения uid, gid и др. за- помните. Сравните вывод id с выводом команды groups.
7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.
8. Просмотрите файл /etc/passwd командой cat /etc/passwd Найдите в нём свою учётную запись. Определите uid пользователя. Определите gid пользователя. Сравните найденные значения с полученными в предыдущих пунктах. Замечание: в случае, когда вывод команды не умещается на одном экране монитора, используйте прокрутку вверх–вниз (удерживая клави- шу shift, нажимайте page up и page down) либо программу grep в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: cat /etc/passwd | grep guest.
9. Определите существующие в системе директории командой ls -l /home/. Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях?
10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home. Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей?
11. Создайте в домашней директории поддиректорию dir1 командой mkdir dir1. Определите командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.
12. Снимите с директории dir1 все атрибуты командой chmod 000 dir1 и проверьте с её помощью правильность выполнения команды ls -l.
13. Попытайтесь создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1 Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой ls -l /home/guest/dir1, действительно ли файл file1 не находится внутри директории dir1.
14. Заполните таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».
15. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 2.2.

# Теоретическое введение

Для всех файлов и директорий Linux устанавливаются следующие права доступа:

* разрешение чтение содержимого файла;
* разрешение на изменение (запись) содержимого файла;
* разрешение на исполнение файла.

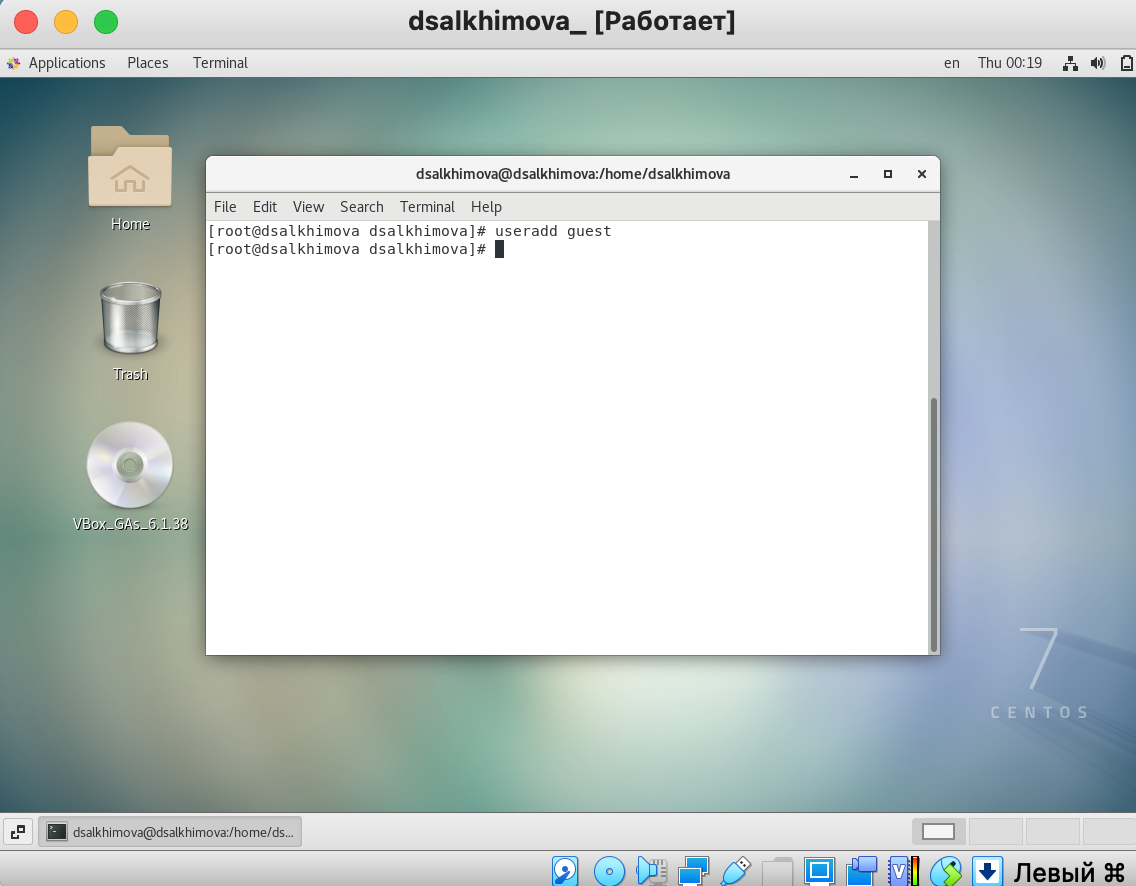
В свойствах каждого файла и директории эти три разрешения устанавливаются отдельно для:

* владельца файла
* группы владельцев файла, которой принадлежит этот файл
* всех остальных.

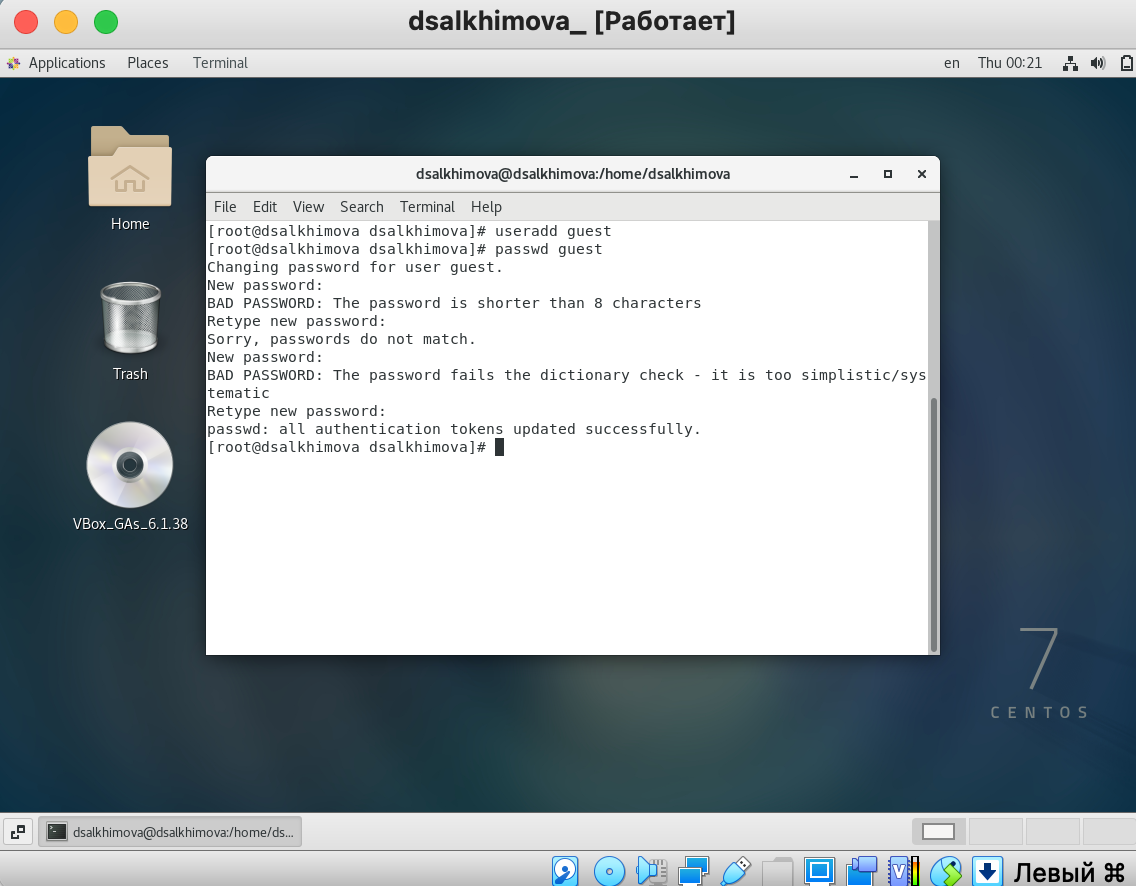
Просмотреть права доступа, а также владельца и группу, к которой относится файл, можно командой ls с опцией -l. Чтобы изменить режим (права доступа) файла или каталога, используется команда chmod с параметрами. Три цифры соответствуют трём параметрам режима доступа: чтение, запись, выполнение. Поэтому права доступа можно представить в виде трёх двоичных цифр, которые можно записать как одну восьмеричную цифру. Используя три восьмеричных цифры, мы можем установить режим файла для владельца, группы владельцев и всех остальных. Хотя запоминание восьмеричного бинарного отображения может показаться неудобным, обычно нужно использовать только несколько часто используемых: 7 (rwx), 6 (rw-), 5 (r-x), 4 (r–) и 0 (—). Либо можно запомнить значение одиночных прав доступа и складывать их значения для получения любых комбинаций: 4 (r–), 2 (-w-), 1 (–x). После можно получить любую комбинацию, для прав чтения и записи это 6 (4+2) (rw-), для прав записи и выполнения это 3 (2+1) (-wx), для прав чтения и выполнения это 5 (4+1) (r-x)

# Выполнение лабораторной работы

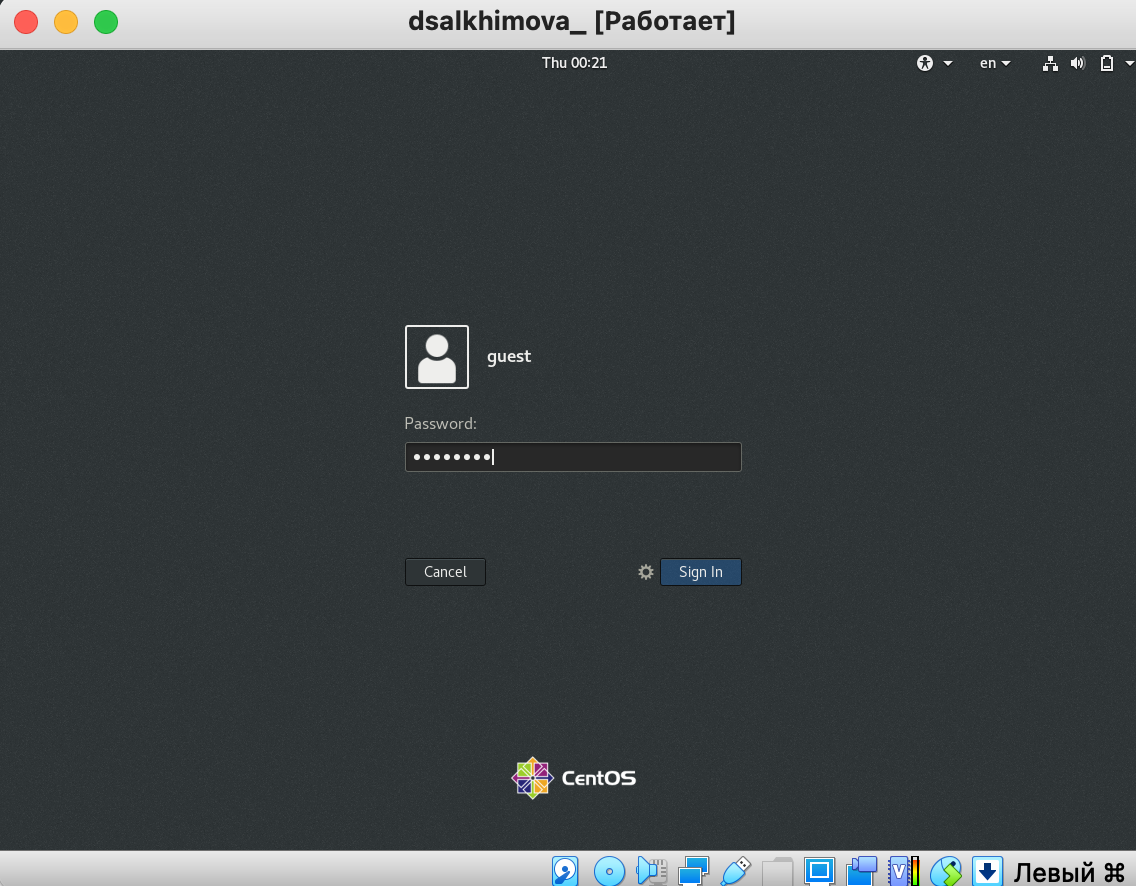
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайла учётную запись пользователя guest (использую учётную запись администратора):  
   useradd guest ([рис. 1](images2/1.png))

* 
* Создание пользователя

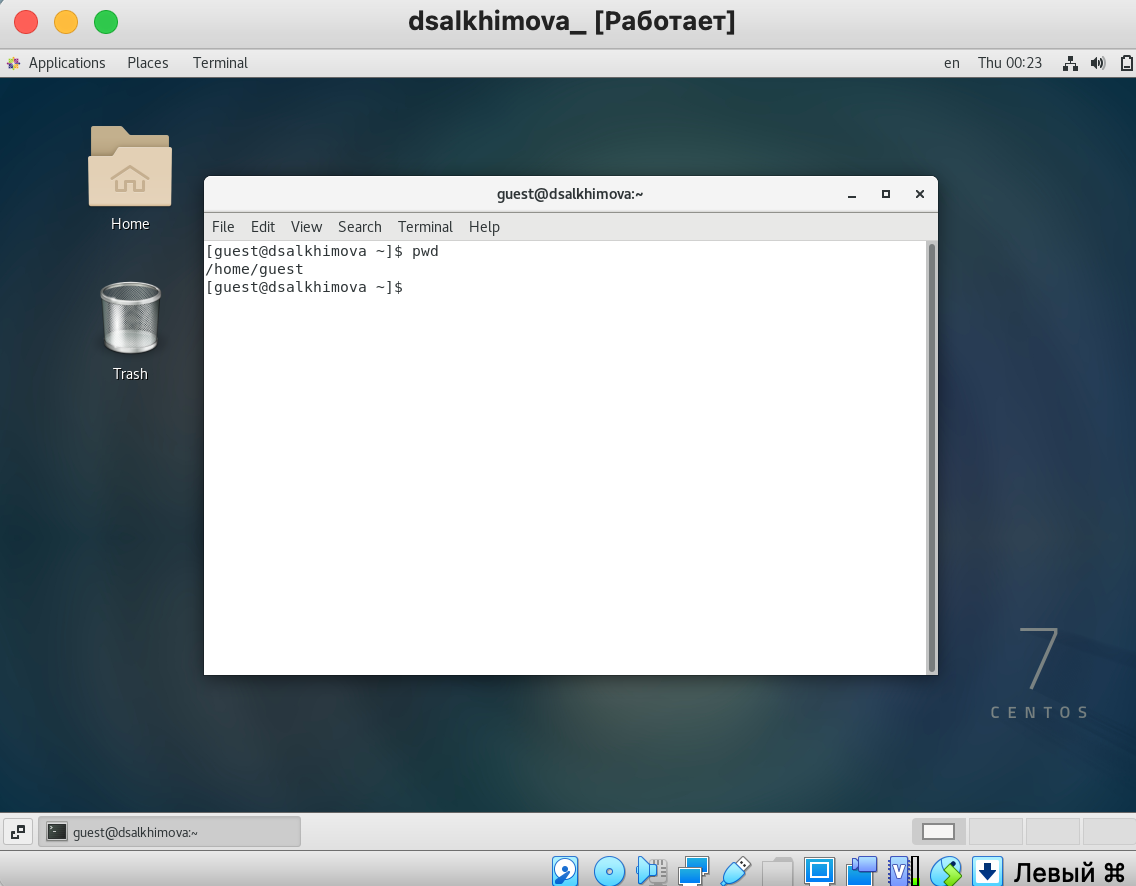
1. Задала пароль для пользователя guest (использую учётную запись администратора): passwd guest ([рис. 2](images2/2.png))

* 
* Установка пароля для пользователя

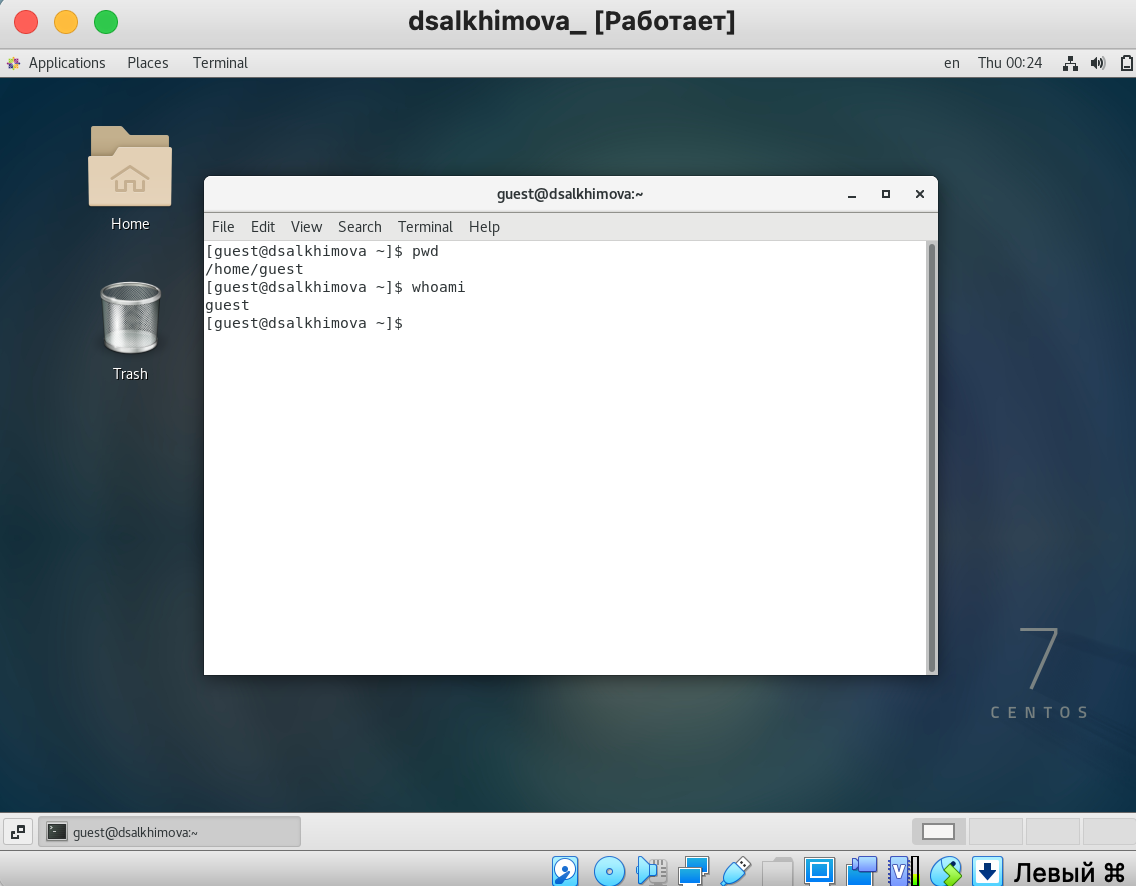
1. Вошла в систему от имени пользователя guest. ([рис. 3](images2/3.png))

* 
* Авторизация под новым пользователем

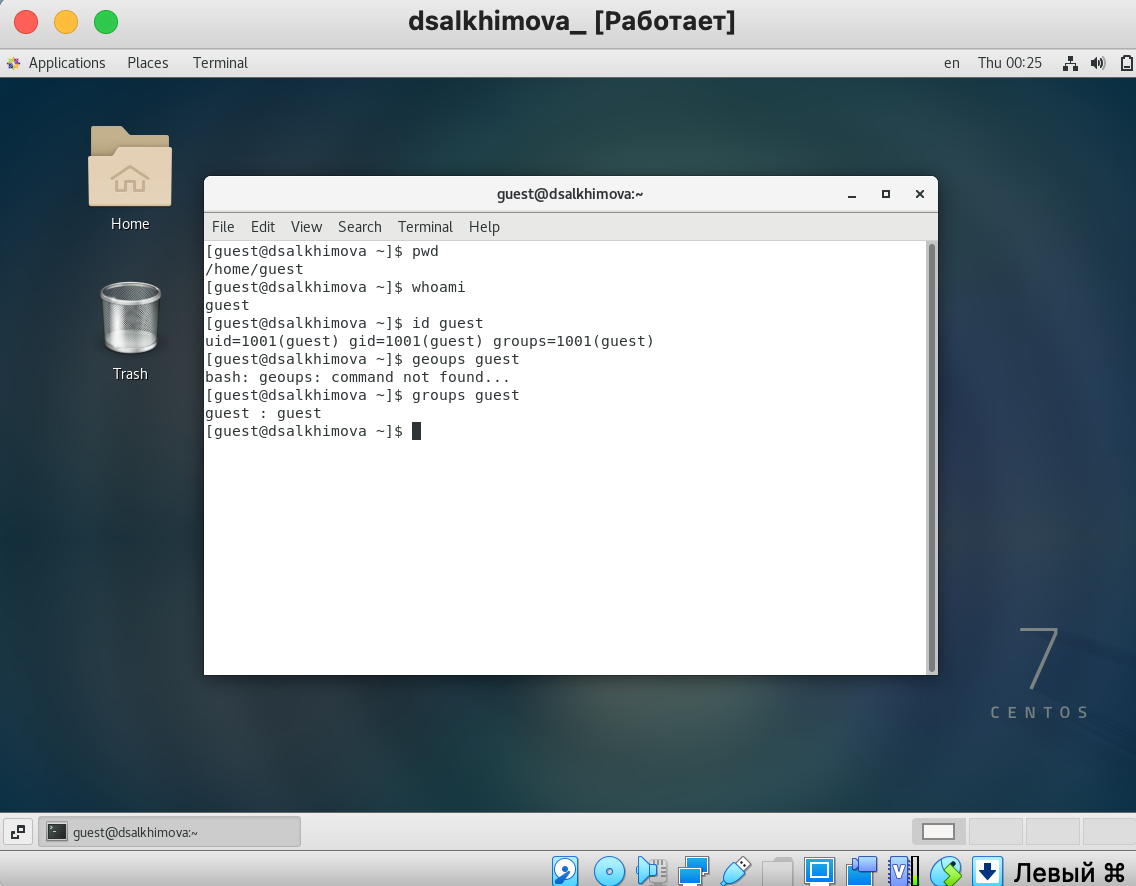
1. Определила директорию,в которой я нахожусь, командой pwd. Данная директория является моей домашней директорией. ([рис. 4](images2/4.png))

* 
* Проверка текущей директории

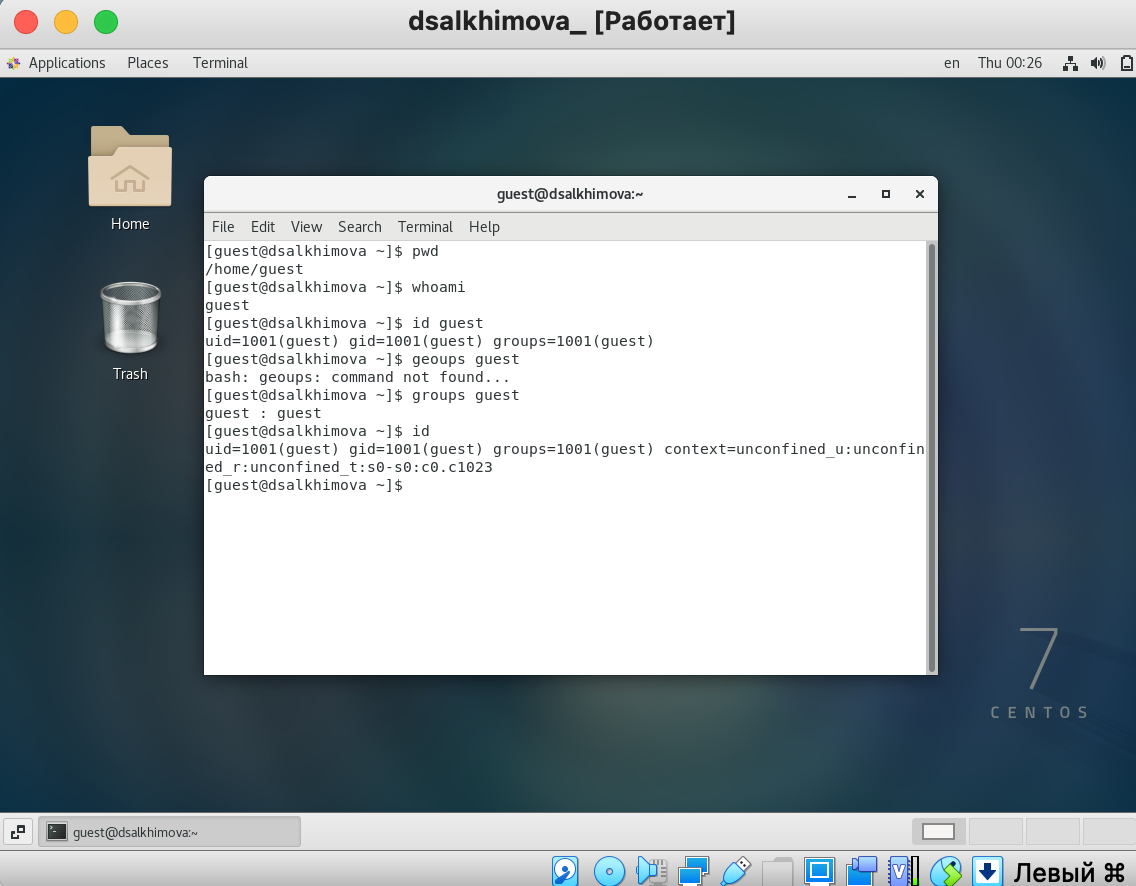
1. Уточнила имя моего пользователя командой whoami. ([рис. 5](images2/5.png))

* 
* Имя пользователя

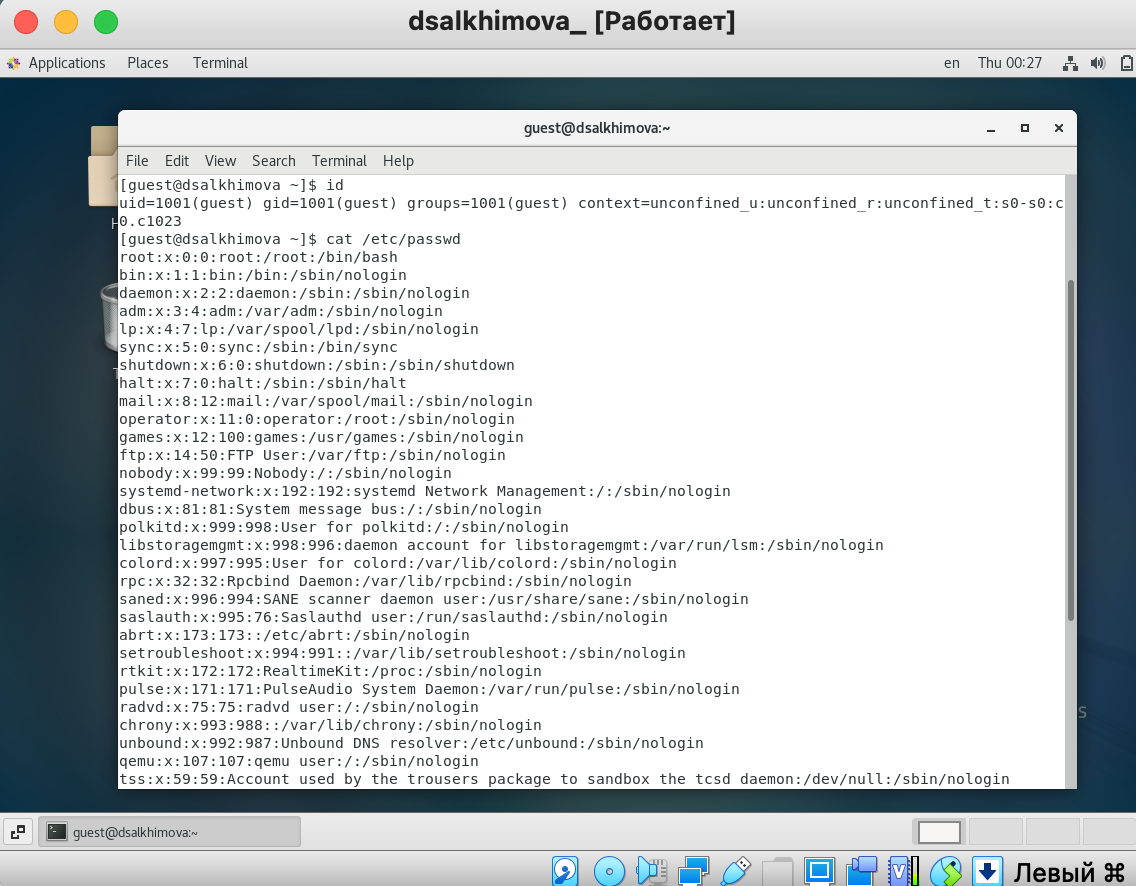
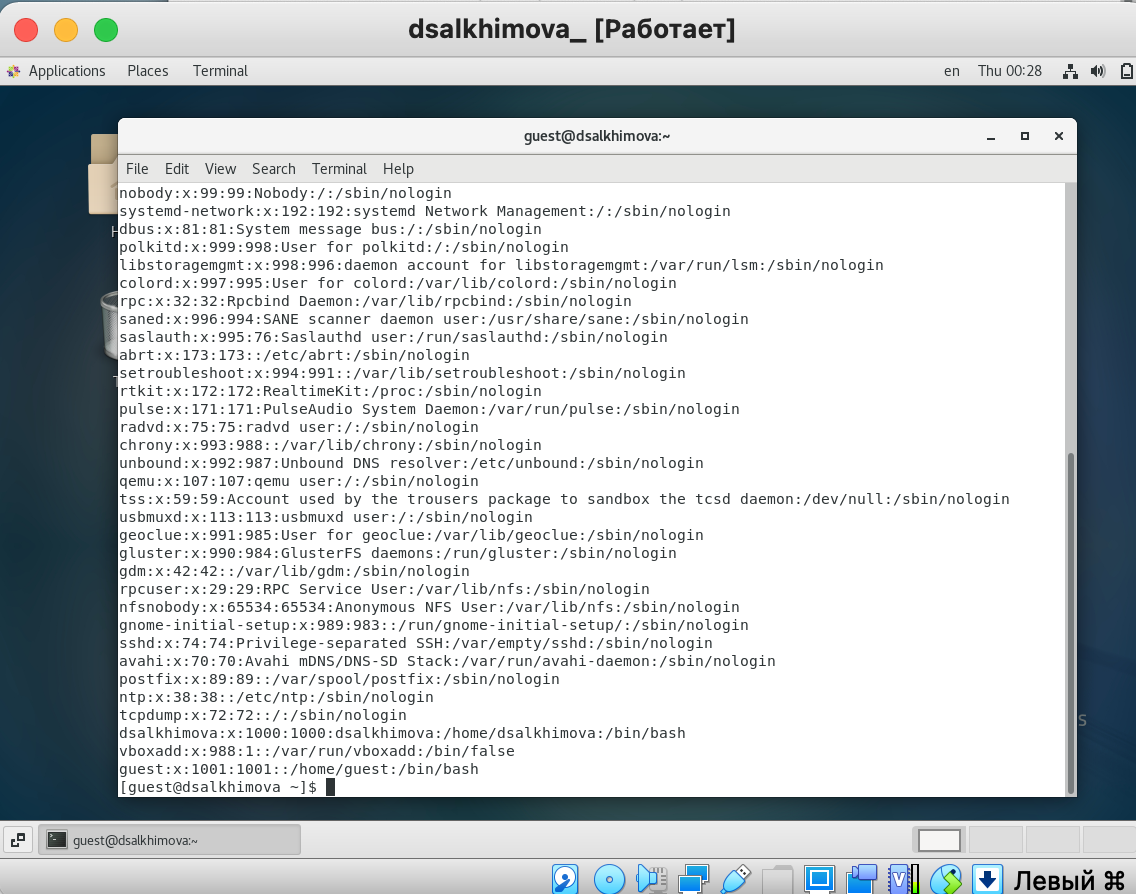
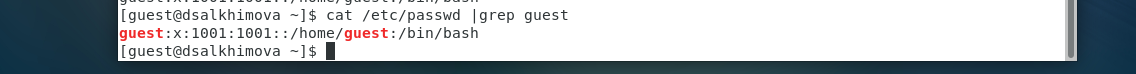
1. Уточнила имя моего пользователя, его группу, а так же группы, куда входит пользователь, командой id. Вывод id содержит больше информации, чем вывод команды groups. ([рис. 6](images2/6.png))

* 
* Информация о пользователей командой id

1. Сравнила полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. ([рис. 7](images7/7.png))

* 
* Сравнение id и приглашения командной строки

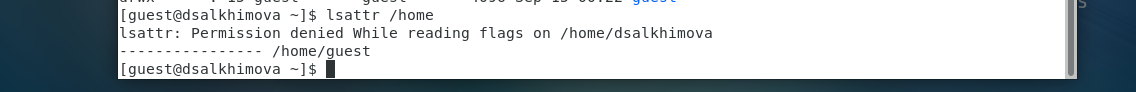
1. Просмотрела файл /etc/passwd командой cat /etc/passwd. Нашла в нём свою учётную запись. Определила uid и gidпользователя: 1001(guest). Найденные значения совпадают с полученными в предыдущих пунктах. ([рис. 8](images2/8.png), [рис. 9](images2/9.png))

* 
* Файл passwd 1/2
* 
* Файл passwd 2/2
* Использовала программу grep в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: cat /etc/passwd | grep guest. ([рис. 10](images2/10.png))
* 
* Файл passwd 2/2

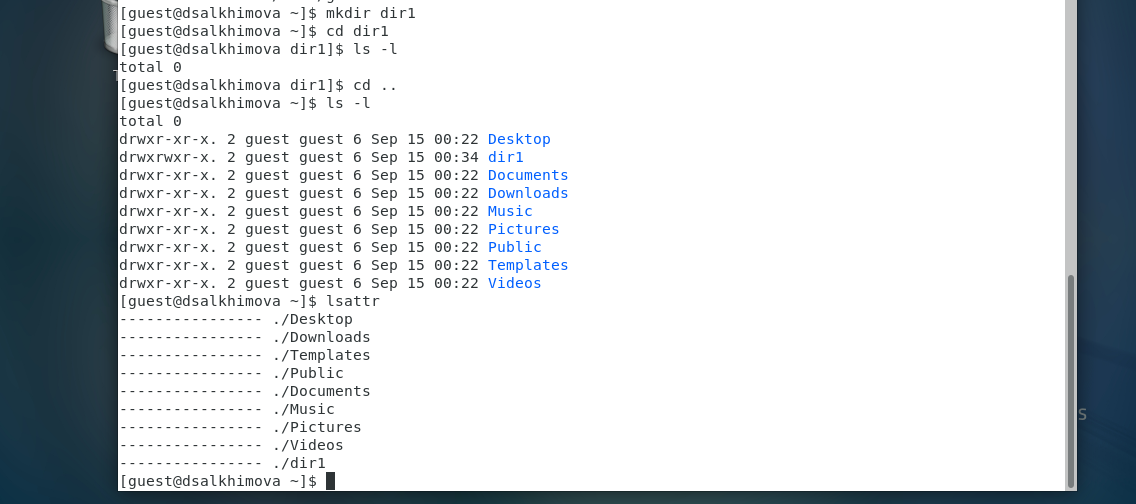
1. Определила существующие в системе директории командой ls -l /home/.  
   Получить список поддиректорий директории /home не удалось, вывело только общее количество. На директориях установлены права на чтение, запись и исполнение есть только для владельцев([рис. 11](images2/11.png))

* 
* Определение существующих директорий

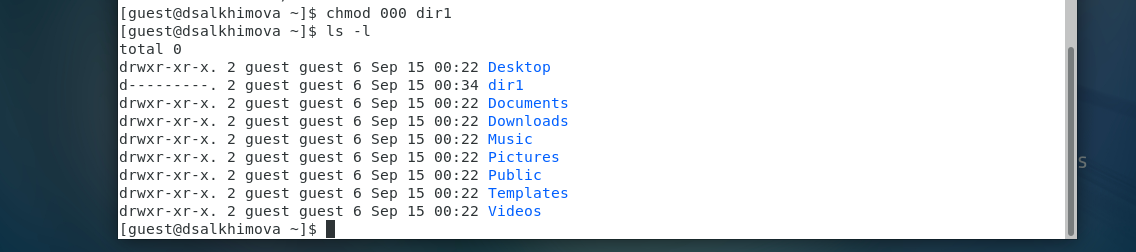
1. Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой lsattr /home.  
   Доступ к расширенным атрибутам директории, а также директорий других пользователей был запрещен. ([рис. 12](images2/12.png))

* 
* Расширенные артибуты директорий

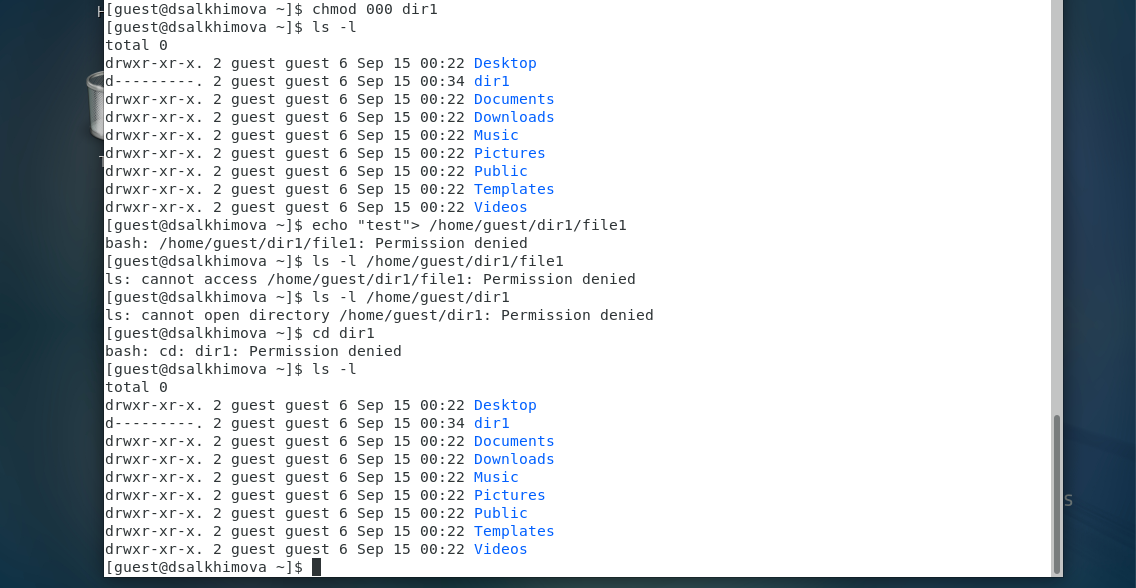
1. Создала в домашней директории поддиректорию dir1 командой mkdir dir1.  
   Определила командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1. ([рис. 13](images2/14.png))

* 
* Создание поддиректории

1. Сняла с директории dir1 все атрибуты командой chmod 000 dir1 и проверила с её помощью правильность выполнения команды ls -l. Права стали удалены у всех пользователей. ([рис. 14](images2/15.png))

* 
* Снятие атрибутов директории

1. Попыталась создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1 и получила отказ в выполнении операции по созданию файла, поскольку на предыдущем шаге я убрала все права с директории dir1. Файл не был создан. ([рис. 15](images2/16.png))

* 
* Создание файла в директории
* Проверила командой ls -l /home/guest/dir1, что файл file1 действительно не находится внутри директории dir1. ([рис. 16](images2/17.png))
* 
* Создание файла в директории

1. Заполнила таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-». [-@tbl:attr]

| Права директории | Права файла | Соз- дание файла | Уда- ление файла | Запись в файл | Чтение файла | Смена дирек- тории | Просмотр файлов в директории | Пере- имено- вание файла | Смена атри- бутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d---------(000) | ----------(000) | - | - | - | - | - | - | - | - |
| d--x------(100) | ----------(000) | - | - | - | - | + | - | - | + |
| d-w-------(200) | ----------(000) | - | - | - | - | - | - | - | - |
| d-wx------(300) | ----------(000) | + | + | - | - | + | - | + | + |
| dr--------(400) | ----------(000) | - | - | - | - | - | - | - | - |
| dr-x------(500) | ----------(000) | - | - | - | - | + | + | - | + |
| drw-------(600) | ----------(000) | - | - | - | - | - | - | - | - |
| drwx------(700) | ----------(000) | + | + | - | - | + | + | + | + |
| d---------(000) | ---x------(100) | - | - | - | - | - | - | - | - |
| d--x------(100) | ---x------(100) | - | - | - | - | + | - | - | + |
| d-w-------(200) | ---x------(100) | - | - | - | - | - | - | - | - |
| d-wx------(300) | ---x------(100) | + | + | - | - | + | - | + | + |
| dr--------(400) | ---x------(100) | - | - | - | - | - | - | - | - |
| dr-x------(500) | ---x------(100) | - | - | - | - | + | + | - | + |
| drw-------(600) | ---x------(100) | - | - | - | - | - | - | - | - |
| drwx------(700) | ---x------(100) | + | + | - | - | + | + | + | + |
| d---------(000) | --w-------(200) | - | - | - | - | - | - | - | - |
| d--x------(100) | --w-------(200) | - | - | + | - | + | - | - | + |
| d-w-------(200) | --w-------(200) | - | - | - | - | - | - | - | - |
| d-wx------(300) | --w-------(200) | + | + | + | - | + | - | + | + |
| dr--------(400) | --w-------(200) | - | - | - | - | - | - | - | - |
| dr-x------(500) | --w-------(200) | - | - | + | - | + | + | - | + |
| drw-------(600) | --w-------(200) | - | - | - | - | - | - | - | - |
| drwx------(700) | --w-------(200) | + | + | + | - | + | + | + | + |
| d---------(000) | --wx------(300) | - | - | - | - | - | - | - | - |
| d--x------(100) | --wx------(300) | - | - | + | - | + | - | - | + |
| d-w-------(200) | --wx------(300) | - | - | - | - | - | - | - | - |
| d-wx------(300) | --wx------(300) | + | + | + | - | + | - | + | + |
| dr--------(400) | --wx------(300) | - | - | - | - | - | - | - | - |
| dr-x------(500) | --wx------(300) | - | - | + | - | + | + | - | + |
| drw-------(600) | --wx------(300) | - | - | - | - | - | - | - | - |
| drwx------(700) | --wx------(300) | + | + | + | - | + | + | + | + |
| d---------(000) | -r--------(400) | - | - | - | - | - | - | - | - |
| d--x------(100) | -r--------(400) | - | - | - | + | + | - | - | + |
| d-w-------(200) | -r--------(400) | - | - | - | - | - | - | - | - |
| d-wx------(300) | -r--------(400) | + | + | - | + | + | - | + | + |
| dr--------(400) | -r--------(400) | - | - | - | - | - | - | - | - |
| dr-x------(500) | -r--------(400) | - | - | - | + | + | + | - | + |
| drw-------(600) | -r--------(400) | - | - | - | - | - | - | - | - |
| drwx------(700) | -r--------(400) | + | + | - | + | + | + | + | + |
| d---------(000) | -r-x------(500) | - | - | - | - | - | - | - | - |
| d--x------(100) | -r-x------(500) | - | - | - | + | + | - | - | + |
| d-w-------(200) | -r-x------(500) | - | - | - | - | - | - | - | - |
| d-wx------(300) | -r-x------(500) | + | + | - | + | + | - | + | + |
| dr--------(400) | -r-x------(500) | - | - | - | - | - | - | - | - |
| dr-x------(500) | -r-x------(500) | - | - | - | + | + | + | - | + |
| drw-------(600) | -r-x------(500) | - | - | - | - | - | - | - | - |
| drwx------(700) | -r-x------(500) | + | + | - | + | + | + | + | + |
| d---------(000) | -rw-------(600) | - | - | - | - | - | - | - | - |
| d--x------(100) | -rw-------(600) | - | - | + | + | + | - | - | + |
| d-w-------(200) | -rw-------(600) | - | - | - | - | - | - | - | - |
| d-wx------(300) | -rw-------(600) | + | + | + | + | + | - | + | + |
| dr--------(400) | -rw-------(600) | - | - | - | - | - | - | - | - |
| dr-x------(500) | -rw-------(600) | - | - | + | + | + | + | - | + |
| drw-------(600) | -rw-------(600) | - | - | - | - | - | - | - | - |
| drwx------(700) | -rw-------(600) | + | + | + | + | + | + | + | + |
| d---------(000) | -rwx------(700) | - | - | - | - | - | - | - | - |
| d--x------(100) | -rwx------(700) | - | - | + | + | + | - | - | + |
| d-w-------(200) | -rwx------(700) | - | - | - | - | - | - | - | - |
| d-wx------(300) | -rwx------(700) | + | + | + | + | + | - | + | + |
| dr--------(400) | -rwx------(700) | - | - | - | - | - | - | - | - |
| dr-x------(500) | -rwx------(700) | - | - | + | + | + | + | - | + |
| drw-------(600) | -rwx------(700) | - | - | - | - | - | - | - | - |
| drwx------(700) | -rwx------(700) | + | + | + | + | + | + | + | + |

1. На основании заполненной таблицы определила минимально необходимые права для выполнения операций внутри директории dir1 и занесла данные в табл.2[#tbl:min].

| * Операция | * Мин. права на директорию | * Мин. права на файл |
| --- | --- | --- |
| * Создание файла | * d-wx------ (300) | * ---------- (000) |
| * Удаление файла | * d-wx------ (300) | * ---------- (000) |
| * Чтение файла | * d--x------ (100) | * -r-------- (400) |
| * Запись в файл | * d--x------ (100) | * --w------- (200) |
| * Переименование файла | * d-wx------ (300) | * ----------(000) |
| * Создание поддиректории | * d-wx------ (300) | * ---------- (000) |
| * Удаление поддиректории | * d-wx------ (300) | * ---------- (000) |

# Выводы

В процессе выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов, а также закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

# Список литературы

1. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>
2. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: <http://bugtraq.ru/library/books/attack/index.html>
3. Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.