1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский государственный политехнический университет
3. —
4. Институт компьютерных наук и технологий
5. **Кафедра «Информационная безопасность компьютерных систем»**
6. **ЛАБОРАТОРНАЯ РАБОТА №3**
7. **Модель управления доступом операционной системы UNIX**
8. по дисциплине «Безопасность операционных систем»
9. Выполнил
10. студент гр. 43508/1 Е.М. Орел

<*подпись*>

1. Руководитель
2. А.А. Минин

<*подпись*>

1. Санкт-Петербург
2. 2017

# ЦЕЛЬ работы

Исследование характеристик механизма защиты, реализованного в операционной системе UNIX.

# ход работы

1. Создание описания системы, в которой реализована модель безопасности ОС UNIX.

В модели присутствуют 4 субъекта (s1, s2, s3, s4) и 2 группы g1, g2. Причем s1 и s2 принадлежат группе g1, а s3 и s4 группе g2.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Объект | Владелец-пользователь | Владелец-группа | Права владельца-пользователя | Права владельца-группы | Права остальных пользователей |
| dir1 | s1 | g1 | rwx | rwx | - |
| dir2 | s1 | g1 | rwx | rwx | rx |
| dir3 | s2 | g1 | rwx | r | rx |
| dir4 | s3 | g2 | rwx | r | rx |
| dir5 | s3 | g2 | rx | r | rx |
| dir6 | s4 | g3 | rx | r | rx |
| file1 | s1 | g1 | rwx | rwx | - |
| file2 | s1 | g1 | rwx | rwx | rx |
| file3 | s4 | g2 | rwx | rwx | rx |
| file4 | s4 | g2 | rwx | x | r |
| file5 | s2 | g1 | rwx | x | r |

Была реализована система, начальное состояние которой отражено в таблице. В системе реализована возможность добавлять и удалять объекты, субъекты и права между ними. Также имеются функции для проверки прав.

Схема расположения файлов:

D:\Google Drive\Учеба\Универ\4 курс\1 семестр\Безопасность ОС\lab3\Диаграмма без названия.png

Проверка корректности программы:

?- can\_read(s1,file1).

true .

?- can\_read(s4,file1).

false.

?- user\_delete\_object(s4,file1).

false.

?- user\_delete\_object(s1,file1).

true.

# контрольные вопросы

* В чем заключается отличие правил контроля доступа к файлам и каталогам в ОС UNIX?

Маска доступа является такой же, но её интерпретация отличается.

* Каков формат маски прав доступа к файлам в ОС UNIX?

ugt | rwx | rwx | rwx

u- SUID – идентификатор пользователя при выполнении файла

g- SGID – идентификатор группы при выполнении файла

t-Sticky bit – бит фиксации

Первая группа rwx – права пользователя-владельца. Вторая – права пользователей, состоящих с владельцем в одной группе, третья – прочие пользователи.

* Где физически хранятся права доступа к файлам в ОС UNIX?

В битовой маске, называемой кодом доступа к файлу и автоматически создаваемой системой при создании файла, с помощью вызовов create или open.

* С какой целью применяется Sticky bit?

В старых версиях – сохранение всего образа программы в памяти/файле подкачки вплоть до выключения системы. В настоящее время такое применение для файлов избыточно. В отношении каталогов он обеспечивает дополнительную защиту – пользователь может удалить лишь те файлы, которыми он владеет или имеет право доступа на запись, т.к. при праве доступа на запись в каталог без этого бита, пользователь может удалять все прочие объекты в нем без проверки прав.

* Позволит ли наличие маски прав доступа [rwx - w – r - x] к каталогу изменить хранящийся в нем файл?

Изменить смогут все, кроме группы владельца, т.к. не установлен бит x.

# выводы

В ходе выполнения работы были изучены принципы и особенности работы механизма защиты операционной системы UNIX. Можно сделать вывод, что с её помощью можно настроить гибкое управление доступа к ФС, что и используется в ОС семейства UNIX.