Дисциплина «Защита в операционных системах»
Лабораторная работа № 9

Тема: Использование механизма «Графический киоск» для расширения возможностей администрирования дискреционного управления доступом.

Цель: Получение навыков администрирования механизма «Графический киоск» для повышения эффективности управления полномочиями пользователей, заданными дискреционными правами доступа.

Порядок выполнения лабораторной работы: работа выполняется самостоятельно под руководством преподавателя.

Время выполнения лабораторной работы (аудиторные часы) - 2 часа.

Оборудование и программное обеспечение: работа выполняется на ПЭВМ типа IBM PC с использованием стандартных функций ОССН Astra Linux.

1. Теоретические сведения

В ОССН Astra Linux SE, помимо дискреционной модели управления доступом, предусмотрен еще один механизм ограничения прав пользователей в системе - **Киоск (или режим киоска)** – это инструмент подсистемы безопасности PARSEC, который служит для управления ограничениями пользователей в системе. Работу режима киоска обеспечивает пакет parsec-kiosk.

В ОССН Astra Linux SE реализованы два варианта режима «Киоск» (см. рис 1):

- **высокоуровневый киоск** – ***Графический киоск*** (ограничение прав на уровне графического интерфейса);

- **низкоуровневый киоск** – ***Системный киоск*** (ограничение прав на уровне ядра системы).

Рисунок 1 – Виды режима «Киоск», реализованных в ОССН Astra Linux SE

В последних версиях ОССН Astra Linux Special Edition режим «Киоск» заменен режимом «Киоск-2», который рекомендован компанией-разработчиком к использованию.

Киоск-2 (или режим Киоск-2) – это новый инструмент PARSEC, заменяющий режим киоска. Работу режима Киоск-2 обеспечивает пакет parsec-kiosk2. Пакет parsec-kiosk2 содержит инструменты для ограничения возможностей, предоставляемых непривилегированным пользователям и представляет собой обновлённую версию пакета parsec-kiosk. Пакет parsec-kiosk2 входит в состав обновления Astra Linux Special Edition (очередное обновление 1.6).

Отличие от системного киоска

Графический киоск ограничивает доступ на уровне графической среды. Системный киоск, в отличие от графического киоска, ограничивает пользователя на более низком уровне — на уровне ядра системы, управляя доступом к конкретным файлам. Системный киоск обеспечивает более надежную защиту от несанкционированного доступа, чем графический.

1.1 Графический киоск

При использовании графического киоска пользователю или группе пользователей разрешается запускать только приложения, явно указанные в их профиле. На пользователя действуют ограничения, только если подкаталог с его профилем существует в каталоге `/etc/fly-kiosk` или этот пользователь входит в группу, для которой существует профиль в каталоге `/etc/fly-kiosk` (этот каталог по умолчанию не существует, и создается при включении режима

графического киоска). Профиль пользователя или группы представляет собой набор ярлыков и настроек. Поиск профиля осуществляется по имени пользователя/группы. Например, профили для пользователя с именем `user` и группы с именем `group` будут найдены, если существуют каталоги:

```
/etc/fly-kiosk/user
/etc/fly-kiosk/group
```

Для группы дополнительно необходимо указать, что это профиль группы. В конфигурационном файле `/etc/fly-kiosk/group/fly-kiosk.conf` должна быть строка `IsGroup=true`.

Внимание!

При одновременном включении графического киоска и у пользователя и у группы будет применен только профиль пользователя.

Настройки

У графического киоска есть следующие возможности:

- **Автозапуск приложений для всех пользователей графического киоска.** Ярлыки приложений должны размещаться в каталоге `/etc/xdg/autostart` и содержать строку `OnlyShowIn=fly-kiosk`;
- **Автозапуск приложений для конкретного профиля пользователя.** Ярлыки приложений должны размещаться в каталоге `/etc/fly-kiosk/user/autostart`;
- **Размещение ярлыков на рабочем столе пользователя.** Ярлыки приложений должны размещаться в каталоге `/etc/fly-kiosk/user/desktop`;
- **Размещение ярлыков на панели задач пользователя.** Ярлыки приложений должны размещаться в каталоге `/etc/fly-kiosk/user/toolbar`;
- **Режим одного приложения.** В данном режиме приложение запускается при входе на весь экран. Панель задач отсутствует, верхняя панель приложения отсутствует (т.е. закрыть "крестом" или свернуть приложение невозможно, необходимо завершать приложение его собственными средствами). При выходе из приложения текущая сессия завершается. Ярлык приложения должен лежать в каталоге `/etc/fly-kiosk/user/single`;
- **Другие разрешенные приложения.** Данные приложения нигде не будут размещены, но могут быть запущены через другие приложения. Ярлыки приложений должны лежать в каталоге `/etc/fly-kiosk/user`

➢ **Конфигурационный файл** `/etc/fly-kiosk/user/fly-kiosk.conf` имеет следующие опции:

`EditableDesktop=false`. Данная опция позволяет создавать файлы на рабочем столе. Например, сохранение документа на рабочем столе;

`EditableTheme=false`. Данная опция позволяет редактировать пользовательские настройки оформления, темы и т.д.;

`IsGroup=false`. Данная опция указывает, является ли данный профиль профилем группы.

Графическая утилита настройки

Все вышеперечисленные настройки для пользователей и групп можно выполнить с помощью графической утилиты "Политика безопасности" ("Меню Пуск" → "Панель управления" → "Безопасность" → "Пользователи" или "Меню Пуск" → "Панель управления" → "Безопасность" → "Группы") (см. рис 2).

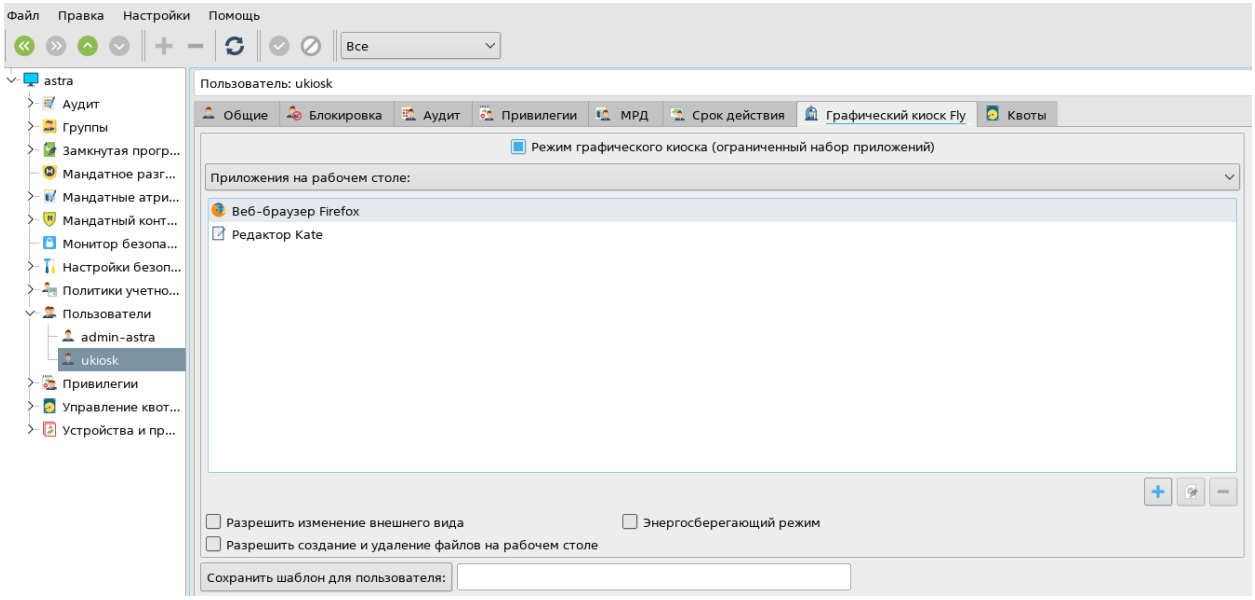

Рисунок 2 – Активация режима графического киоска

В графической утилите присутствуют дополнительные возможности:

- Сохранение настроенного профиля по указанному пути. Например, для последующего распространения через системы управления конфигурациями.

- Настройка FireJail для выбранного приложения.

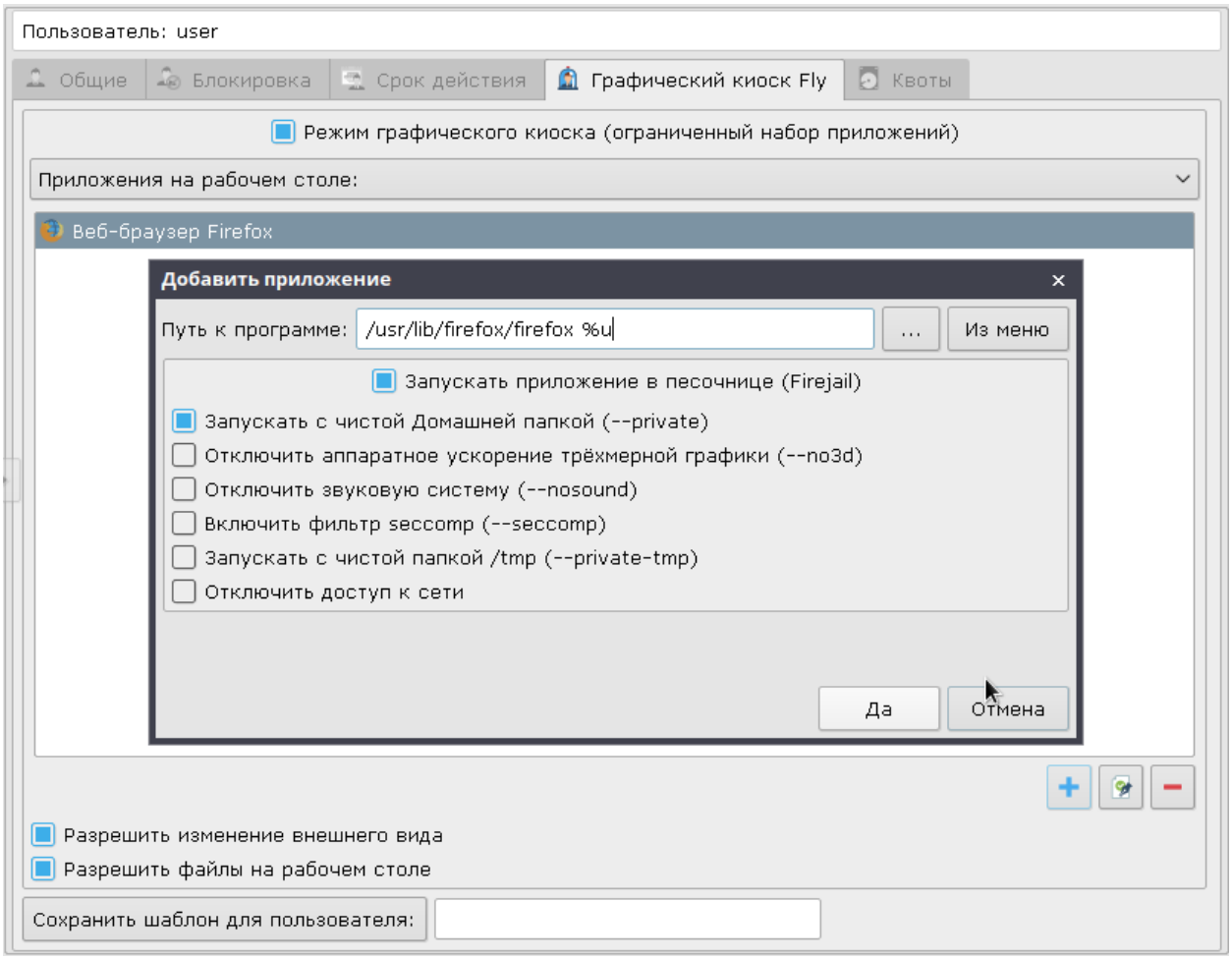

Рисунок 3 – Дополнительные настройки исполняемого файла в режиме Графического киоска

Ограничения командного интерпретатора rbash

В графическом киоске по умолчанию используется более ограниченный и безопасный командный интерпретатор rbash, из-за ограничений которого возникают следующие особенности запуска приложений через firejail:

- в ярлыках приложений нельзя использовать полные пути к файлам приложений.

Пример полного пути:

```
Exec=firejail /usr/bin/goldendict
```

- следует использовать только имя файла:

```
Exec=firejail goldendict.
```

2. Задание

1. От имени привилегированного администратора безопасности ОССН на уровне целостности «Высокий» в разделе «Пользователи» графической утилиты «Управление политикой безопасности» (fly-admin-smc):

- создать учетную запись пользователя с именем `ukiosk`;

- в разделе «Графический киоск *Fly»* для учетной записи пользователя `ukiosk` активировать «Режим графического киоска»;
- добавить в список размещенных на рабочем столе и доступных для запуска приложений браузер *Firefox,* указав полный путь к соответствующему исполняемому файлу

2. Выполнить вход в систему от имени учетной записи пользователя `ukiosk` *и* убедиться, что ему доступно для запуска только одно приложение – браузер *Firefox.*

3. По аналогии с пунктами 1-2 задать перечень доступных приложений для запуска из панели задач (или в режиме автозапуска, или в режиме одного приложения) и указать особенности их применения.

4. Отключить «Режим графического киоска» и завершить все активные сессии от имени учетной записи пользователя *ukiosk.*

3. Контрольные вопросы

1. Какие режимы «Киоск» реализованы в ОССН Astra Linux SE?
2. Для чего предназначен режим «Графический киоск»?
3. Чем режим «Графический киоск» отличается от режима «Киоск-2»?
4. Как настроить приложения на рабочем столе в режиме «Графический киоск»?
5. Как настроить автозапуск приложений при входе пользователя в режиме «Графический киоск»?
6. Для чего предназначен режим одного приложения в режиме «Графический киоск»?

4. Требования к отчёту

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4. На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, группа, проверил: преподаватель ФИО (образец титульного листа представлен в приложении 1).

Отчет должен содержать:

— титульный лист;
— цель работы;
— краткие теоретические сведения, ответы на контрольные вопросы;
— описание хода выполнения работы со скриншотами;
— выводы