

## **Режим киоска в РЕД ОС как инструмент ограничения прав пользователей**

*Родионов Алексей Анатольевич, ООО «РЕД СОФТ»*

*121205, город Москва, территория Сколково инновационного центра, ул. Нобеля, д. 5,*

*эт.2, пом. 4*

*alexey.rodionov@red-soft.ru*

### **Введение**

Режим киоска сам по себе не является средством защиты информации, а является собой инструмент для ограничений прав пользователей на уровне операционной системы. Однако, его можно рассматривать как компонент целостной системы защиты информации на уровне РЕД ОС.

Программное обеспечение режима киоска обеспечивает безопасность, предотвращая злонамеренные атаки и неправильное использование предоставляемых функций. Не менее важным является способность программного обеспечения в данном режиме ограничивать пользователей, не являющихся злоумышленниками, определёнными заданными действиями, чтобы устройство можно было использовать для выполнения конкретной задачи или функции.

Режим киоска в РЕД ОС представляет собой рабочую среду для пользователя или группы пользователей с чётко ограниченным функционалом – пользователи имеют доступ только к тем приложениям, которые явно указаны для их профиля. Такой подход позволяет интегрировать использование режима киоска в общую политику информационной безопасности компании, дополняя уже имеющиеся ограничения и функции контроля пользователей.

### **Основные функции режима киоска в РЕД ОС**

Режим киоска является важным компонентом для защиты устройств от непреднамеренного использования и несанкционированного доступа. В программном обеспечении киоска есть возможность для администратора настроить программное обеспечение в соответствии с требованиями корпоративной политики информационной безопасности и выполняемых рабочих функций пользователей и ограничить их поведение.

Очень важно, чтобы программное обеспечение режима киоска не позволяло пользователю получать полный доступ к рабочему столу или файловой системе. Этот тип защиты может быть затруднён в реализации, поскольку, например, стандартный диалог печати позволяет распечатать содержимое в файл и предоставить пользователю доступ к файловой системе. То же самое верно для многих гиперссылок внутри разрешённого программного обеспечения, которые позволяют обращаться как к файловой системе, так и к ресурсам в Сети Интернет.

Если киоск оснащён клавиатурой, программное обеспечение также должно отключить все проблемные специальные клавиши и последовательности нажатий клавиш. Часто вместо физической клавиатуры используется клавиатура с сенсорным экраном или «виртуальная» клавиатура, функционал которых также необходимо ограничивать, чтобы не позволить пользователю выйти из ограничений режима киоска.

Одной из важнейших функций программного обеспечения киоска является возможность очистки кэша, истории использования и данных о пользователях. Это предотвращает доступ пользователей к личным данным и защищает как устройство, так и пользователя от несанкционированного доступа к данным.

Ещё одной важной особенностью режима киоска является возможность отключения портов USB и других устройств внешнего доступа, включая ограничения по работе с сетью, когда применяется не только глубокая фильтрация пакетов, но и отключение сетевых интерфейсов по усмотрению администратора.

## Способы реализации ограничений

Режим киоска в РЕД ОС реализуется с помощью доработанной командной оболочки Bash и окружения рабочего стола MATE.

Базовый функционал киоска реализован в нескольких пакетах и находится в выключенном состоянии. Режим киоска с утилитами для его настройки становится доступным после установки пакета redos-kiosk-utils.

При включенном режиме киоска пользователю становятся недоступны:

- запуск программ с графическим интерфейсом, кроме явно разрешённых;
- выполнение сценариев на любом языке при явном их запуске пользователем;
- запуск на выполнение файлов с установленным битом SUID;
- изменение свойств и содержимого главной панели на Рабочем столе, а также изменение содержимого Рабочего стола;
- автоматическое монтирование внешних накопителей;
- смена виртуальной консоли по сочетанию клавиш Ctrl+Alt+Fn;
- использование «горячих клавиш»;
- недоступность ряда утилит окружения MATE (включая Центр управления) для исключения возможности обойти запреты режима киоска. Даже при ручном запуске данных утилит их выполнение блокируется;
- дополнительное ущемление прав и возможностей пользователя путём запуска приложений в «песочнице» (Firejail).

Фильтрация приложений осуществляется по принципу «серого списка», чтобы не усложнить как администрирование киоска, так и работу пользователя, когда приложение требует для своей работы ряд других программ, но они попадают под запрет, если используется принцип «белых списков». И в то же время не позволяет пользователю обойти ограничения режима киоска, если бы использовался принцип «чёрных списков».

Реализация режима киоска в РЕД ОС позволяет использовать его не только в графических сеансах, но и в консольном режиме работы — в таком случае большая часть работы ложится на командный интерпретатор Bash.

## Проблемы

К основным проблемам можно отнести следующие:

- многообразие оборудования (в первую очередь клавиатур), которые позволяют в редких случаях выходить за рамки ограничений режима киоска;
- сложные собственные схемы защиты информации, используемые у пользователей РЕД ОС, которые затрудняют настройку режима киоска;
- профильное специфическое программное обеспечение у пользователей РЕД ОС, которое не всегда хорошо функционирует в режиме киоска.

## Заключение

Режим киоска в РЕД ОС как способ дополнительных ограничений для пользователя предоставляет администраторам дополнительный инструментарий, который позволяет расширить возможности в реализации политик информационной безопасности средствами операционной системы.