## ЗАКЛЮЧЕНИЕ

В данной работе представлены алгоритмы учёта позиционных лимитов, позволяющие корректно обработать исключительные ситуации, вызванные неверными входными параметрами движения. Применение разработанных алгоритмов в системе KPA MCL помогло численно решить задачу нахождения максимальной скорости прохождения траектории.

### Литература


1. Technical Paper PLCopen Technical Committee 2 – Task Force Function Blocks for motion control: Part 4 –Coordinated Motion PLCopen Document, Version 1.0, Published
2. *Kröger T.* On-Line Trajectory Generation: Nonconstant Motion Constraints. In Proc. of the IEEE International Conference on Robotics and Automation, pp. 2048-2054, Saint Paul, MN, USA, May 2012.
3. *Беклемишев Д. В.* Курс аналитической геометрии и линейной алгебры. Издание 12-е, исправленное. / Д.В. Беклемишев. – М.: Физматлит, 2009. – 312 с. – ISBN 978-5-9221-0979-6.
4. *Абрашина-Жадаева Н. Г.* Аналитическая геометрия в примерах и задачах / Н.Г. Абрашина-Жадаева, Л.Л. Березкина, А.Н. Ковальчук, Н.К. Филиппова. –Мн.: РИВШ, 2008.–156 с.


# РАЗРАБОТКА ПОЛИТИК МАНДАТНОГО УПРАВЛЕНИЯ ДОСТУПОМ В ОС FEDORA НА ОСНОВЕ SELINUX


**А. О. Козлов, Е. Е. Попко**


## ВВЕДЕНИЕ

В операционных системах используются механизмы управления доступом, которые определяют, может ли субъект (пользователь или программа) получить доступ к определенному ресурсу.

Контроль доступа к объектам операционной системы Linux может осуществляться следующими механизмами разграничения доступа:

- дискреционный контроль доступа (discretionary access control, DAC);
- механизм, реализующий списки контроля доступа (access control list, ACL);
- средства разграничения доступа, позволяющие реализовать механизм мандатного контроля доступа (mandatory access control, MAC).

Основным механизмом контроля доступа является дискреционный контроль доступа, который определяет права для трех категорий: пользователь-владелец файла; члены группы, являющейся владельцем файла;

остальные пользователи. Для каждой категории определяется три типа прав доступа: на чтение, запись и выполнение.

Механизм, реализующий списки контроля доступа, позволяет расширить стандартные права доступа и установить индивидуальные разрешения для каждого пользователя или отдельной группы.

Достоинством дискреционного управления доступом является простая реализация системы разграничения доступа. Однако, защищенность системы, в которой используется механизмы только дискреционного контроля доступа, в некоторых случаях будет недостаточной. Поэтому использование модулей, позволяющих реализовать механизмы мандатного контроля доступа, повышает уровень безопасности системы.

Целью данной работы является исследование механизма реализации мандатного управления доступом Security Enhanced Linux на примере ОС Fedora и реализация собственной политики.

## SECURITY-ENHANCED LINUX (SELINUX)

Security Enhanced Linux – это реализация мандатного управления доступом в ядре Linux, проверяющего разрешение операций после проверки стандартного дискреционного управления доступом. [1]

Работа SeLinux доступна в трех режимах:

- enforcing (принудительный) – все действия, которые нарушают текущую политику безопасности, блокируются, а попытка нарушения будет зафиксирована в журнале;
- permissive (разрешающий) – информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы;
- disabled (отключен) – полное отключение системы принудительного контроля доступа, используются только правил DAC [1].

В системе обеспечения мандатного контроля доступа SELinux все объекты и субъекты помечаются с помощью специальных меток, которые называются контекстом безопасности. Когда субъект пытается произвести какое-либо действие в отношении объекта, информация об этом действии поступает к обработчику подсистемы безопасности. Обработчик анализирует контексты безопасности субъекта и объекта и, сверяясь с написанными ранее правилами, принимает решение о дозволенности действия.

Контекст безопасности – это набор всех атрибутов в системе SELinux, которые связаны с объектами и субъектам, имеющий вид [2, 3]:

user : role : type [: level ], где

- user – атрибут-пользователь, ассоциированный с одним или более пользователем операционной системы;
- role – атрибут-роль, ассоциированный с одним или более типом, к которым пользователь SELinux имеет доступ;
- type – атрибут-тип, определяющий возможные виды доступа сущностей данного типа (домен для процессов и тип для файлов);
- level – атрибут-уровень безопасности при использовании мандатных механизмов безопасности MLS или MCS.

## СОЗДАНИЕ НОВОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ SELINUX

Целевая политика (targeted) – это политика, используемая в ОС Fedora по умолчанию. Политика безопасности задается один раз в момент установки системы и представляет собой набор текстовых файлов, которые загружаются в память ядра Linux при старте системы.

Когда используется целевая политика, процессы, которые являются целевыми, запускаются в ограниченном домене, остальные процессы запускаются в неограниченном домене. Например, по умолчанию пользователи, прошедшие авторизацию, работают в домене unconfined_t и системные процессы, запущенные при инициализации, запускаются в домене initrc_t – оба домена неограниченные [1].

Пользователи SELinux – это часть политики системы безопасности SELinux. Пользователи операционной системы сопоставляются с пользователями системы безопасности через политику SELinux. В политике существует определенное число ограниченных (confined) и неограниченных (unconfined) пользователей.

В ОС Fedora, пользователи операционной системы работают неограниченно по умолчанию, но могут быть сопоставлены с ограниченными пользователями SELinux для получения преимуществ использования ролей безопасности и применяемых к ним механизмов.

Например, сопоставление пользователя Linux с пользователем SELinux user_u, приводит к тому, что пользователь операционной системы не может выполнить (до тех пор, пока не будет сконфигурировано обратное) приложение с использованием SUID бита (setuid), такие как sudo и su, также предотвращает возможность записи ими в их домашние директории – и если сконфигурировано, то предотвращает запуск пользователями вредоносного программного обеспечения из их домашних директорий [1].

Для повышения безопасности системы необходимо настроить подсистему мандатного управления доступом таким образом, чтобы по умолчанию Linux-пользователи сопоставлялись ограниченным SELinux-

пользователям. В случае, если пользователи операционной системы в процессе работы должны выполнять задачи отличные от возможностей, встроенных по умолчанию ограниченных пользователей, необходимо создать новых SELinux-пользователей с определенными политиками безопасности и сопоставить им пользователей операционной системы.

Одним из способов решения данной задачи является создание пользовательского домена SELinux на основе существующего ограниченного профиля user_t [4].

Таким образом, основными этапами реализации являются:

1. Создать новое окружение пользователя SELinux на основе пользовательского домена *user_t* и установить его в модуль политики SELinux (SELinux Policy Module).

    1.1. Создать новый ограниченный пользовательский домен, почти идентичный *user_t*, сопоставленный по умолчанию пользователю SELinux *user_u.*

    1.2. Добавить политики, разрешающие выполнение необходимых для данного ограниченного пользователя действий.

    1.3. Сопоставить программно пользовательский домен новому пользователю SELinux.

2. Собрать из исходной политики бинарный модуль политики SELinux.

3. Установить вновь созданный бинарный модуль политики.

4. Определить для нового SElinux-пользователя контекст безопасности по умолчанию, чтобы программы входа знали, какой домен пользователя использовать.

5. Добавить нового пользователя операционной системы и сопоставить его новому SELinux-пользователю.

**ЗАКЛЮЧЕНИЕ**

В большинстве сценариев работы пользователей операционной системы Linux должно хватать возможностей предопределенных (ограниченных и неограниченных) пользователей SELinux. Если ни один из предопределенных SELinux-пользователей не подходит профилю пользователя операционной системы следует реализовать новую ограниченную среду под свои определенные требования.

В результате работы был создан и протестирован модуль пользовательской политики безопасности SELinux и создан новый пользователь с ограниченными правами, который получил отличные от существующих в системе SELinux-пользователей возможности.

**Литература**

1. Интернет-адрес: https://docs.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced_Linux/index.html
2. *Колисниченко Д. Н.* Linux от новичка к профессионалу / 3-е издание. С.-П., БХВ-Петербург, 2011.
3. Интернет-адрес: http://selinuxproject.org/
4. Интернет-адрес: http://www.opennet.ru/base/sec/selinux_tips.txt.html

# РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ НА БАЗЕ ОС ANDROID ДЛЯ КОНТРОЛЯ ПЕРЕМЕЩЕНИЯ ПЕРСОНАЛА И ТРАНСПОРТА

**Д. С. Королев**

## ВВЕДЕНИЕ

Задача повышения эффективности производственного процесса всегда остается важнейшей проблемой в работе предприятий. Мониторинг персонала в режиме реального времени, дает уникальную возможность всегда иметь точную и достоверную информацию о реальном местоположении работников и транспортных средств. Появляется возможность контролировать время прибытия, количество часов, проведенных на рабочем месте, пробег, а также маршрут движения.

Данная статья посвящена разработке полноценного комплекса на базе ОС Android для контроля перемещения персонала и транспорта с помощью мобильных устройств. Особое внимание в данной статье уделено: высокоточному определению географических координат, максимальному энергосбережению, вопросом безопасности и коммуникации с существующими системами мониторинга местоположения, что в полной мере не могут обеспечить аналоги.

## МОДУЛИ ПРИЕМА ГЕОГРАФИЧЕСКОГО МЕСТОПОЛОЖЕНИЯ

Предоставленная Android SDK логика сглаживает лишь часть проблем и недостатков GPS приемников в мобильных устройствах, поэтому стандартного API становится недостаточно.

Получение своевременно достоверного местоположения является наивысшим приоритетом в работе нашего приложении. Именно по этой причине обработка и получение координат осуществляется в отдельном потоке, что существенно сокращает время «холодного» и «теплого»