Московский физико-технический институт (государственный университет)
Факультет радиотехники и кибернетики
Кафедра информатики и вычислительной техники

Централизованная настройка системы мониторинга действий пользователя в операционной системе Эльбрус

Выпускная квалификационная работа
(бакалаврская работа)

Выполнил: Таранцов Сергей, 313 гр.
Научный руководитель: Межуев Ю. В.

Мониторинг событий в едином пространстве пользователей

Единое пространство пользователей (ЕПП) представляет собой средства организации работы пользователя в сети компьютеров, работающих под управлением ОС «Эльбрус».

Система мониторинга действий пользователя:

- регистрация действий субъектов (пользователей, процессов) и операций над защищаемыми объектами (файлами, каталогами, устройствами);
- основана на подсистеме аудита ядра ОС.

Состав подсистемы аудита:

- модуль ядра ОС, перехватывающий системные вызовы (события с точки зрения ядра) и регистрирующий событие;
- демон auditd, записывающий зарегистрированное событие на диск;
- утилиты управления (настройка подсистемы, формирование правил и просмотр зарегистрированных событий).

Цель

Реализация централизованной настройки системы мониторинга действий пользователя в ЕПП на основе подсистемы аудита.

Задачи

- Исследование системных вызовов Linux;
- Доработка графического интерфейса управления ЕПП с целью формирования набора правил аудита для каждого пользователя;
- Организация централизованного хранения правил аудита для пользователей ЕПП;
- Разработка метода аутентификации, устанавливающего набор правил аудита при входе в систему и удаляющего набор после выхода из сессии.

Требования

- Язык разработки: C;
- Поддержка архитектуры Эльбрус, Intel x86.

Исследование системных вызовов

Системный вызов – обращение пользовательской программы к ядру ОС с запросом на выполнение определенной операции. В ядре Linux более 300 системных вызовов.

Необходимость отслеживания действий пользователя обусловлена тем, что по итогам 2016 года утечки информации вследствие некорректных или противоправных системных вызовов составляют значительную часть от общего числа. Эти утечки представляют собой передачу конфиденциальной информации по сети либо на внешние носители.

На основе этих данных в первой версии программы был составлен список наиболее востребованных системных вызовов для регистрации нарушения конфиденциальности информации. При необходимости возможно расширение списка до всех системных вызовов ядра Linux.

Выбранные для мониторинга системные вызовы

Группа	**Системные вызовы**	**Описание**
cap	capget, capset	Возможности процесса
chroot	chroot	Смена корневого каталога
uid	setuid, setreuid, setfsuid, setresuid, getuid, geteuid, getresuid, (и -32)	Работа с идентификаторами пользователей
mount	mount, umount, umount2	Файловые системы
net	socketcall	Сист. вызовы сокетов
chmod	chmod, fchmod, fchmodat	Права доступа к файлу
chown	chown, lchown, fchown, -32, fchownat	Изменение владельца файла
xattr	set-, lset-, fset-, get-, lget-, fget-, аналог. list-, remove-, -xattr	Работа с расширенными атрибутами
open	open, openat	Открытие файлов или устройств
rename	rename, renameat	Изменение имени файлов
creat	creat, mkdir	Создание файлов и каталогов
delete	unlink, unlinkat, rmdir	Удаление файлов и каталогов
module	create_, init_, query_, delete_module	Загружаемые модули ядра
gid	setgid, getgid, getegid, setregid, setfsgid, setresgid, getresgid, -32, setpgid, getpgid	Работа с идентификаторами групп
exec	execve	Выполнение программы

Организация ЕПП для централизованной настройки аудита

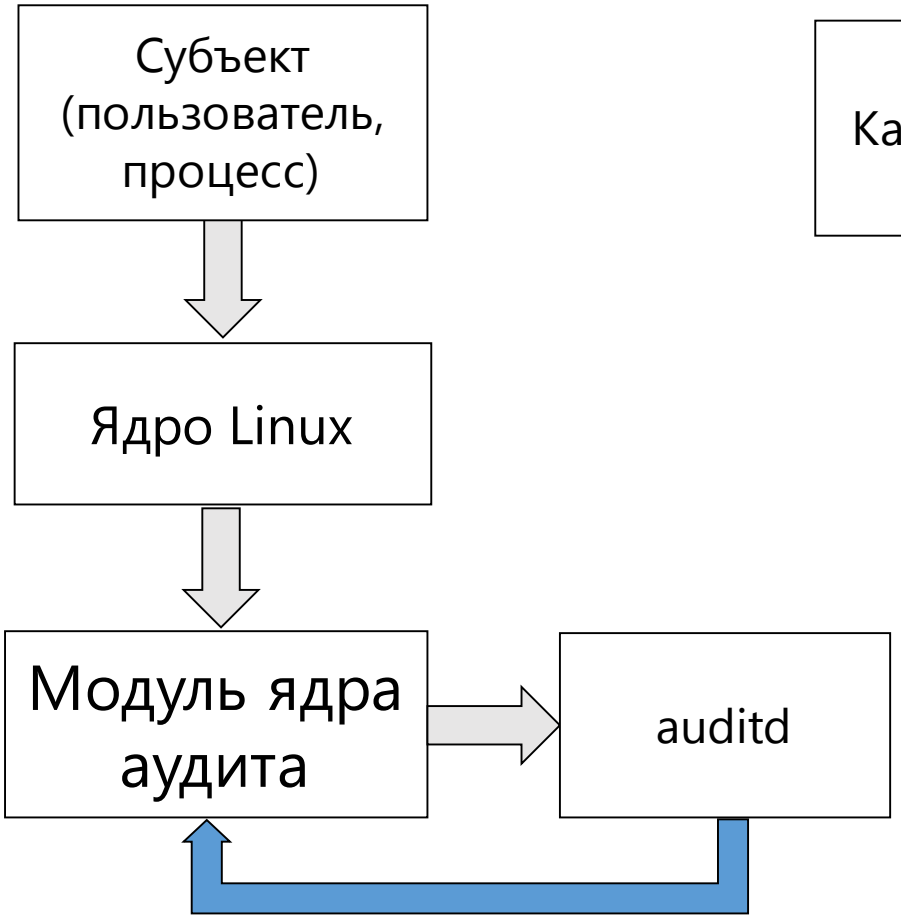
В ЕПП сетевая аутентификация и централизация хранения информации реализуется механизмом PAM и протоколом LDAP.

- PAM (Pluggable Authentication Modules) интегрирует низкоуровневые методы аутентификации. Состоит из набора библиотек и конфигурационных файлов – сценариев процедур аутентификации.
- LDAP (Lightweight Directory Access Protocol) – осуществляет доступ к удаленным данным. Источник данных для сервисов на базе PAM.

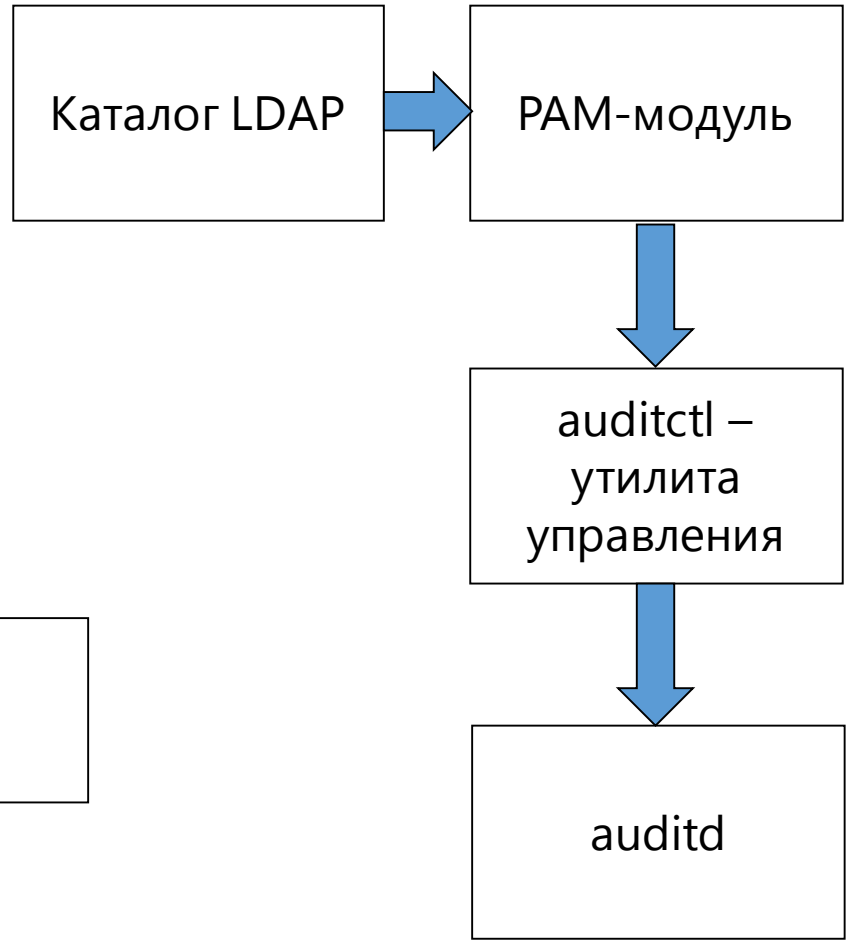
В ЕПП разработана централизация настройки подсистемы аудита с помощью LDAP, осуществляющего хранение всех политик аудита – наборов правил для каждого пользователя. Политики редактируются посредством интерфейса управления ЕПП. Добавление правил аудита осуществляется механизмом PAM при аутентификации пользователя.

Подсистема аудита

Обработка системных вызовов



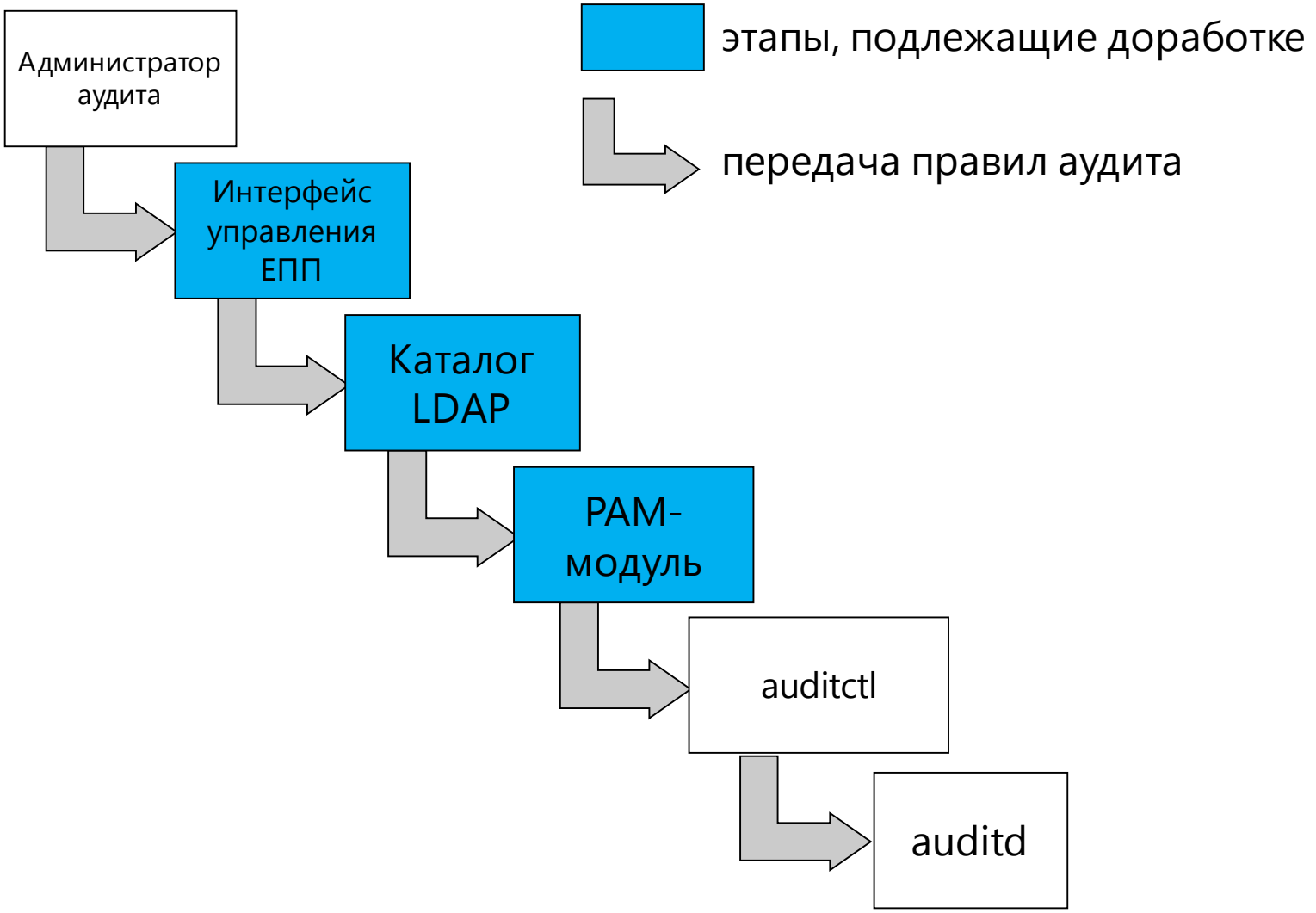
Принятая и реализованная схема настройки правил аудита при входе в систему



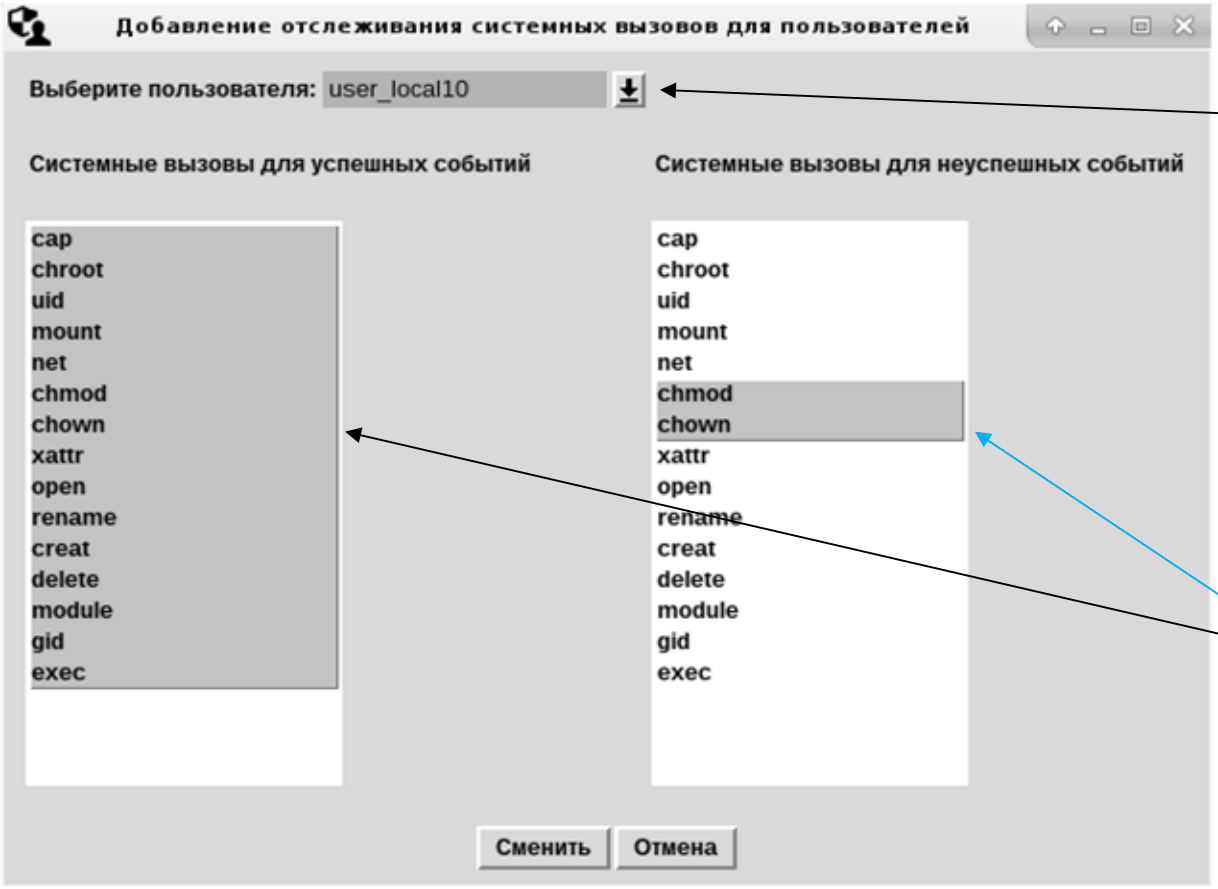
системный вызов

правила аудита

Реализованный маршрут политик аудита



Графический интерфейс управления ЕПП



поле выбора пользователя

поля выбора политик мониторинга успешных (выполненных) и неуспешных (невыполненных) системных вызовов

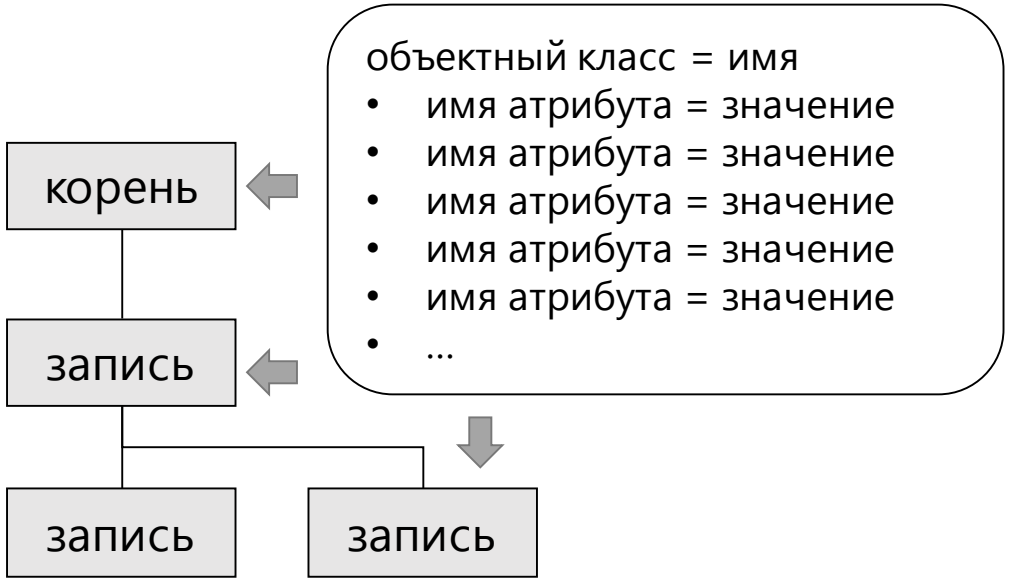
Доработан графический интерфейс управления ЕПП для работы с подсистемой аудита. Добавлены настройки подсистемы аудита для консольной утилиты управления ЕПП.

Доработка каталога LDAP

Хранение правил аудита, задаваемых с помощью графического либо консольного интерфейса управления ЕПП, реализовано в службе каталогов LDAP. Для каждого пользователя ЕПП в конфигурационном файле, хранящемся на сервере LDAP, записана строчка вида:

<имя пользователя>:<код набора аудита для выполненных вызовов>:
<код набора аудита для невыполненных вызовов >

В LDAP данные представлены как иерархия записей – информационное дерево каталогов. Записи состоят из объектных классов, классы – из атрибутов. В схеме данных LDAP в ЕПП набор правил аудита реализован как дополнительный атрибут записи, в которой хранятся аутентификационные данные пользователя для ЕПП. Имя атрибута – **elmac-user-audit**.

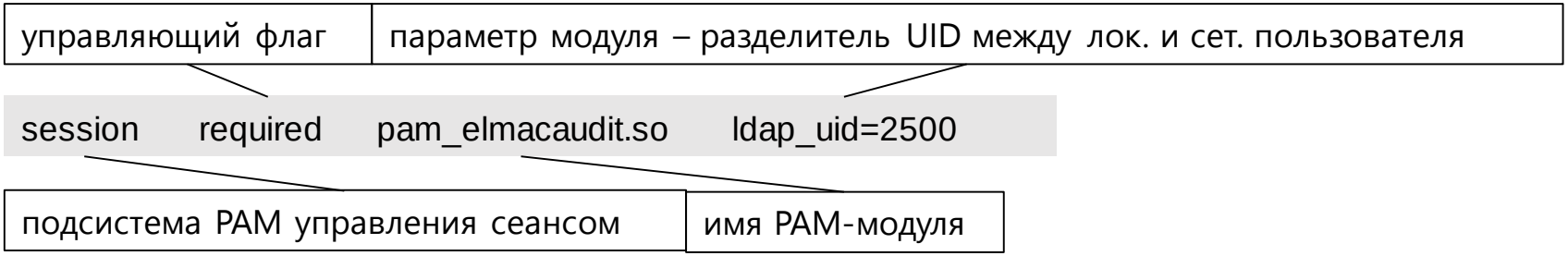


Разработанный PAM-модуль

Конфигурация модуля

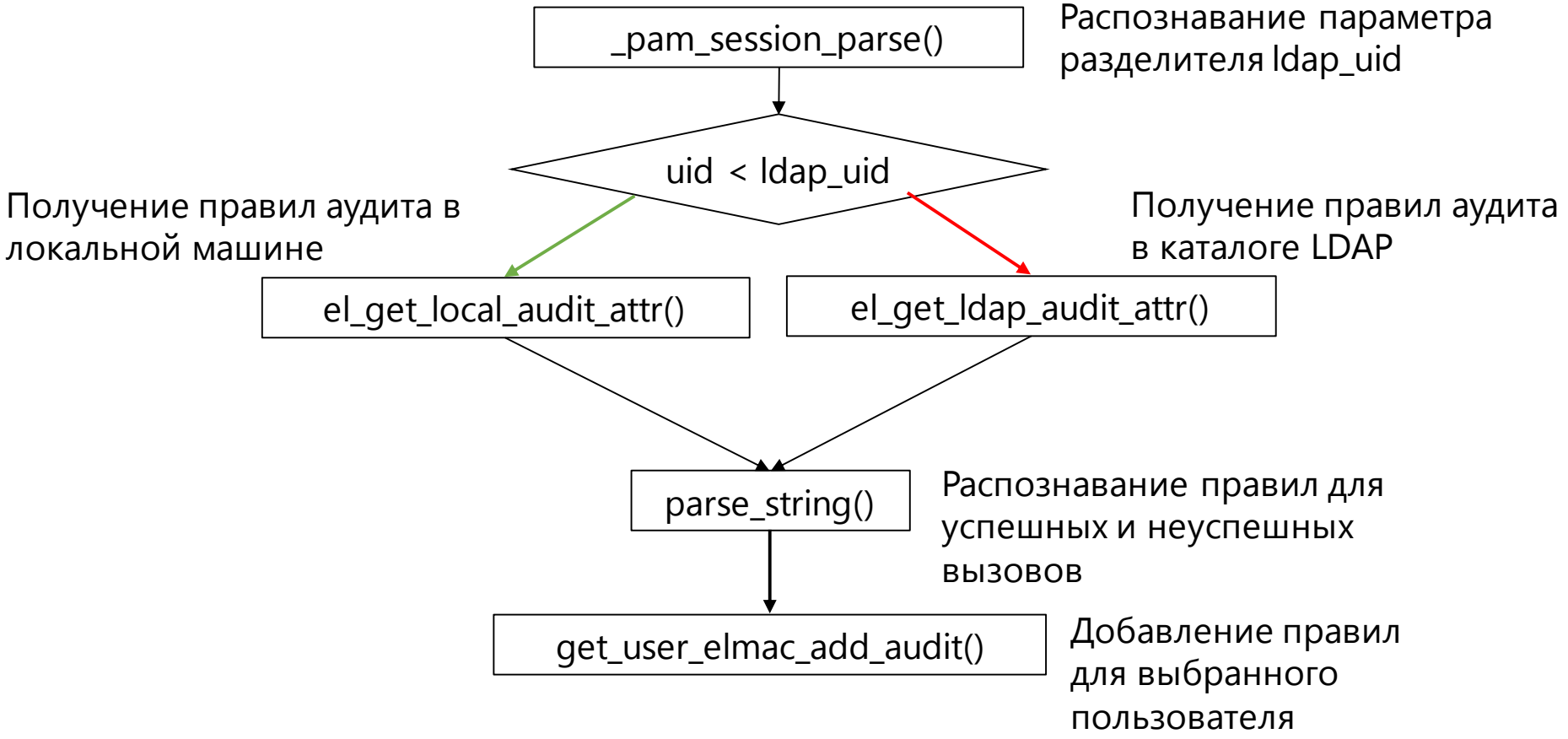
Добавление правил аудита осуществляется при входе пользователя в сессию с помощью PAM-модуля **pam_elmacaudit.so**. Исходный код библиотеки разработан на языке C.

Данная библиотека аутентификации добавляется к списку стандартных библиотек, запускаемых при входе в сессию. Это реализуется добавлением файла библиотеки в /lib64/security и добавлением в конфигурационный файл /etc/pam.d/login строчки :



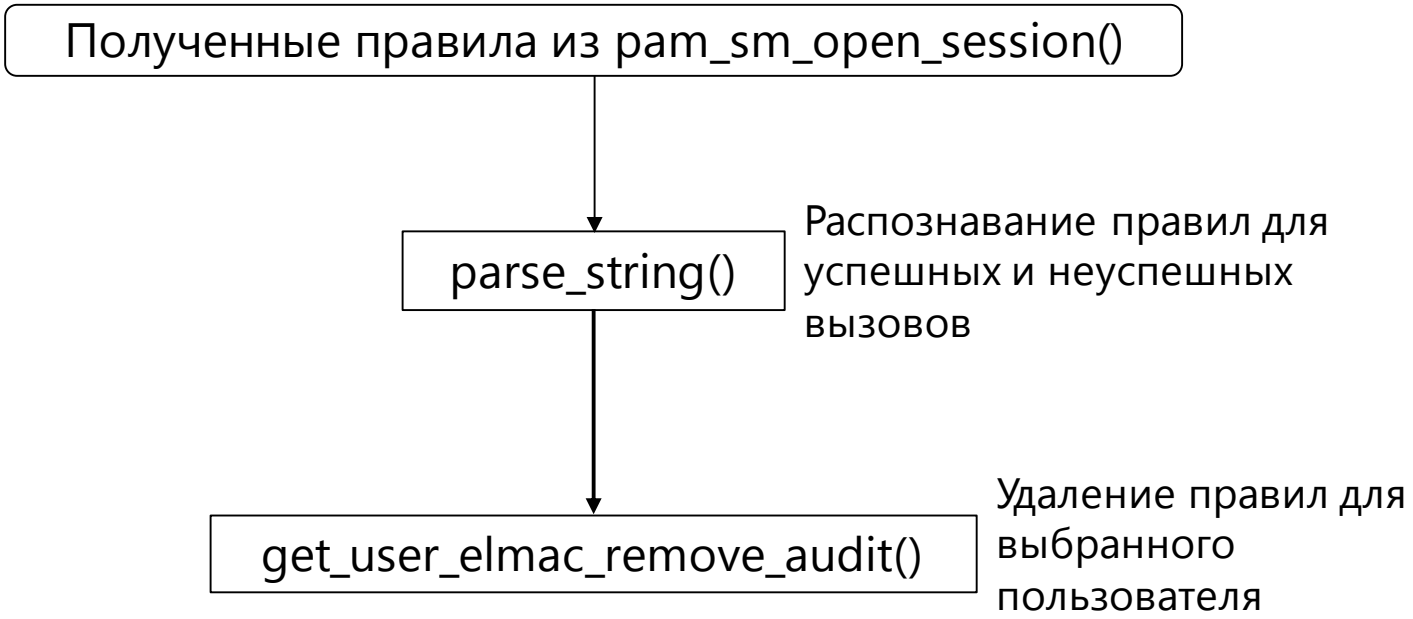
Разработанный PAM-модуль

Вход в сессию реализуется функцией pam_sm_open_session()



Разработанный PAM-модуль

Выход из сессии реализуется функцией pam_sm_close_session()



Результаты

- Проведено исследование системных вызовов и отобраны вызовы, наиболее целесообразные для мониторинга
- Доработан графический интерфейс управления ЕПП для работы с подсистемой аудита и формирования правил для каждого пользователя в ЕПП
- Организовано централизованное хранение правил аудита для пользователей ЕПП с помощью службы каталогов LDAP
- Разработан PAM-модуль, реализующий установку набора правил аудита при входе в сессию и удаление набора при выходе из сессии