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

Выпускная квалификационная работа магистра

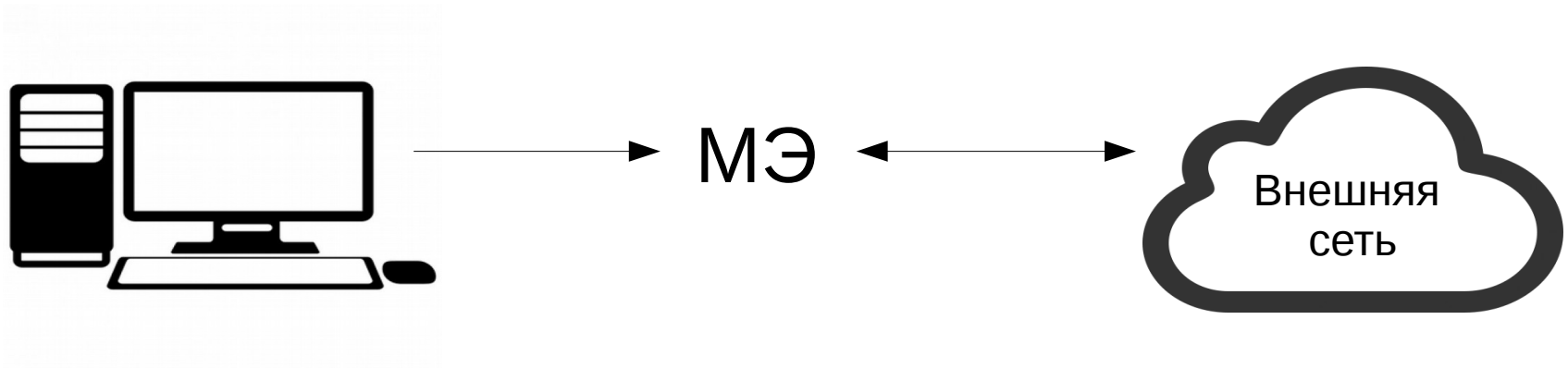
Разработка межсетевого экрана уровня узла второго класса защиты в операционной системе "Эльбрус-Д"

Студент: Имкенов А.А., 313 группа
Научный руководитель: к.т.н. Морозов Ю.В.

Межсетевой экран уровня узла

Межсетевой экран (МЭ) представляет собой программное средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков.

МЭ уровня узла применяется на узле (хосте) информационной системы.



Цель работы

Доработать межсетевой экран операционной системы «Эльбрус-Д» с целью выполнения требований ФСТЭК (*Федеральная служба по техническому и экспортному контролю)* для межсетевых экранов уровня узла второго класса:

- Контроль и фильтрация информационных потоков
- Управление функциями безопасности
- Регистрация событий безопасности (аудит)
- Обеспечение бесперебойного функционирования и восстановления
- Централизованное управление

Задачи

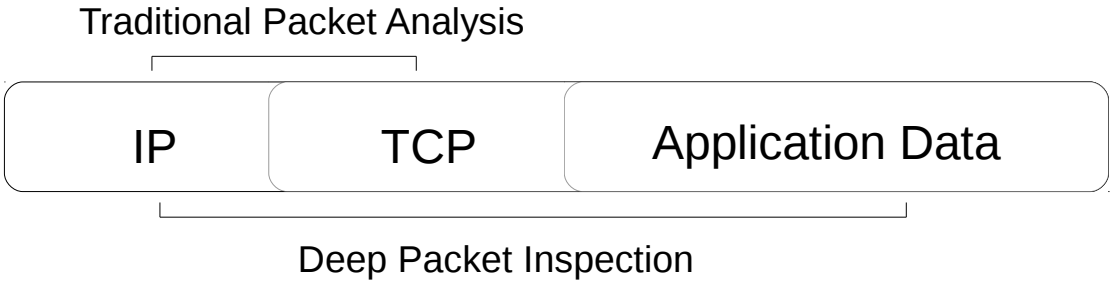
В операционной системе «Эльбрус-Д» в качестве межсетевого экрана используется подсистема Netfilter, встроенная в ядро Linux.

На основе анализа стандартного функционала Netfilter были определены отсутствующие в нем требования:

- Обеспечение возможности фильтрации сетевых пакетов на уровне прикладных протоколов
- Реализация фильтрации на основе мандатных меток в сетевых пакетах
- Графический интерфейс централизованного управления МЭ

Фильтрация сетевых пакетов на уровне прикладных протоколов

Для фильтрации на основе прикладных протоколов используется технология Deep Packet Inspection (DPI). В отличие от стандартных межсетевых экранов, DPI анализирует не только заголовки сетевых пакетов, но и полное содержимое трафика на верхнем уровне сетевой модели OSI.



В основе DPI лежит статистический анализ данных пакетов. На основе частоты встречи определенных символов, длины пакета и других параметров создается шаблон для того или иного прикладного протокола. Сетевые пакеты, удовлетворяющие шаблону, подвергаются дальнейшей фильтрации согласно заданным правилам.

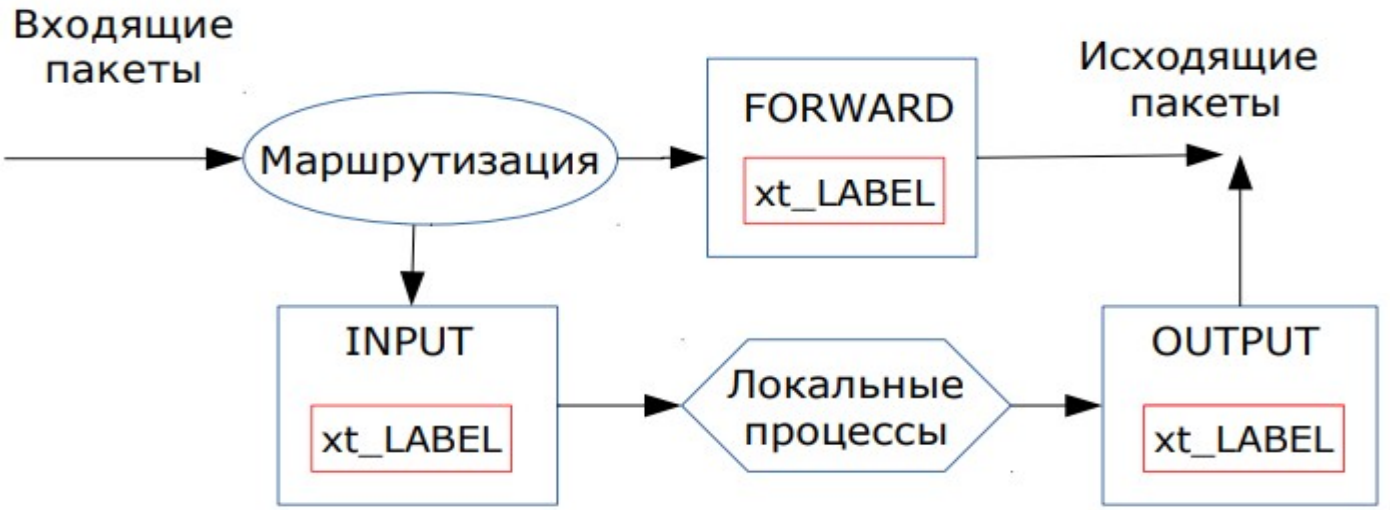
В рамках работы для ОПО «Эльбрус-Д» был портирован opensource модуль ndpi, реализующий технологию DPI для межсетевого экрана Netfilter. Ndpi поддерживает такие протоколы, как HTTP, DNS, NTP, FTP и др.

Фильтрация на основе мандатных меток

В операционной системе «Эльбрус-Д» реализована мандатная модель разграничения доступа в качестве модуля Elmac.

В целях контроля доступа пользователей к сетевым ресурсам в дополнительный заголовок IPv4 добавляется мандатная метка: уровень и категория доступа.

В рамках работы был реализован модуль фильтрации сетевых пакетов на основе мандатных меток xt_LABEL. Он производит разбор заголовков сетевых пакетов и сравнивает метку пакета с меткой, заданной в правилах фильтрации. По итогам сравнения принимается решение о пропуске либо блокировке пакета.



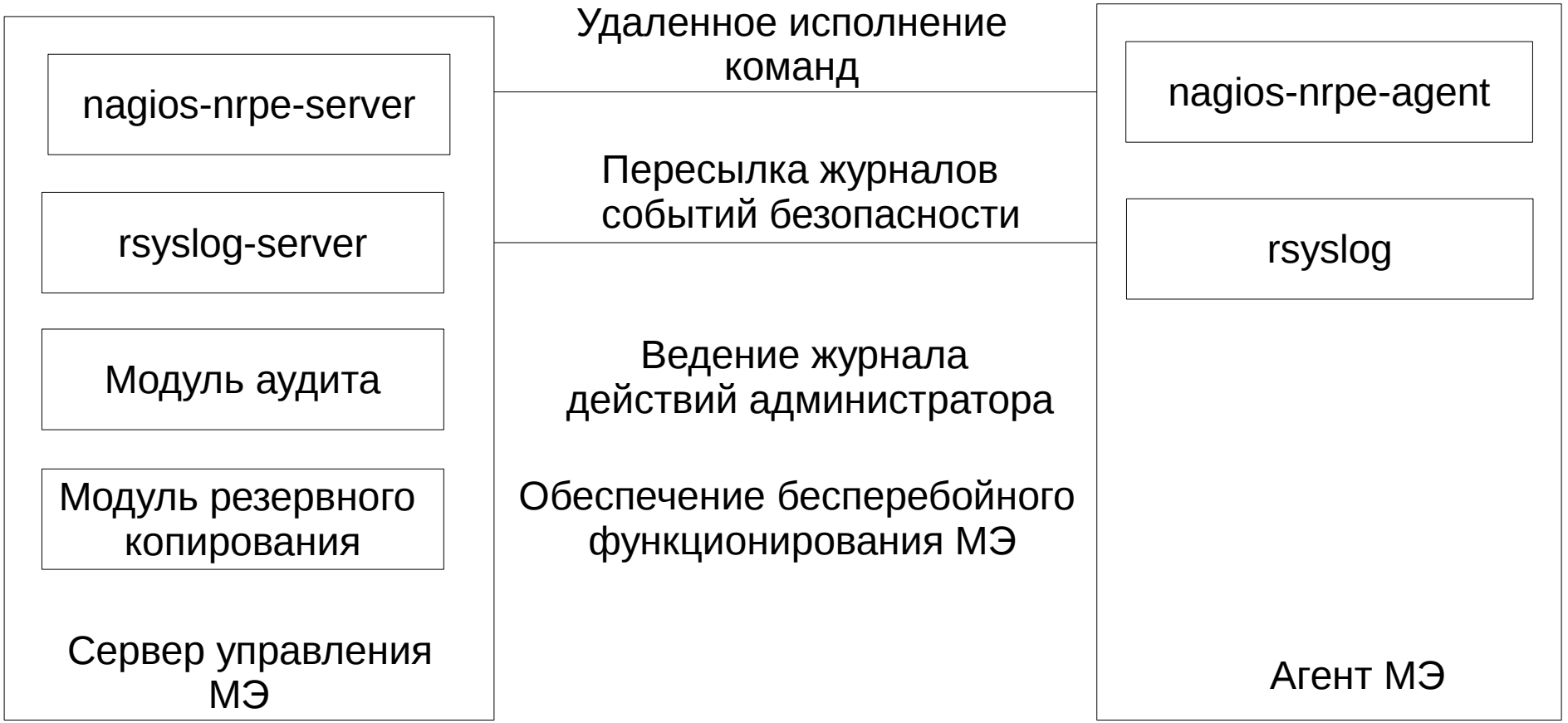
Централизованное управление межсетевым экраном

Централизованное управление МЭ – ПО для удаленного управления правилами фильтрации на межсетевых экранах, установленных на АРМ в компьютерной сети.

**АРМ – автоматизированное рабочее место*

Общая структура реализации

В качестве инструмента разработки использована библиотека QT5, включенная в состав ОПО «Эльбрус-Д». ЦУ состоит из двух компонентов – сервер управления, откуда посылаются управляющие команды и агент, исполняющий эти команды на узле.



Реализованные функции графического интерфейса МЭ

Название функции в GUI	Методы QT	Требование ФСТЭК
Применение правил Сброс правил Список активных правил Создание набора правил	apply_rules() reset_rules() get_rules() set_rules()	Управление функциями безопасности
События безопасности Журнал МЭ	events() journ()	Регистрация событий безопасности
Создание резервной копии Восстановление из резервной копии	create_backup() restore_backup()	Бесперебойное функционирование и восстановление
Авторизация	login_dialog()	Авторизация

Результаты

- Модуль фильтрации на основе прикладных протоколов ndpi включен в состав дистрибутива «Эльбрус-Д».
- Разработан и включен в дистрибутив «Эльбрус-Д» модуль фильтрации мандатных меток в сетевых пакетах.
- Разработана утилита централизованного управления межсетевым экраном, реализующая требования ФСТЭК.
- Разработанный межсетевой экран готовится к сертификации в системе ФСТЭК.