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

Выпускная квалификационная работа бакалавра

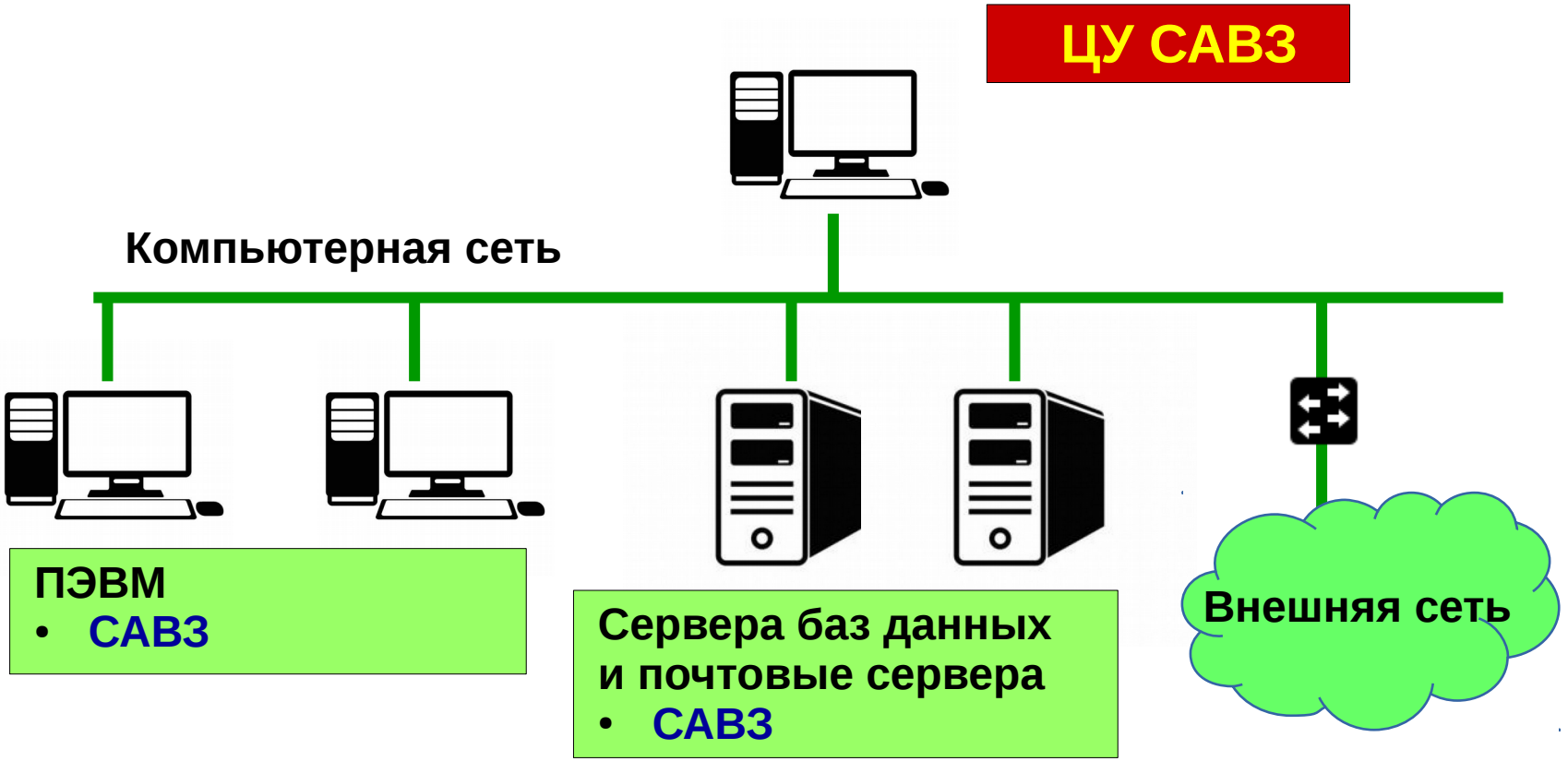
РАЗРАБОТКА СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ АНТИВИРУСОМ КАСПЕРСКОГО В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФСТЭК ДЛЯ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ «ЭЛЬБРУС»

Студент: Якимчиков М.В., 413 группа
Научный руководитель: к.т.н. Морозов Ю.В.

Система централизованного управления антивирусом

Система антивирусной защиты **(САВЗ) — антивирус.**

Система централизованного управления (ЦУ) САВЗ — ПО для **управления** и **мониторинга САВЗ,** установленных на ЭВМ в компьютерной сети.



Цель работы

Разработка системы централизованного управления для САВЗ Касперского

Требования заказчика:
1) Графический интерфейс
2) Среда **ОПО «Эльбрус»** на СВТ, построенных на базе процессоров **Эльбрус 4С, 8С, 1С+**

Требования ФСТЭК:
1) Уведомление об обнаруженных вирусах
2) Установка обновлений антивирусных баз
3) Управление функциями безопасности САВЗ
4) Авторизация в системе
5) Ведение аудита
6) Получение журналов событий САВЗ
7) Удалённая установка САВЗ

Интерфейс взаимодействия с САВЗ

Объектом управления системы ЦУ является **Антивирус Лаборатории Касперского 8.0 для Linux File Server** (далее САВЗ)**.**

Предоставляемые интерфейсы взаимодействия с САВЗ:

1) **Командая строка (SSH)**
2) **Web Management Console (WM Console)** - веб-интерфейс для удалённого управления (**HTTP**)

*САВЗ Касперского для связи с WM Console использует встроенный HTTP сервер. Данные между ними передаются **по внутреннему протоколу взаимодействия в формате JSON-сообщений*** *поверх HTTP*.

Достоинства:

- Удобство разбора JSON (множество библиотек)
- Возможность воспроизведения пользовательского интерфейса WM Console для пользовательского интерфейса ЦУ САВЗ

- Интерфейс **WM Console** предоставляет управление всем функционалом САВЗ, поэтому **было решено использовать его для взаимодейсвтия между ЦУ и САВЗ**

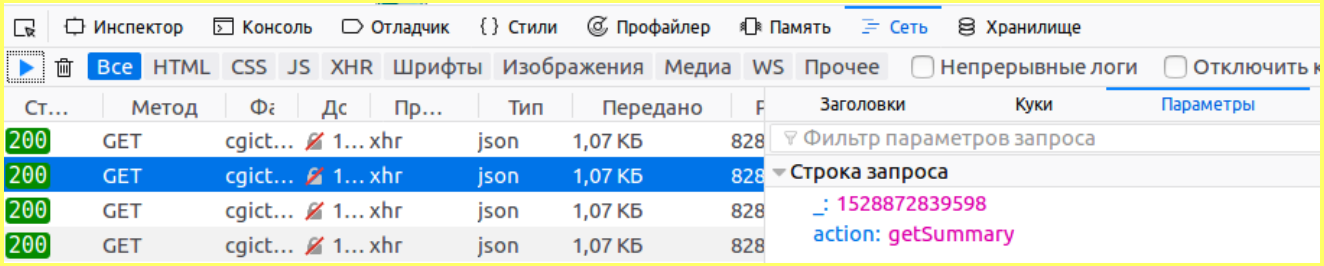
*** JSON - текстовый формат обмена данными**

Внутренний протокол взаимодействия с CAB3 Касперского

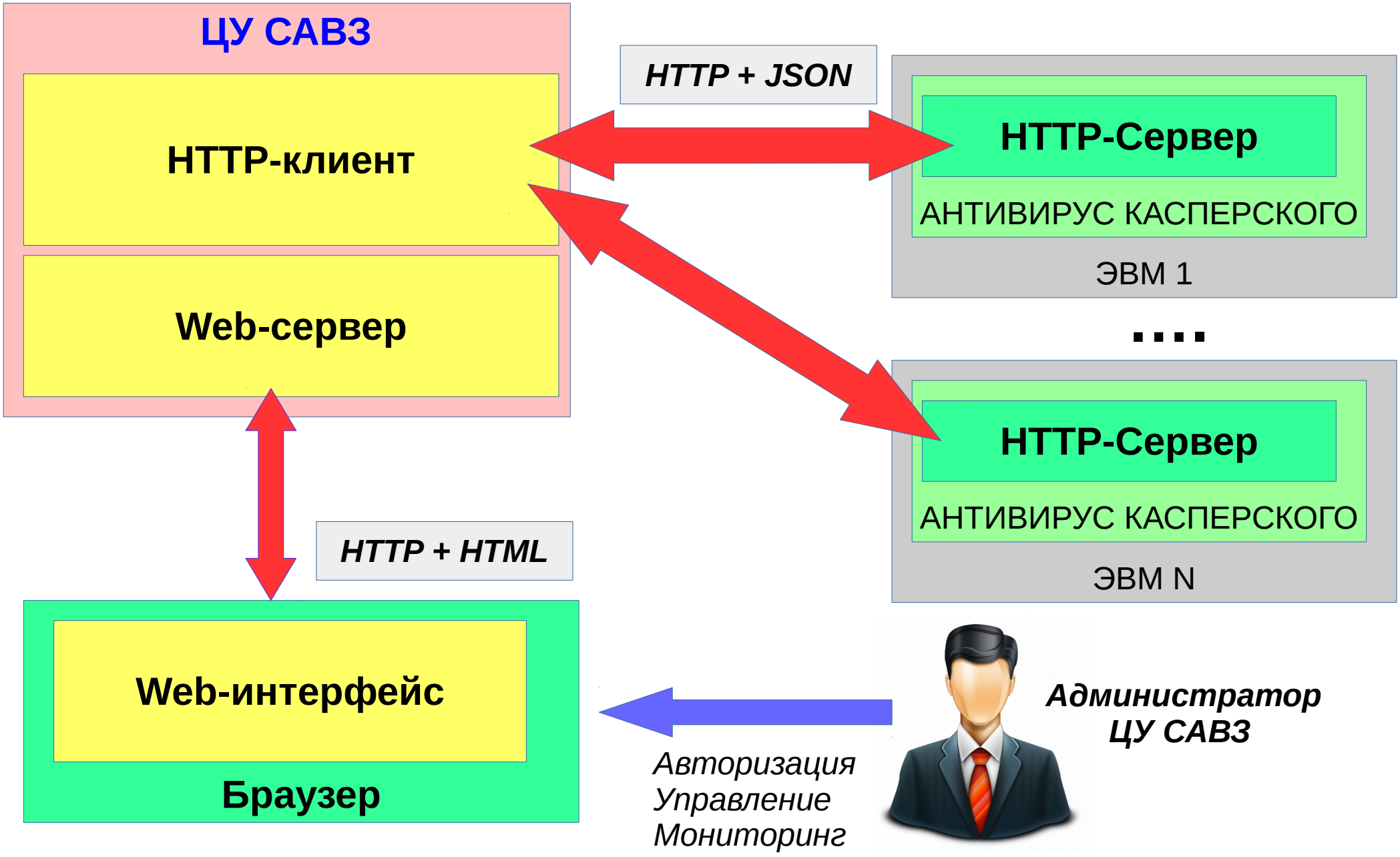
Внутренний протокол общения между сервером Касперского и WM Console не документирован, поэтому требовалось изучить механизм его работы

1. изучение исходного JS кода программы WM Console

2. анализ HTML запросов и полученных JSON с помощью браузера



ЦУ САВЗ на основе HTTP-клиента



Инструменты программной реализации

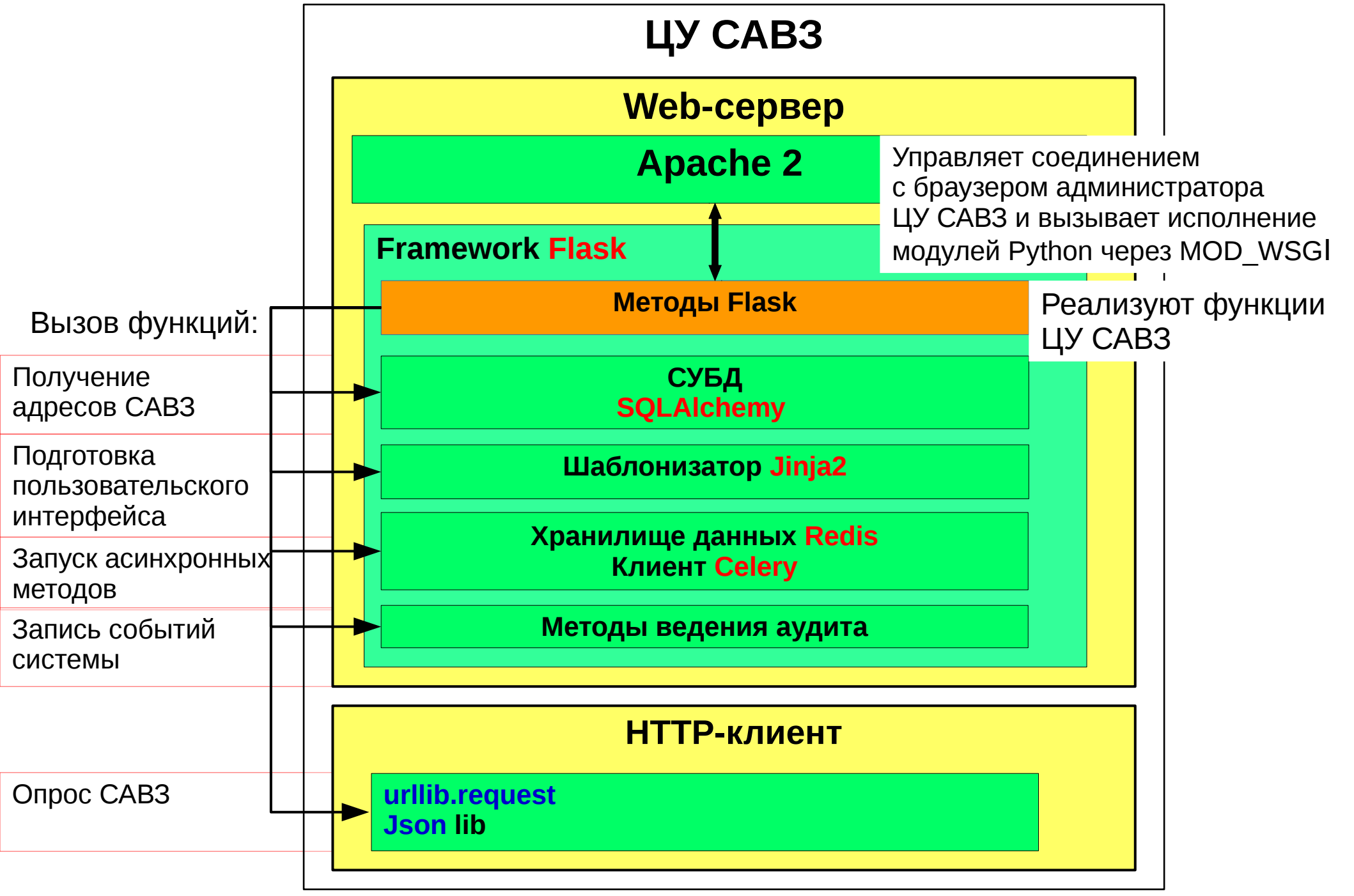
Использован скриптовый язык Python, поддержка которого включена в **ОПО «Эльбрус».** Библиотеки, не входящие в стандартную поставку Python 3.4, проверены на работоспособность в целевой среде.

Библиотеки: Внешние Стандартные

Модули Python

Framework Flask	Реализует подход к созданию Web-приложения.
Методы Flask	Обрабатывают HTTP-запросы и подготавливают HTTP-ответы.
Шаблонизатор Jinja2	Подготавливает **графический web-интерфейс** для администратора ЦУ САВЗ.
Key-value хранилище Redis **Клиент Celery**	Используются для асинхронного запуска методов HTTP-клиента.
urllib.request **Json lib**	Опрашивает САВЗ Касперского по HTTP и передает полученные JSON в виде Python-словарей методам Flask.
База данных SQLAlchemy	ORM Python-БД. Хранит информацию о подключенных САВЗ.

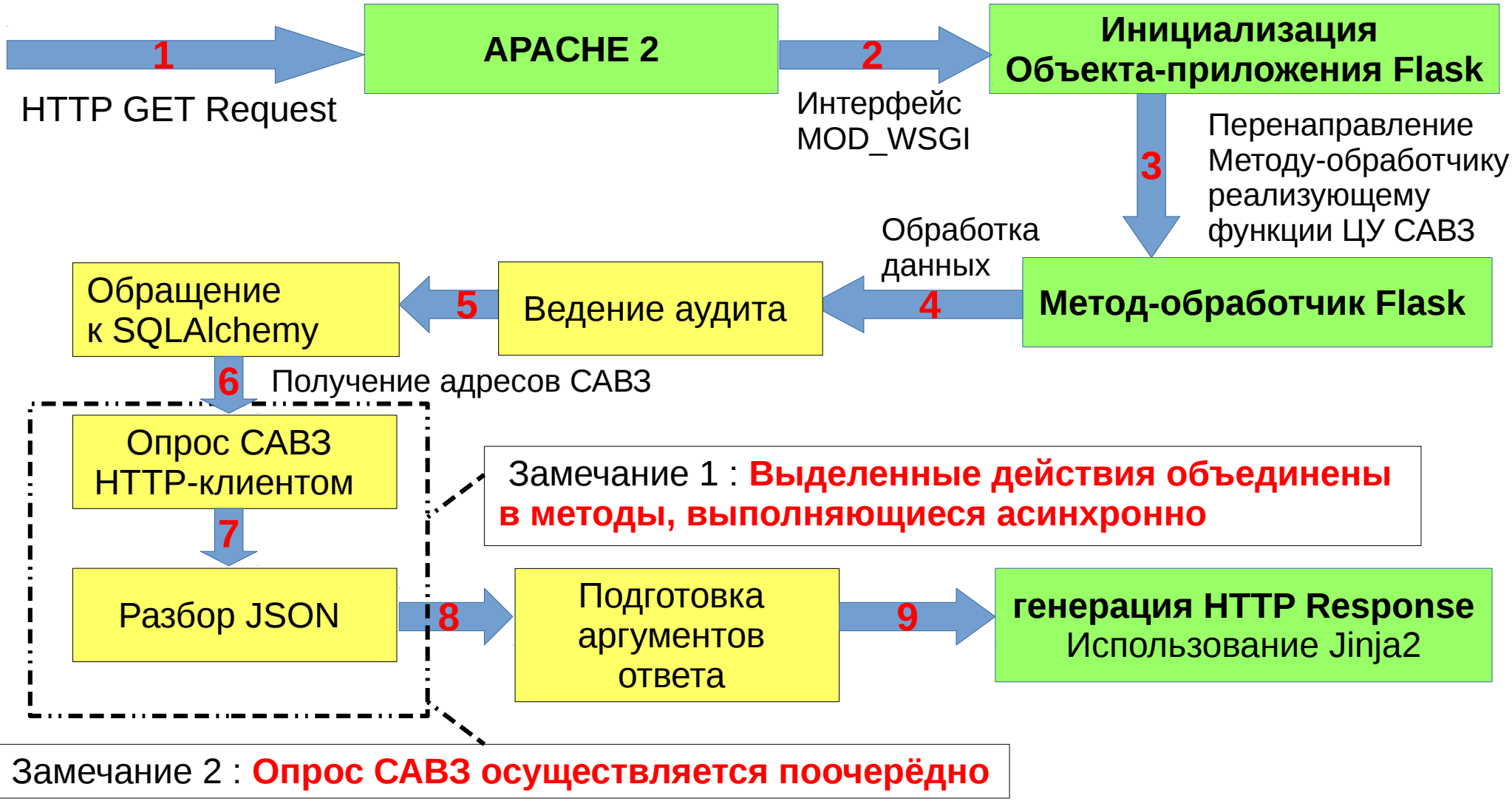
Структура реализации ЦУ САВЗ



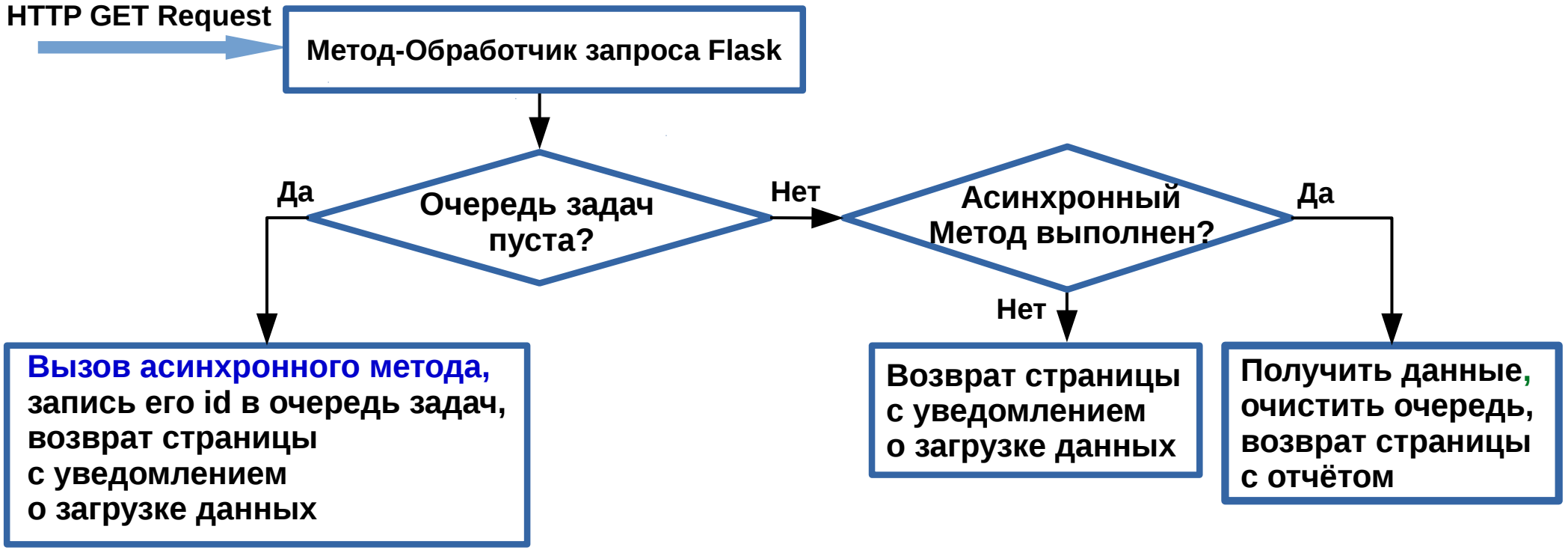
Реализованные функции ЦУ САВЗ

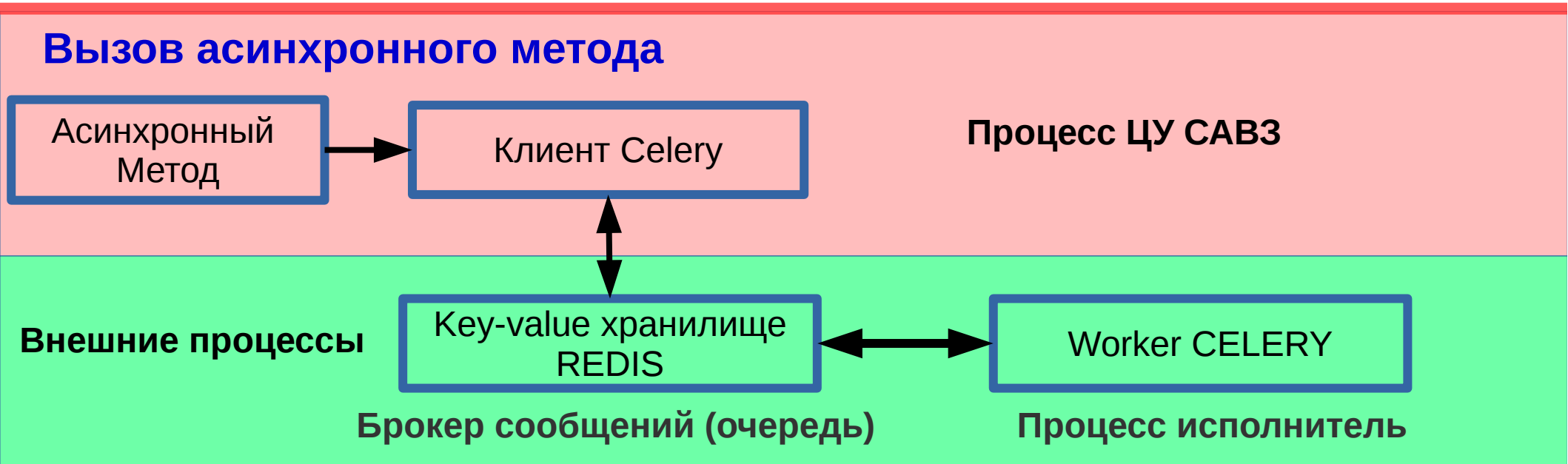
Имя в GUI	Методы Flask	Требование ФСТЭК
Обновление	update()	Установка обновлений антивирусных баз
Постоянная защита	rt_protection()	Управление функциями безопасности САВЗ
Обзор	main()	
Проверка по требованию	on_demand_scan()	
Карантин	quarantine()	
Управление окружением	env_management()	
Журнал	logs()	Получение журналов событий САВЗ
Уведомления	smtp()	Уведомление об обнаруженных вирусах
administrator Выйти	login()	Авторизация в системе
Не треб. GUI	Внутри методов	Ведение аудита
Управление задачами	task_management()	Удалённая установка САВЗ

Алгоритм обработки запроса администратора ЦУ САВЗ



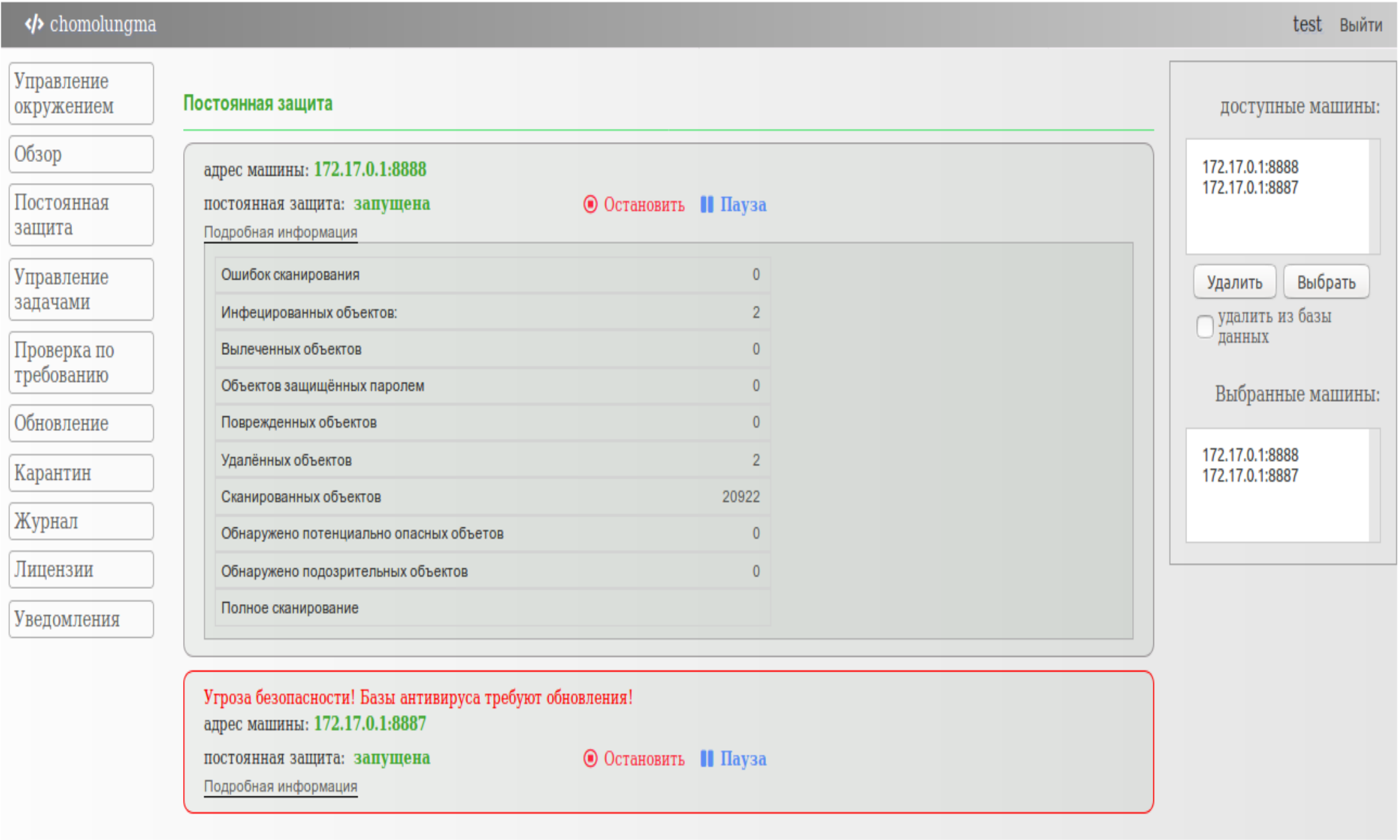
Алгоритм работы асинхронных методов





Результаты

- Изучен принцип работы сервера Касперского и интерфейсов взаимодействия с ним
- Разработана программа ЦУ САВЗ Касперского, реализующая требования ФСТЭК РД и заказчика.
- Проверена работоспособность и выдана рекомендация по включению использованных внешних библиотек Python, а также ПО Redis и Celery в ОПО «Эльбрус».
- Подход, примененный для решения задачи, может быть обобщен на создание систем ЦУ для других САВЗ (например Dr. Web).


chomolungma
test
Выйти
Управление окружением
Обзор
Постоянная защита
Управление задачами
Проверка по требованию
Обновление
Карантин
Журнал
Лицензии
Уведомления
Постоянная защита
адрес машины: 172.17.0.1:8888
постоянная защита: запущена
Остановить
Пауза
Подробная информация
Ошибок сканирования 0
Инфецированных объектов: 2
Вылеченных объектов 0
Объектов защищённых паролем 0
Поврежденных объектов 0
Удалённых объектов 2
Сканированных объектов 20922
Обнаружено потенциально опасных объетов 0
Обнаружено подозрительных объектов 0
Полное сканирование
Угроза безопасности! Базы антивируса требуют обновления!
адрес машины: 172.17.0.1:8887
постоянная защита: запущена
Остановить
Пауза
Подробная информация
доступные машины:
172.17.0.1:8888
172.17.0.1:8887
Удалить
Выбрать
удалить из базы данных
Выбранные машины:
172.17.0.1:8888
172.17.0.1:8887