

Программно-аппаратный комплекс контроля активности информационной сети предприятия и обнаружения вторжений

Студент 5 курса ИКБиСП

Группы БАСО-02-13

А.Н. КУЖЕЛЕВ

руководитель – к.т.н. , доцент кафедры

КБ-1 С.И. ЖУРАВЛЕВ


Информационная сеть

технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Каждая ИС обладает следующими свойствами:

- мультимедийностью;
- открытостью;
- интеллектуальностью;
- широкополосностью;
- инвариантностью доступа;
- многооператорностью.



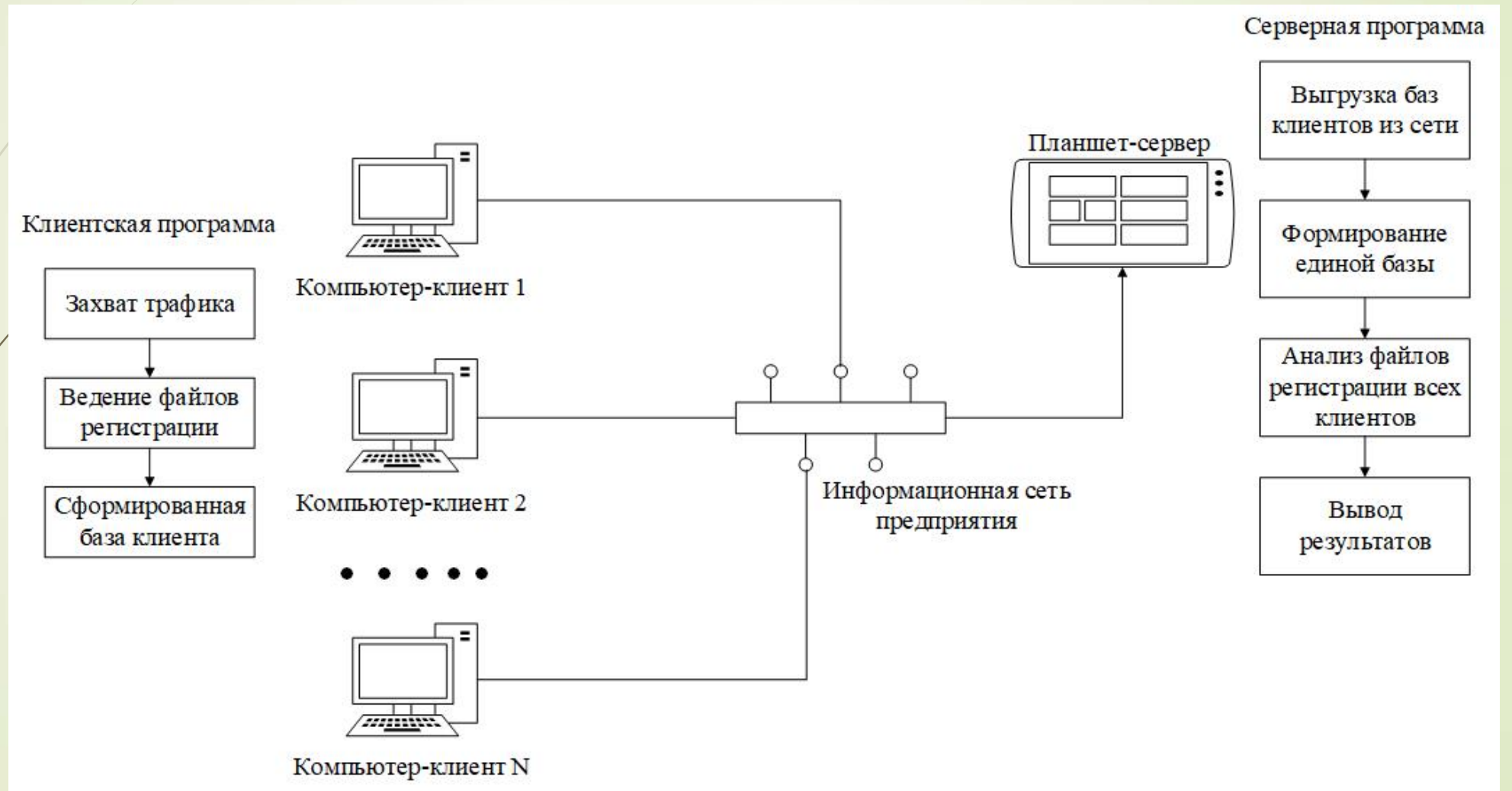


Актуальность проверки ПО в сети определяется необходимостью совершенствования методов и средств мониторинга активности и обнаружения вторжения в распределенные сетевые информационные системы.

Для реализации проверки ПО поставлены и решаются следующие задачи:

- проводится анализ проблематики и необходимости контроля активности в информационной сети;
- проводится анализ характеристик существующих и вновь разрабатываемых комплексов сетевой защиты периметров предприятия;
- описываются информационные сети и особенности протоколов обмена информацией в них.

Архитектура разрабатываемого ПАК



Структура клиента разрабатываемого ПАК

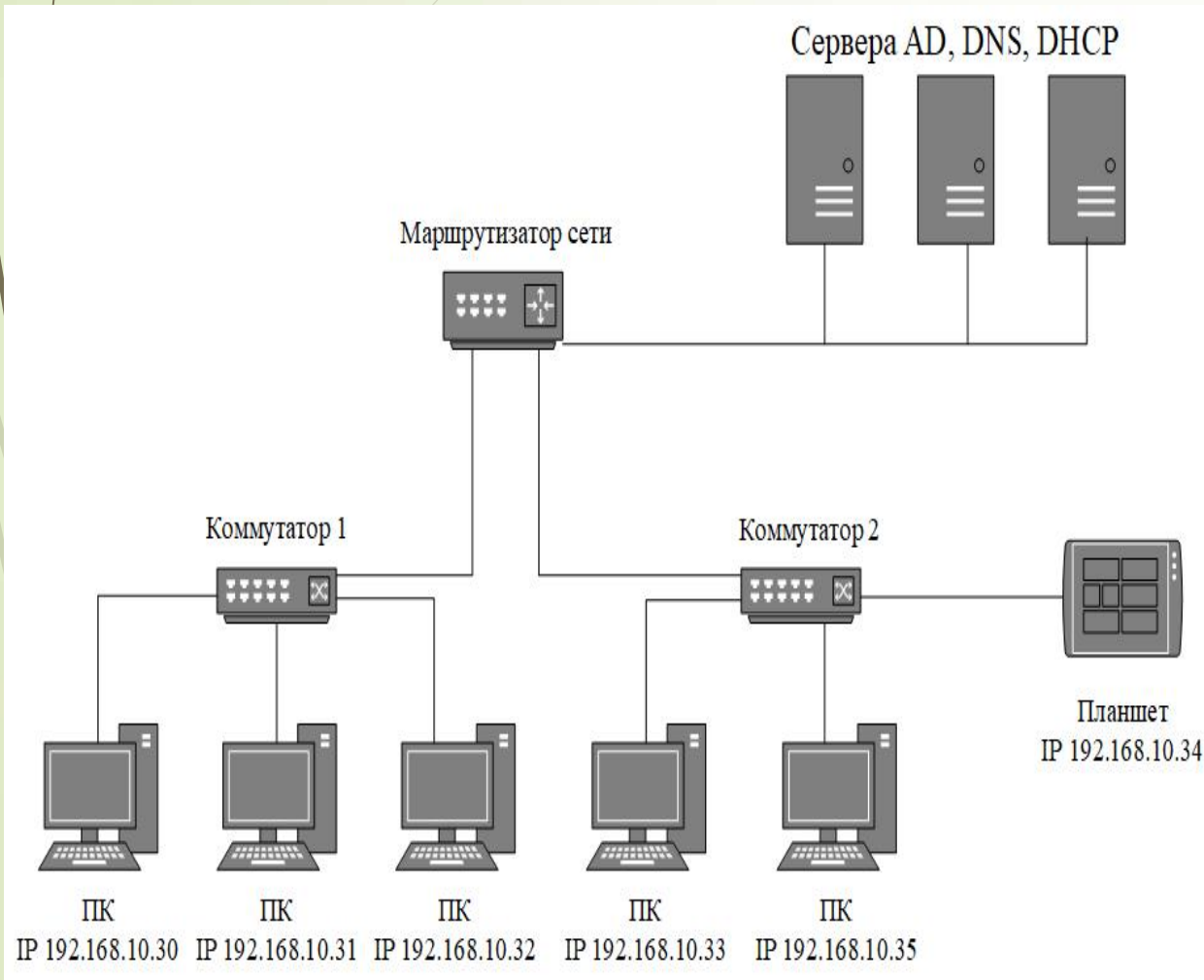


Структура сервера разрабатываемого ПАК



Тестирование программы для ПАК

Макет тестируемой сети



Интерфейс разработанного ПАК

Selector - Enter something
admin1
173.194.222.94
Description
Show

Selector - Enter something
user
Description
Show

```
pi@raspberrypi:~$ sudo apt-cache search scrot
Чтение списков пакетов... Готово
Построение дерева зависимости
Чтение информации о состоянии... Готово
Уже установлен пакет scrot
scrot установлен вручную.
обновлено 0, установлено 0 пакетов, не обновлено.
pi@raspberrypi:~$ scrot
scratch script
scratch2 scriptreplay
scrotch old scrot
screendump
pi@raspberrypi:~$ scrot
pi@raspberrypi:~$ scrot
pi@raspberrypi:~$ scrot
pi@raspberrypi:~$ scrot
```

667 logs found:

Time	Source IP	Destination IP	Timestamp
1	EST [192.168.10.30]	[5.45.59.253]	[2018-04-11 12:26:00]
2	EST [192.168.10.30]	[52.40.133.43]	[2018-04-11 12:26:06]
3	EST [192.168.10.30]	[104.16.41.2]	[2018-04-11 12:26:13]
4	EST [192.168.10.30]	[54.230.14.162]	[2018-04-11 12:26:17]
5	EST [192.168.10.30]	[54.230.14.162]	[2018-04-11 12:26:17]
6	EST [192.168.10.30]	[54.230.14.162]	[2018-04-11 12:26:18]
7	EST [192.168.10.30]	[93.184.220.29]	[2018-04-11 12:26:18]
8	EST [192.168.10.30]	[52.40.133.43]	[2018-04-11 12:26:19]
9	EST [192.168.10.30]	[52.40.133.43]	[2018-04-11 12:26:19]
10	EST [192.168.10.30]	[213.180.204.63]	[2018-04-11 12:26:22]
11	EST [192.168.10.30]	[213.180.204.63]	[2018-04-11 12:26:23]
12	EST [192.168.10.30]	[213.180.204.63]	[2018-04-11 12:26:23]
13	EST [192.168.10.30]	[77.88.55.88]	[2018-04-11 12:26:23]
14	EST [192.168.10.30]	[77.88.55.88]	[2018-04-11 12:26:23]
15	EST [192.168.10.30]	[77.88.55.88]	[2018-04-11 12:26:23]
16	EST [192.168.10.30]	[5.45.205.233]	[2018-04-11 12:26:23]
17	EST [192.168.10.30]	[5.45.205.233]	[2018-04-11 12:26:23]

Target had 1 machine names:
KB1 -> 24 times
Target had 1 different source IPs:
192.168.10.31 -> 24 times
Target had 1 different destination IPs:
173.194.222.94 -> 24 times

Аппаратный модуль ПАК

