



Проектирование системы сбора и корреляции событий информационной безопасности

Дупенко И.С.

Группа: АБ-220

Научный руководитель: Старший преподаватель
кафедры защиты информации Туманов С.А.

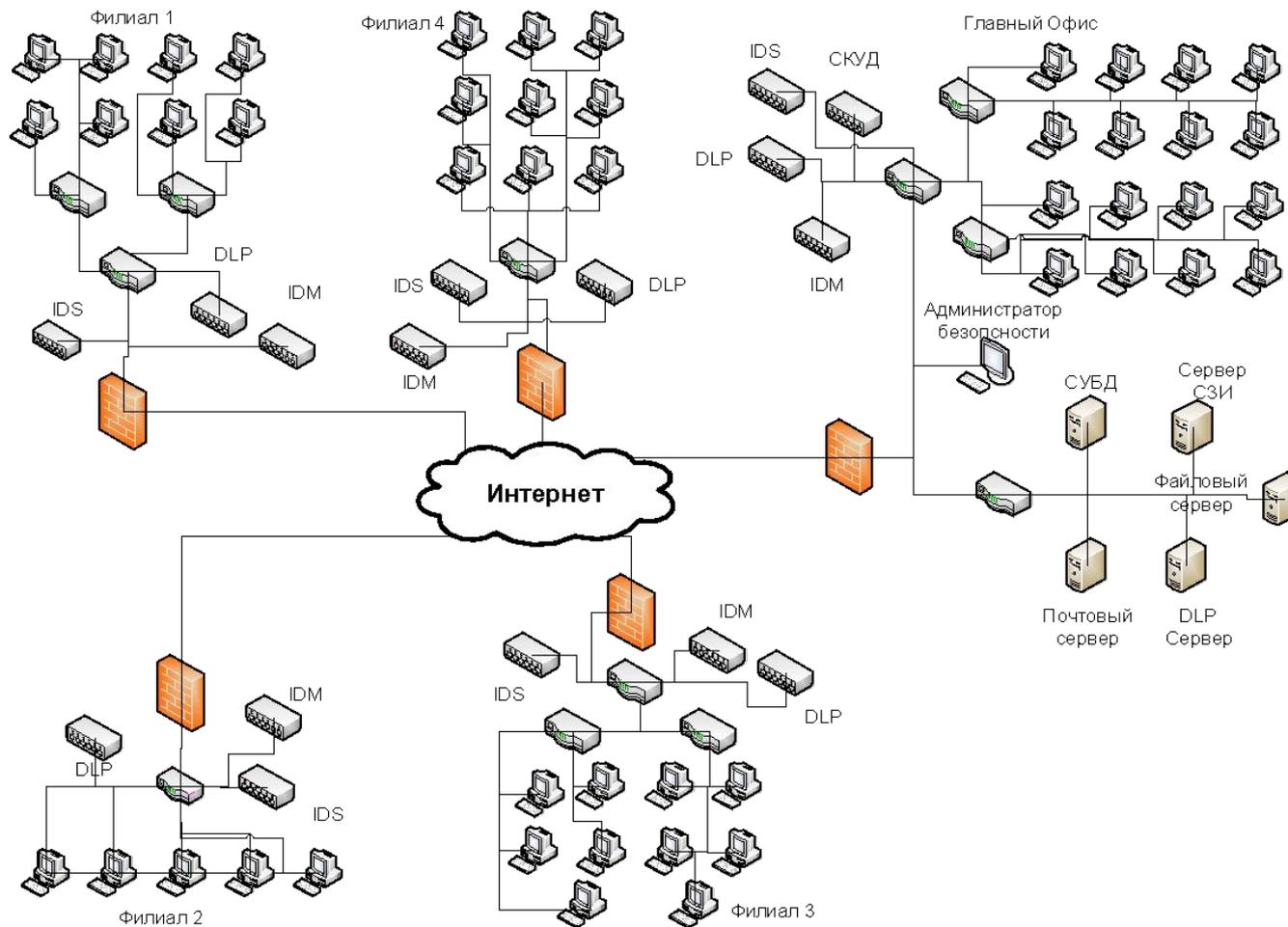
Цель работы:

- проектирование системы сбора и корреляции событий информационной безопасности.

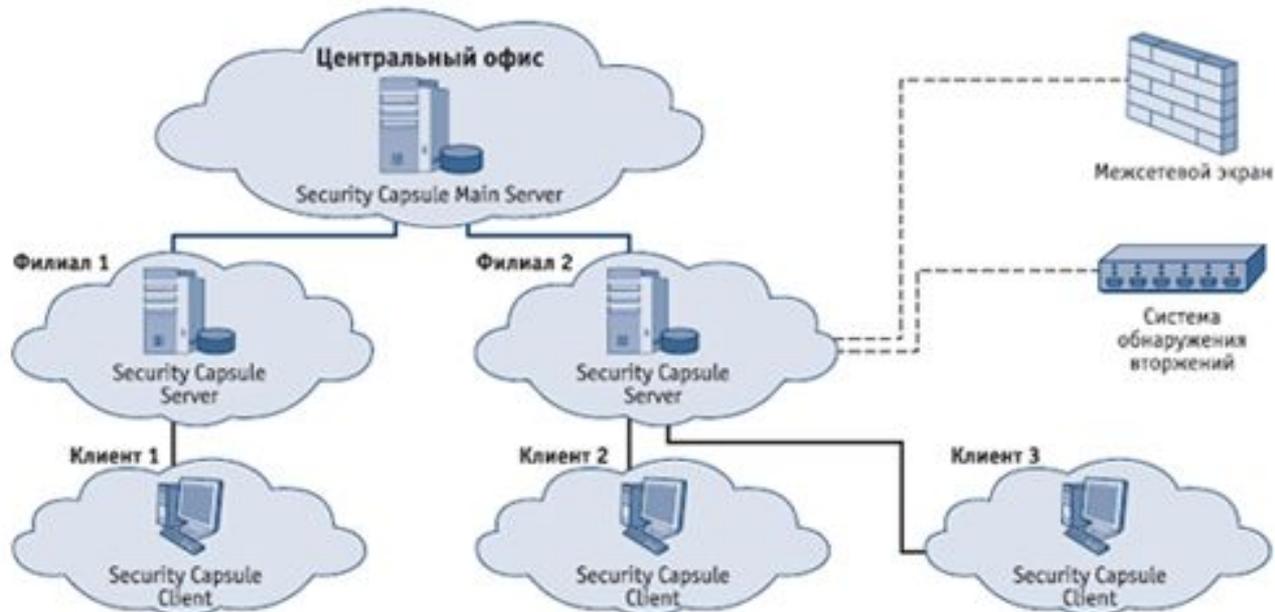
Задачи:

- Изучить рынок SIEM систем и сравнить их по качественным показателям
- Спроектировать сеть, в которую в последствие будет внедрена SIEM система
- Внедрить систему

Сеть до внедрения системы



Проектирование системы



Состав клиента

- ПО «Token PKI Client»
- СЗИ от НСД «Блок-хост Сеть»
- ПО Zlock
- ПО Security Capsule Client
- Оператор АРМ
- ОС Windows

Состав сервера

- SQL база данных
- ПО Security Capsule Server
- Администратор ИБ
- ОС Windows Server

- Клиент
- Интернет
- - - - - Протокол Syslog

Сеть после установки системы

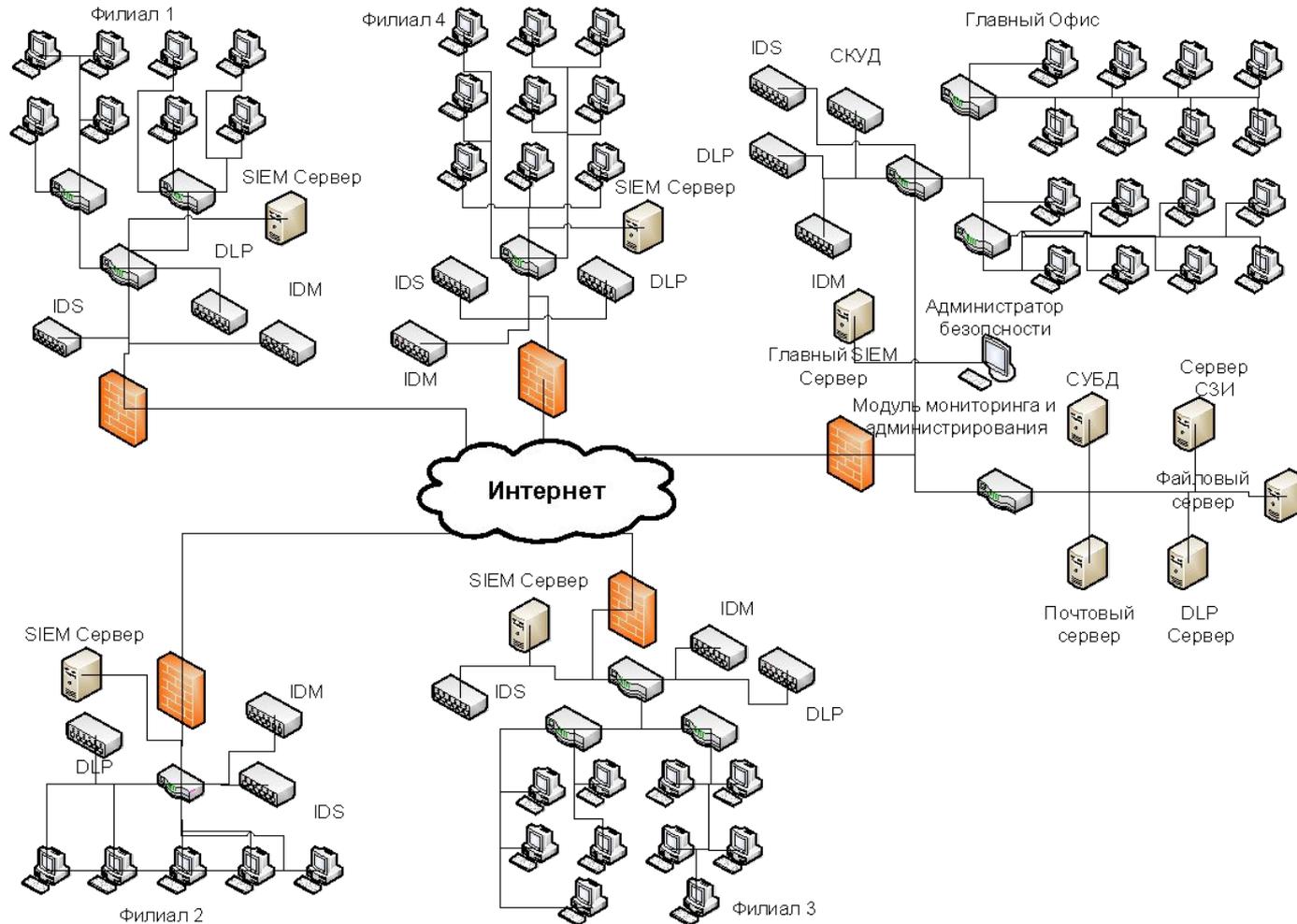
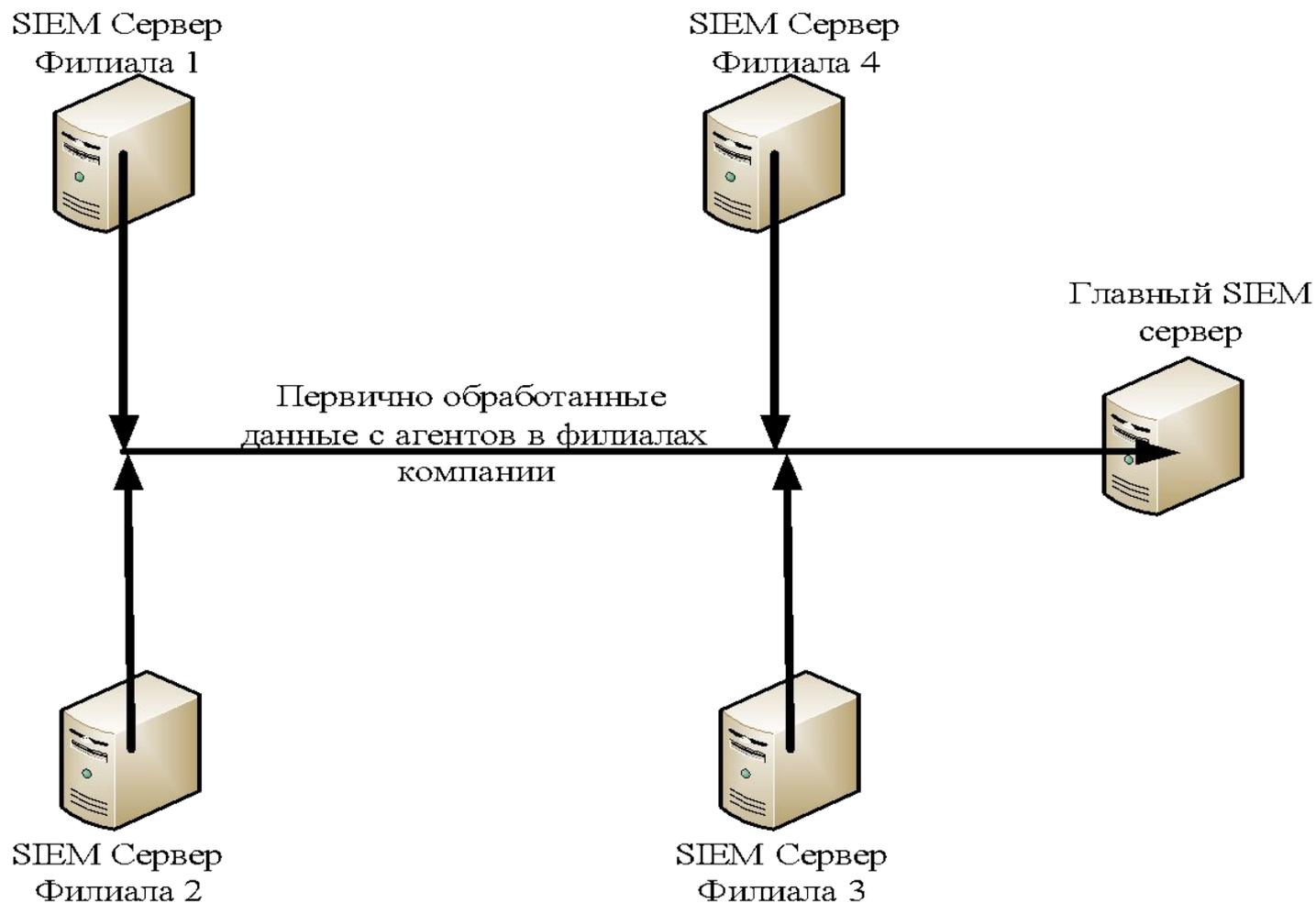


Схема работы спроектированной системы



Заключение

- В данной работе были рассмотрены различные системы сбора и корреляции событий, как лидеры рынка, так и не очень популярные.
- Были сравнены между собой несколько систем
- Спроектирована система сбора и корреляции событий информационной безопасности

Спасибо за внимание!

