

ПРИМЕНЕНИЕ СИСТЕМ МОНИТОРИНГА СОБЫТИЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Выполнил:

студент 5 курса Зенчик Николай

Руководители:

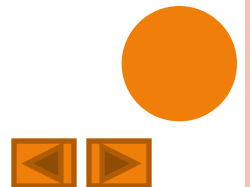
Воротницкий Ю. И.

Позняков А. М.



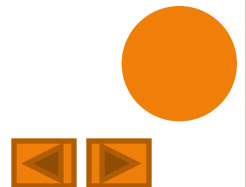
ЦЕЛЬ

- Обеспечить функционирование системы мониторинга в информационной системе организации
- Задачи
 - Произвести анализ рынка систем мониторинга событий
 - Разработать требования к системам мониторинга, описать их структуру
 - Привести конфигурацию системы и источников, необходимую для работы



НЕОБХОДИМОСТЬ ИСПОЛЬЗОВАНИЯ СИСТЕМ МОНИТОРИНГА

- Получение информации о состоянии информационной системы
- Сбор информации об инцидентах безопасности информационной системы
- Возможность оперативного получения информации о происшедших в информационной системе событиях
- Наблюдение за системой при внесении изменений в ее конфигурацию



СОБЫТИЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

□ Классификация сообщений

● По типу источника

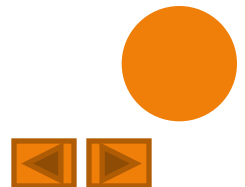
- События от активного сетевого оборудования
- События от операционных систем серверов
- События от пользовательских ПК
- События от программного обеспечения

● По важности источника

- критические
- некритические

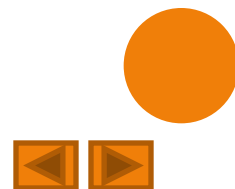
□ Способы получения

- Syslog (RFC5424)
- Чтение из log файла



ОСНОВНЫЕ ТРЕБОВАНИЯ К СИСТЕМАМ МОНИТОРИНГА

- Централизованный сбор сообщений
- Возможность добавления новых источников
- Работа в режиме реального времени
- Анализ сообщений (нормализация и корреляция)
- Наличие системы оповещения



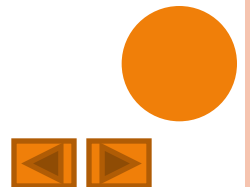
ОБЗОР РЫНКА СИСТЕМ МОНИТОРИНГА

	Arcsight ESM	netForensics Cinxi One	Logzilla
Масштабируемость	Да	Нет	Нет
Мониторинг событий в режиме реального времени	Да	Условно	Да
Анализ сообщений	Да	Да	Нет
Система оповещения	Да	Да	Нет
Расширяемость	Написание собственных модулей для сбора событий	Подключение источников по реализованным в системе протоколам	Поддержка только Syslog источников
Плата за пользование	Высокая	Высокая	Отсутствует

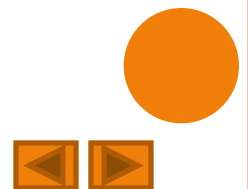
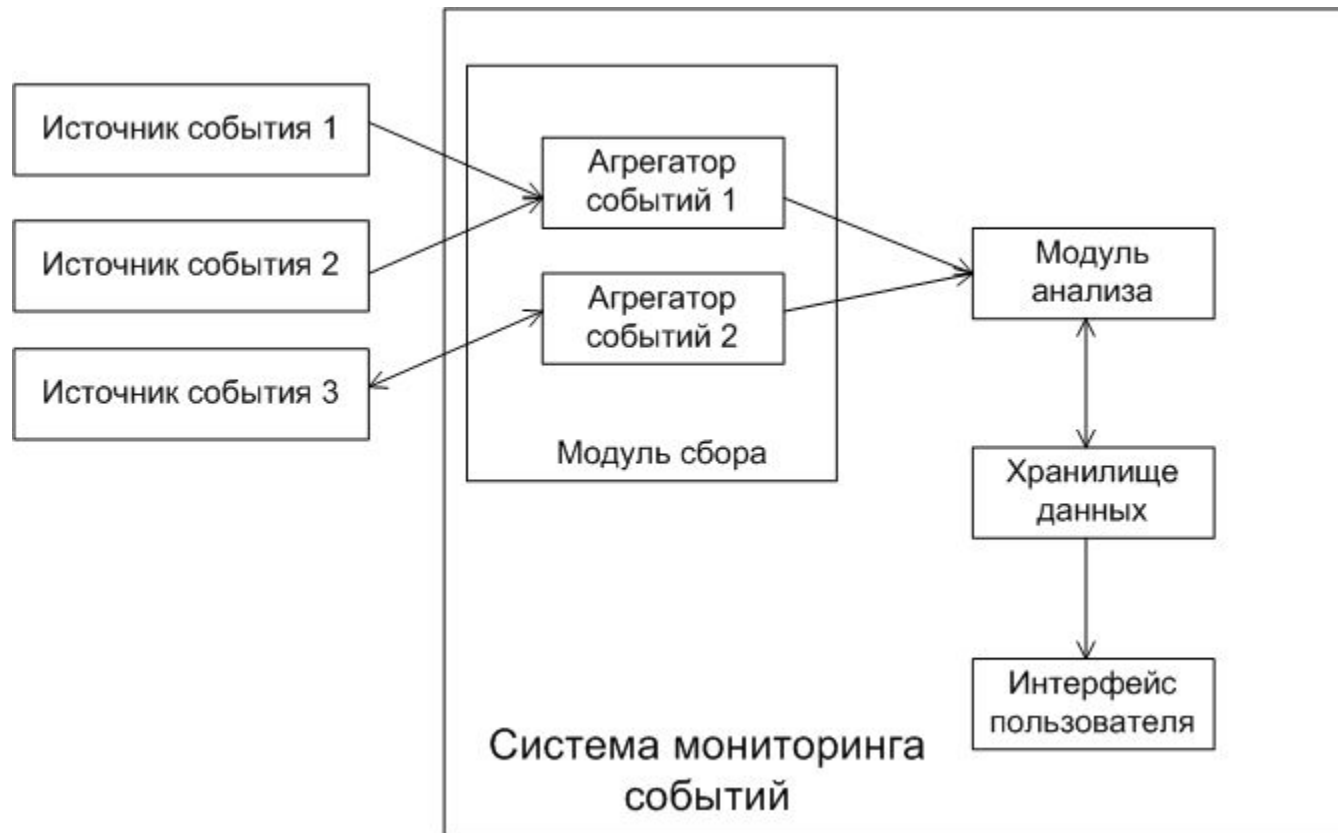


СТРУКТУРА СИСТЕМЫ МОНИТОРИНГА

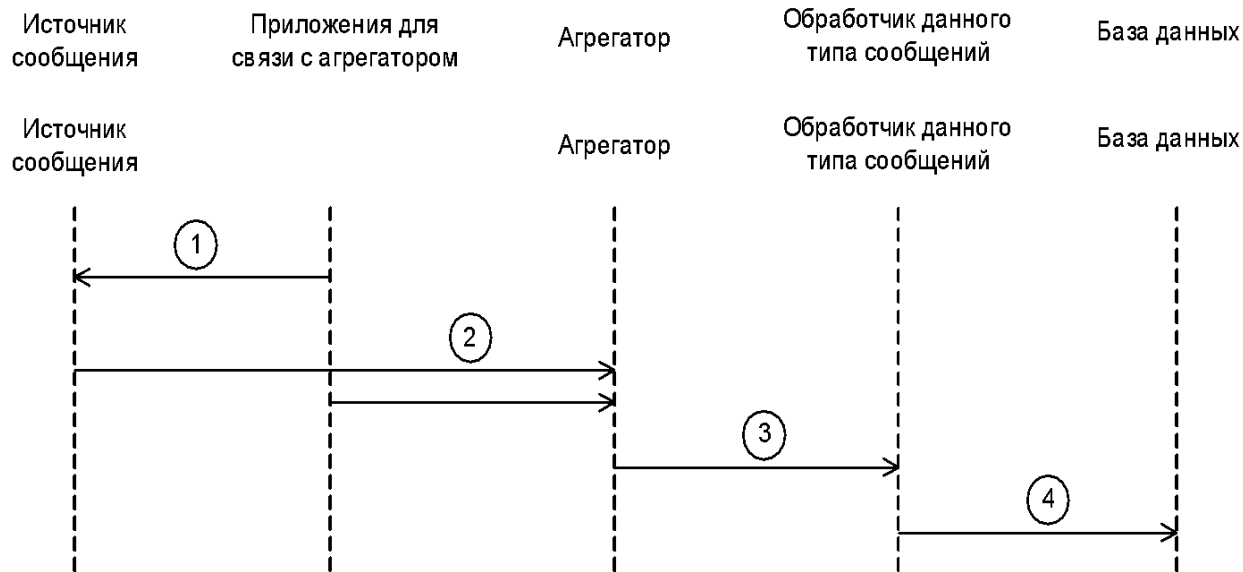
- **Функции системы мониторинга:**
 - Получение сообщений от источников
 - Обработку и анализ сообщения
 - Хранение сообщений
 - Предоставление интерфейса для мониторинга событий
- **Основные роли:**
 - Администратор
 - Оператор



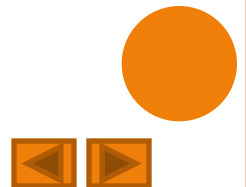
ТИПОВАЯ СТРУКТУРА СИСТЕМЫ МОНИТОРИНГА



ПРОЦЕСС ПОЛУЧЕНИЯ И ОБРАБОТКИ СОБЫТИЯ

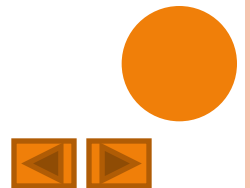


- 1 – генерация сообщения источниками и в случае необходимости чтение его приложением для связи со агрегатором;
- 2 – передача сообщения соответствующему данному типу источника агрегатору;
- 3 – передача сообщения обработчику данного типа сообщений;
- 4 – запись обработанного сообщения в базу данных.



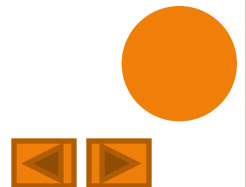
ПОДКЛЮЧЕНИЕ НОВОГО УСТРОЙСТВА

- Настройка источника сообщений
- Регистрация источника в системе
 - Адрес источника
 - Название
 - Тип
 - Производитель
- Обеспечение доступности на пути от источника до агрегатора событий
- Тестирование



ЗАКЛЮЧЕНИЕ

- Проведен анализ рынка систем мониторинга и выбрана система Arcsight
- Рассмотрена общая схема функционирования систем мониторинга
- Описана процедура подключения источников следующего типа к системе Arcsight:
 - Активное сетевое оборудование (Syslog)
 - Операционные системы семейства Unix, Solaris, Windows





СПАСИБО ЗА ВНИМАНИЕ

