Лабораторная работа №2

«Развертывание Infowatch Traffic Monitor 6 и Infowatch Device Monitor»

Цель работы – получение профессиональных компетенций по этапам развертывания автоматизированной системы IW TM 6 и модуля IW DM.

1. Содержание технологических этапов выполнения работы.

1. Совместно с тренером рассмотреть и изучить этапы установки системы, а также архитектуру IW TM 6. При развертывании учебного стенда опираться на материалы из базы знаний:

- https://kb.infowatch.com/pages/viewpage.action?pageId=125533217 (установка IW TM 6)
- https://kb.infowatch.com/pages/viewpage.action?pageId=125533308 (установка IW DM)

2. Установка системы Red Hat Enterprise Linux (IW TM 6 Enterprice в режиме «все в одном»):

- Выбор базы данных;
- выбор режима установки;
- выбор часового пояса;
- установка пароля суперпользователя Системы;
- выбор способа разбиения дискового пространства;
- настройка сети;
- настройка синхронизации времени (NTP-server);
- настройка локализации;
- настройка автоматического удаления событий из БД;
- завершение установки.

3. Установка InfoWatch Device Monitor:

- Установка серверной части;
- установка агента.

2. Контрольные вопросы.

1. Перечислите отличия IW TM 6 Enterprice от IW TM 6 Standart.
2. В каких случаях рекомендуется отдельная установка сервера TM и сервера базы данных?
3. К какому внутреннему формату приводятся объекты в системе IW TM 6?
4. Какие СУБД поддерживаются системой IW TM 6?
5. За прием каких данных отвечают компоненты sniffer и proxy?
6. Какая компонента системы IW TM 6 извлекает текст из полученного объекта?

7. Какая компонента системы IW TM 6 отвечает за запуск технологий анализа?

8. В какой файл прописываются политики информационной безопасности?

9. Для чего в системе используется формат 2liro?

10. Для чего используется связка компонент системы SMTPD и Deliverd?