Система анализа и мониторинга состояния ИБ DATAPK

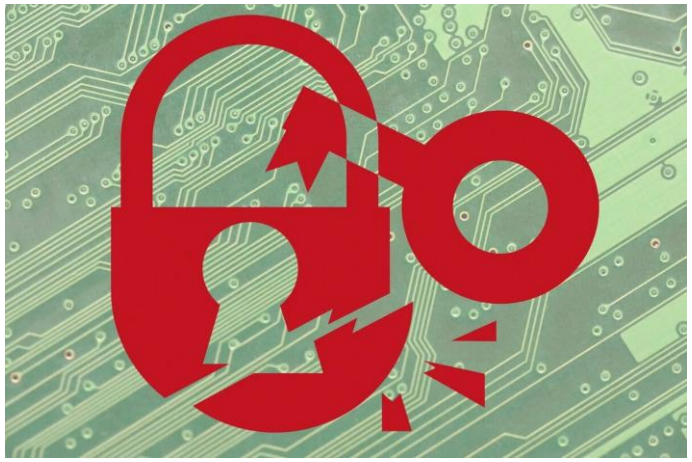
Тема 5. Настройка проверок на уязвимости и соответствие требованиям информационной безопасности.

udv|group

Общие сведения

Уязвимости:

1. ошибки в коде, снижающие уровень безопасности в системе
2. ошибки в настройках / недостаточно безопасная конфигурация (снижают безопасность сильнее, чем (1))



Режимы сканирования:

- аудит (подключение к активу, сбор необходимых данных, интерпретация) – используется в DATAPK
- pentest – попытка в некотором виде проэксплуатировать уязвимость – часто запрещено в АСУ ТП, отсутствует в DATAPK

Обычно (1) устраняется обновлением ПО, что в технологических сетях зачастую затруднительно и не всегда возможно в принципе (работа техпроцесса приоритетнее / надо тестировать обновления, не всегда АСУ ТП на вендорской поддержке / совместимы с современными ОС и пр.)

А вот (2) – это необходимая гигиена, которая позволит существующими средствами сильно снизить поверхность атаки (это не отменяет тестирования на совместимость, но в реализации обычно проще)

Поиск уязвимостей в DATAPK

Модуль Configuration Management (CM)

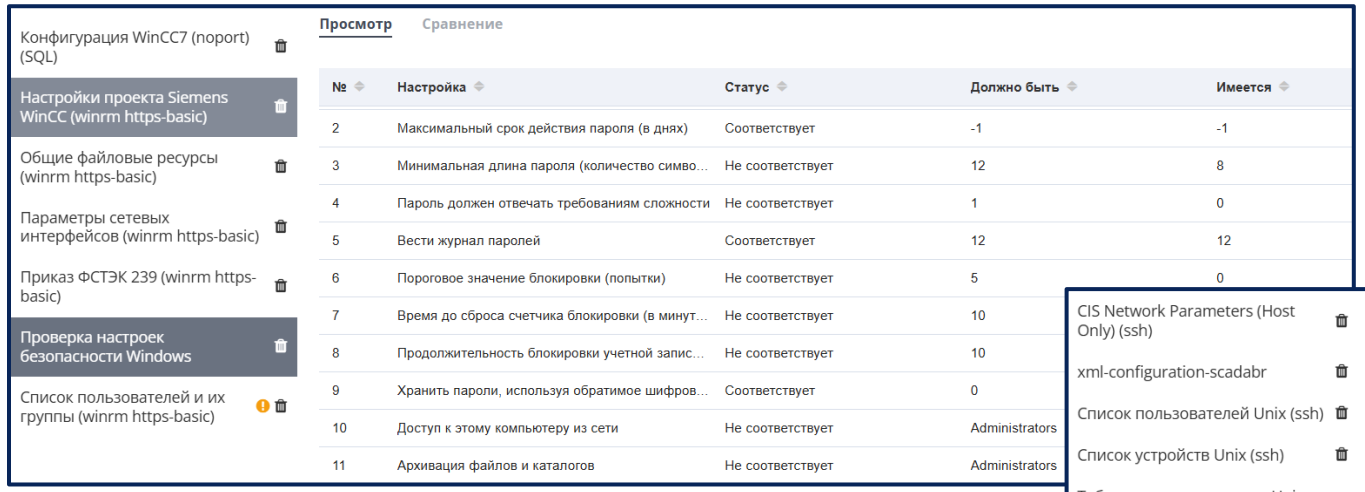
- сбор конфигураций + проверка на соответствие заданным настройкам (можно корректировать под внутренние регламенты);
- сканеры с типом «Версия ОС» и «Установленное ПО» - их результаты используются для поиска уязвимостей;
- сканеры сбора для сбора OVAL-объектов

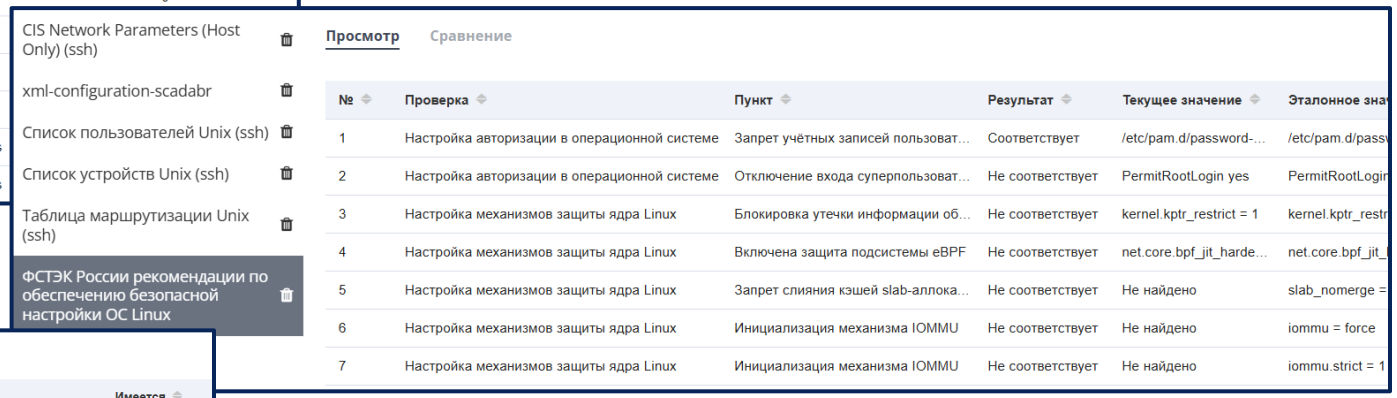
Модуль Vulnerability Management (VM)

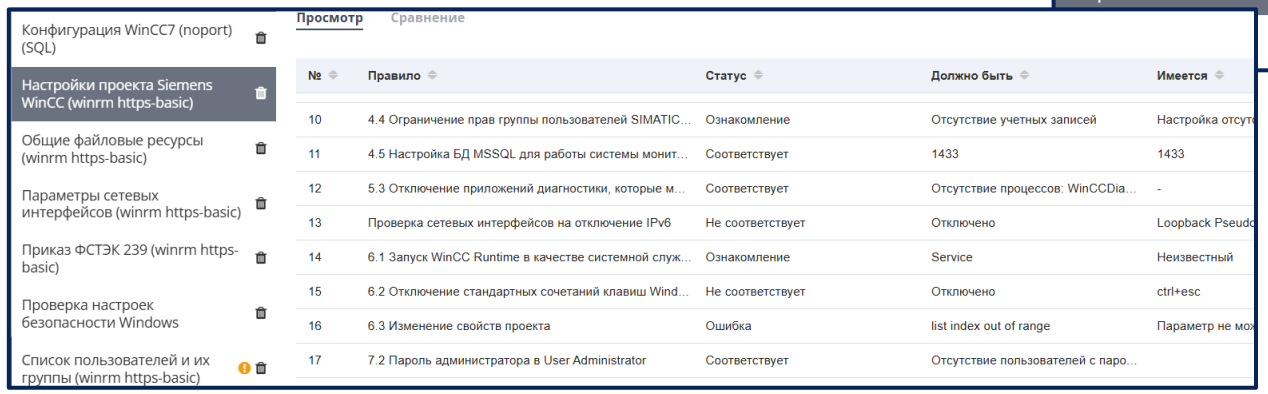
- **OVAL** – открытый стандарт описания состояния активов, есть базы CIS, БДУ ФСТЭК России, но инструмент сбора информации с активов имеет существенные ограничения (обязательно опрашивать актив здесь и сейчас, много запросов в сторону актива, не поддерживаются ПЛК и пр.), в ближайшее время планируется к исключению из DATAPK (в курсе не рассматривается). Базы поставляются производителем DATAPK.
- **CVE2CPE** – альтернативный механизм – с помощью сканеров сбора типа «Версия ОС» и «Установленное ПО» собирается информация с активов, преобразуется в CPE (поля Vendor, Product, Version), и осуществляется поиск уязвимостей для этих ОС/прошивок/ПО по базе CVE и БДУ ФСТЭК России. Поиск можно проводить без обращения к активу «здесь и сейчас» (по ранее собранному слепку, например в режиме ТО). Производитель DATAPK поставляет обновления баз, таблицы маппинга (как интерпретировать собранные данные с актива в формат CPE).

CyberLympha®

Проверка настроек безопасности







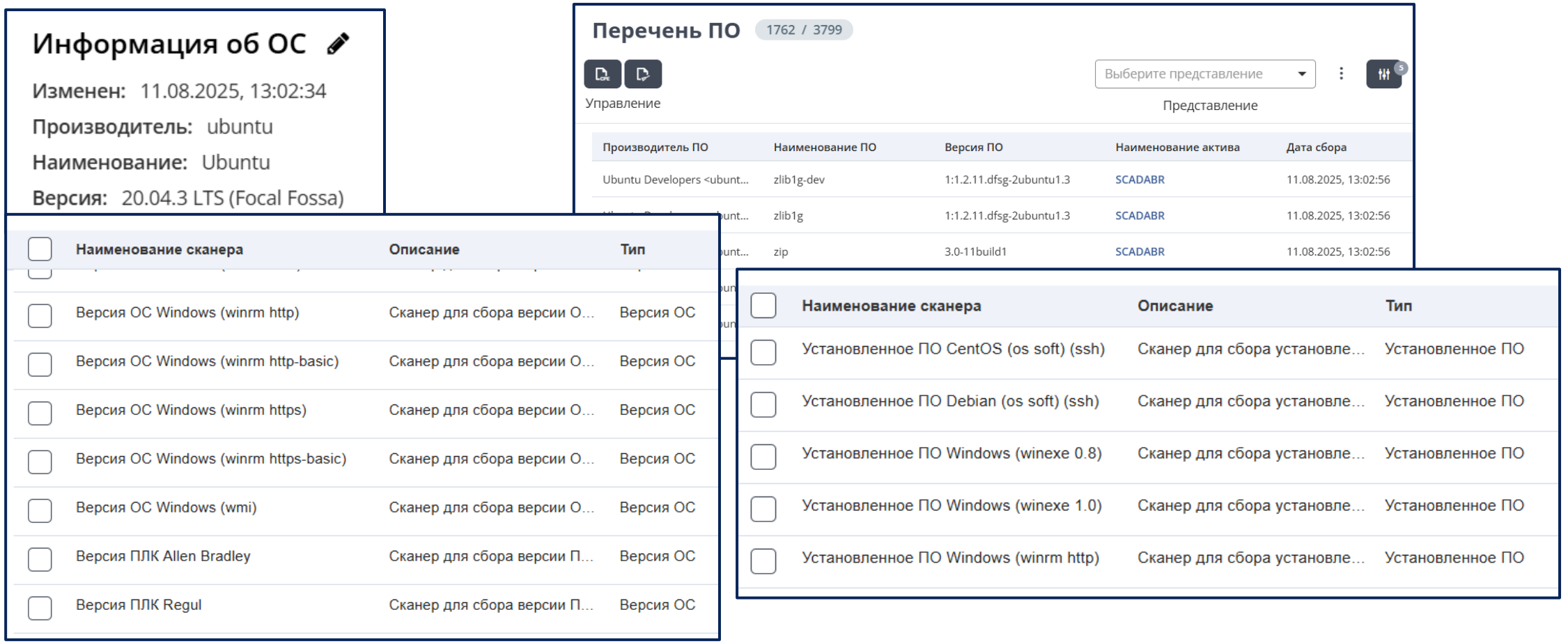
- рекомендации вендоров ОС/ПО
- рекомендации регуляторов
- рекомендации вендоров СЗИ / интеграторов
- стандарты организации

Как реагировать на отклонения:

- *устранять в первую очередь / запланировать устранения в ТО (после тестов на невлияние)*
- *в случае ошибок сбора – скорректировать сканер (воспользоваться рекомендациями из темы 3)*

Поиск уязвимостей (CVE2CPE)

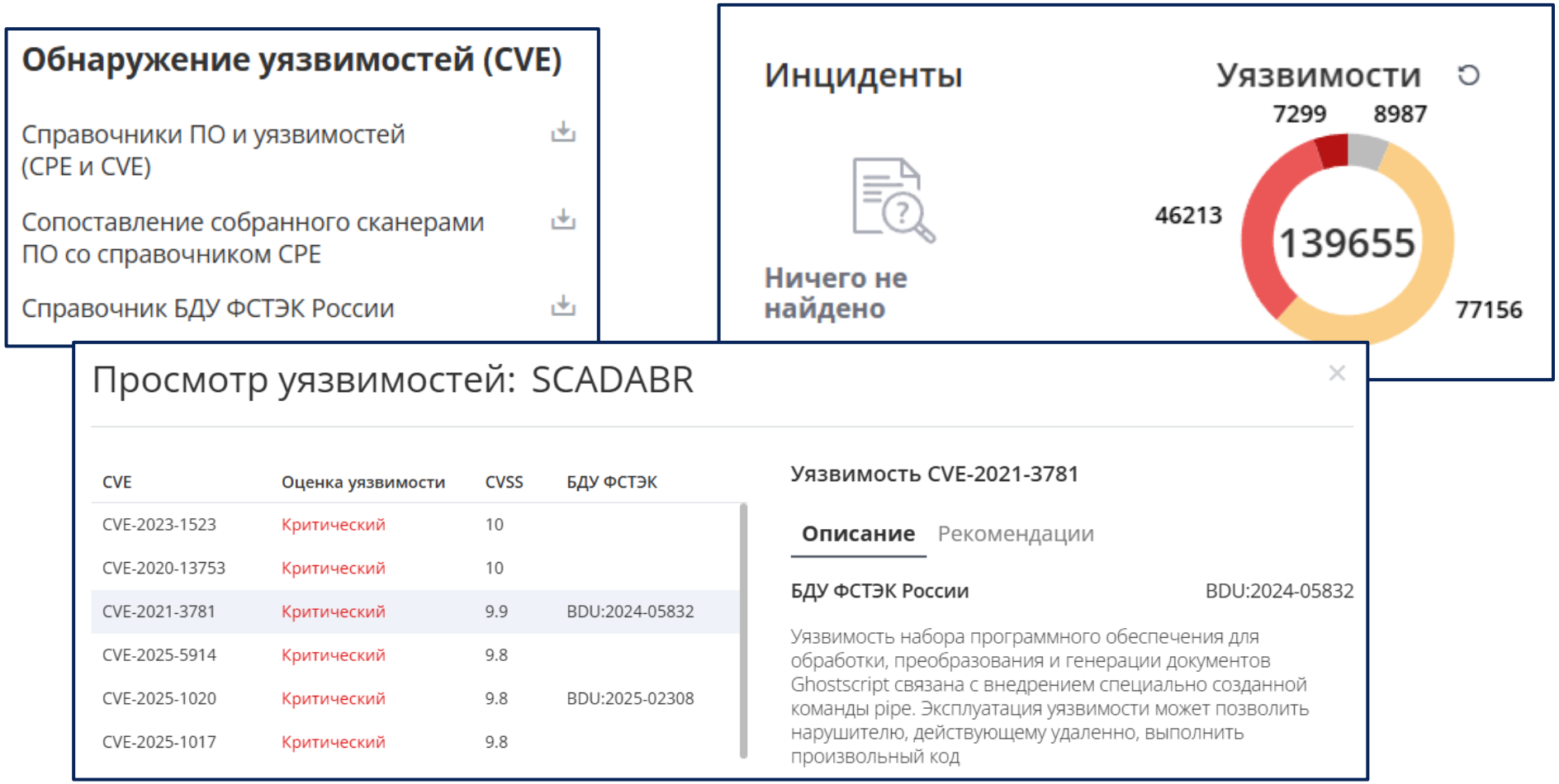
Сперва нужно собрать информацию об ОС (прошивке) и перечень ПО (для АРМ/серверов – для ПЛК/АСО неприменимо)



CyberLympha®

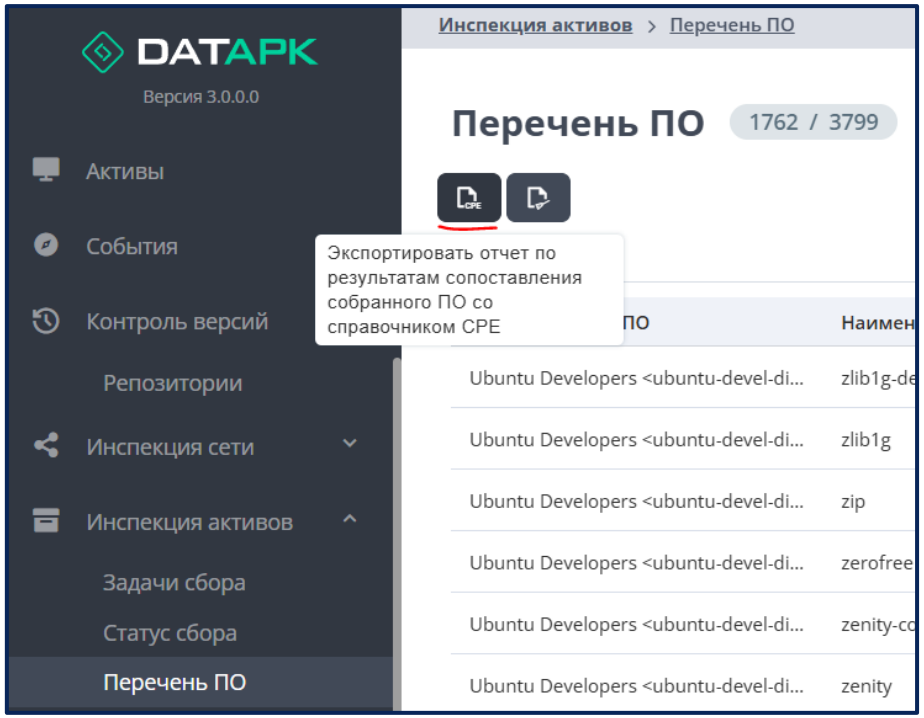
Поиск уязвимостей (CVE2CPE)

Далее – выполнить поиск уязвимостей (предварительно д.б. импортированы справочники)



Поиск уязвимостей (CVE2CPE)

Для дополнения таблицы маппинга необходимо экспортировать отчет результатов сопоставления со страницы «Перечень ПО» и передать производителю DATAPK (после того, как выполнили сбор ОС и ПО со всего интересующего оборудования и выполнили поиск уязвимостей)



Соседняя кнопка «Очистить отчет по результатам сопоставления» обнуляет прошлый отчет, и после ее нажатия необходимо повторить поиск уязвимостей на узлах, с которых требуется передать информацию производителю DATAPK (крайне редкий кейс – в типовых инсталляциях ее нажимать не нужно).

Вопросы?

udv|group